DoD O-2000.12-H

# DEPARTMENT OF DEFENSE

# DoD
# ANTITERRORISM
# HANDBOOK

## 9 February 2004

**ASSISTANT SECRETARY OF DEFENSE**

**FOR**

**SPECIAL OPERATIONS AND LOW INTENSITY CONFLICT**

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

FEB 9 2004

SPECIAL OPERATIONS/
LOW-INTENSITY CONFLICT

# FOREWORD

This Handbook is reissued under the authority of DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003 (reference (a)). It provides procedures and recommendations for reducing the risk and vulnerability of DoD personnel, their family members, facilities, and assets from acts of terrorism.

DoD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 1993 (reference (b)), is hereby canceled.

This Handbook applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard (when operating as a Military Service in the Navy). The term "Commanders," as used herein refers to personnel assigned to command positions at all levels and the heads of the Defense Agencies and Field Activities.

This Handbook is effective immediately. All measures that protect DoD assets and personnel from terrorist attack, whether or not they are specifically included in this Handbook, should be implemented consistent with local requirements identified by senior military commanders or civilian managers as appropriate. The Heads of the DoD Components may issue supplementary instructions when necessary to provide for unique requirements within their organizations.

Pursuant to subparagraph C3.2.1.2.1, DoD 5400.7-R, "DoD Freedom of Information Act Program" (reference (c)), this Handbook is For Official Use Only. Release of this Handbook to the public is subject to approval by the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (SO/LIC). The National Disclosure Policy shall govern disclosure of this document to foreign governments. Applicable portions of the Handbook may be released to DoD family members and foreign nationals employed by the Department of Defense to provide them with appropriate guidance on protection measures.

Submit recommended changes to this Handbook to:

Office of the Assistant Secretary of Defense
(Special Operations and Low-Intensity Conflict)
2500 Defense Pentagon, Room 5E368
Washington, DC 20301-2500

The DoD Components may obtain copies of this Handbook at the OASD (SO/LIC) and/or the Joint Staff Deputy Director for Antiterrorism/Homeland Defense (DDAT/HD) Secure Internet Protocol Network (SIPRNET) sites or via the Antiterrorism Enterprise Portal (ATEP): //www.atep.smil.mil.

Thomas W. O'Connell

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

APPENDICES

FIGURES

TABLES

REFERENCES

(a) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
(b) DoD O-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 1993 (hereby canceled)
(c) DoD 5400.7-R, "DoD Freedom of Information Act Program, " 4 September, 1998
(d) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," June 5, 2003
(e) DoD Instruction 2000.16, "DoD Antiterrorism Standards," June 14, 2001
(f) Section 1072(2) of Title 10, United States Code
(g) White House Report, "The National Strategy for Combating Terrorism," February, 2003[1]
(h) Presidential Decision Directive -39 (PDD-39), "U.S. Policy on Counterterrorism (U)," June 21, 1995[2]
(i) Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, April 24, 1996
(j) Presidential Decision Directive -62 (PDD-62)[3]
(k) Section 129, Atomic Energy Act of 1954 as amended (public Law 83-703)[4]
(l) Section 304, 309, Nuclear Nonproliferation Act of 1978 (Public Law 95-242)[5]
(m) DoD Directive 5210.56, "Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties," November 1, 2001
(n) DoD Directive 3025.15, "Military Assistance to Civil Authorities" February 18, 1997
(o) DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," January 15, 1986
(p) DoD Directive 5525.7, "Implementation of the Memorandum of Understanding between the Department of Justice and Department of Defense relating to the Investigation and Prosecution of Certain Crimes," January 22, 1985
(q) Sections 4801-4805 of Title 22, United States Code[6]
(r) FM 3-100.12, "Risk Management - Multi-service Tactics, Techniques, and Procedures for Risk Management," February 15, 2001
(s) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(t) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982
(u) DoD Directive 5200.27, "Acquisition Of Information Concerning Persons And Organizations Not Affiliated With The Department Of Defense," January 7, 1980
(v) Public Law 101-604, "Aviation Security Improvement Act of 1990"
(w) DoD Directive 5160.54 "Critical Asset Assurance Program (CAAP)," January 20 1998
(x) DoD "Antiterrorism Force Protection Installation Planning Template," June 1, 1998

[1] Copy of report can be found at http://www.defenselink.mil.pubs

[2] Copy of PDD can be found at http://fas.org/irp/offdocs/pdd39.htm

[3] Copy of PDD can be found at http://fas.org/irp/offdocs/pdd-62.htm

[4] Copy can be found at http://www.nrc.gov/who-we-are/governing-laws.html

[5] Copy can be found at http://www.nrc.gov/who-we-are/governing-laws.html

[6] Copy can be found at http://uscode.house.gov

(y) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January, 1995
(z) DoD 5220.22-R, "Industrial Security Regulation," December 1985
(aa) Weapons of Mass Destruction Appendix, "Antiterrorism Force Protection Installation Planning Template," November 1, 1998[7]
(ab) Joint Publication 5-00.2, "Joint Task Force Planning Guidance and Procedures," January 13, 1999[8]
(ac) Army FM 3-11.9, "Potential Military Chemical/Biological Agents and Compounds," May 6, 1996
(ad) DoD Instruction 2000.18, "Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines," December 4, 2002
(ae) Antiterrorism Act of 1990, Pub. L. 101-519, Sec. 132, November 5, 1990
(af) DoD 7000.14-R, "DoD Financial Management Regulation (FMRs), Volumes 1-15, current editions
(ag) CJCSI 3170.01C, "Joint Capabilities Integration and Development System," June 24, 2003[9]
(ah) Chapter 169, Title 10, United States Code
(ai) CJCSI 5261.01C, "Combating Terrorism Readiness Initiatives Fund," April 1, 2003[10]
(aj) DoD, Management Initiative Decision 913 (MID 913), 22 May 2003[11]
(ak) DoD Directive 3224.3, "Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing Evaluation, Production, Procurement, Deployment, and Support," February 17, 1989
(al) DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996
(am) DoD Directive 5230.16, "Nuclear Accident and Incident Public Affairs (PA) Guidance," December 20, 1993
(an) DoD Directive 5410.1, "Release of Information Concerning Accidental Casualties Involving Military Personnel or Equipment," September 27, 1973
(ao) DoD Directive 5410.14, "Cooperation with U.S. News Media Representatives at the Scene of Military Accidents Occurring Outside Military Installations," October 25, 1963
(ap) DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crisis," November 6, 1990
(aq) Joint Publication 4-0, "Doctrine for Logistics Support of Joint Operations," April 6, 2000[12]
(ar) Section 3261, Chapter 212, Title 18, United States Code
(as) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements, June 30, 1998
(at) DoD Directive C-4500.51, "DoD Non-Tactical Armored Vehicle Policy (U)," May 4, 1987

---

[7] Copy available from the DD AT/HD

[8] Copy can be found at http://www.dtic.mil/doctrine/jpplanningsseriespubs.htm

[9] Copy can be found at http://www.dtic.mil/cjcs_directives

[10] Copy can be found at http://www.dtic.mil/cjcs_directives

[11] Copy of MID available from OASD(SOLIC)

[12] Copy can be found at http://www.dtic.mil/doctrine/jplogisticsseriespubs.htm

(au) DoD 5200.8-R, "Physical Security Program," May 1991
(av) DoD Directive 5200.8, "Security of DoD Installations and Resources," April 25, 1991
(aw) UFC 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings," October 8, 2003[13]
(ax) UFC 4-010-02, "DoD Minimum Antiterrorism Standoff Distances for Buildings" (FOUO), October 8, 2003[14]
(ay) Federal Acquisition Regulation, current edition
(az) DoD Foreign Clearance Guide, current edition[15]

[13] Copy can be found at http://www.projnet.org/report/doc_ufc.html

[14] Copy can be found at http://www.atep.smil.mil or is available from OASD(SOLIC) or DD AT/HD

[15] available at www.fcg.pentagon.mil

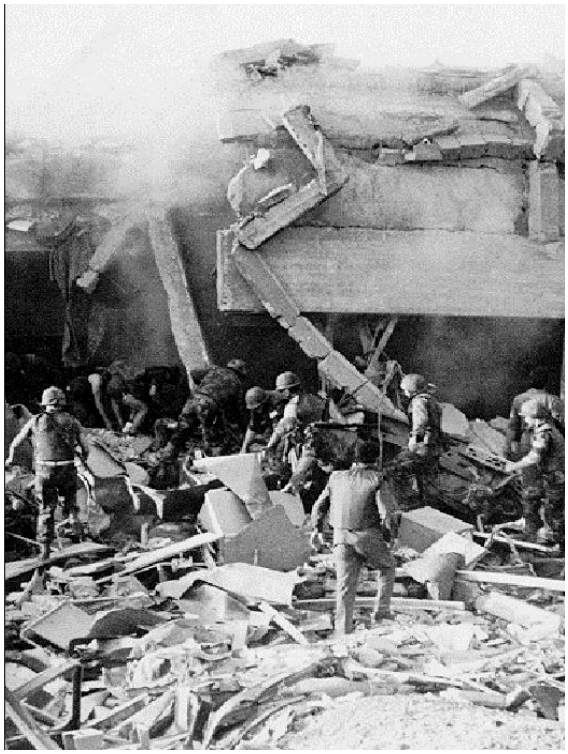
# C1. CHAPTER 1
# THE DoD ANTITERRORISM HANDBOOK

## C1.1. INTRODUCTION

C1.1.1. Terrorism is "the calculated use of unlawful violence or threat of unlawful 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" (JCS Pub 01-2 (reference (d)). Department of Defense (DoD) personnel, facilities, and materiel, Symbols of the U.S. Government, are identifiable targets for terrorists seeking to change U.S. policies at home or abroad. DoD personnel are the largest contingent of U.S. representatives overseas.

C1.1.2. History has shown that DoD personnel and facilities make lucrative targets for terrorist attack. The future predicts little change. Attacks on DoD personnel and facilities by individuals and organizations operating outside the formal command and control structure of national governments have claimed many lives; the cost to the U.S. Government is measured in millions of dollars.

**Figure C1.F1. The U.S. Marine Headquarters in Beirut, Lebanon, following a truck-bomb explosion in late October 1983.**



C1.1.3. The destruction of the U.S. Marine Headquarters at the Beirut International Airport in October 1983 was the greatest loss of American military personnel attributed to a single terrorist act. Although there were many lessons learned from this devastating attack, several subsequent attacks have been successfully carried out against the Department of Defense and other U.S. Government personnel at home and abroad.

C1.1.4. In June 25, 1996, terrorists struck again by bombing the Khobar Towers complex in Dhahran, Saudi Arabia. This watershed event took the lives of 19 American service personnel and injured more than 500. In the aftermath of Khobar Towers, extensive policy changes were made, antiterrorism (AT) standards were developed, and training programs were formalized laying the foundation for the Department of Defense's AT program that we have today.

**Figure C1.F2. A massive bomb gutted Building 131 in the Khobar Towers Complex in Dhahran, Saudi Arabia, on June 25, 1996, killing 19 U.S. Service members and injuring hundreds of others.**

**Figure C1.F3. The aftermath of a vehicular bombing of the U.S. Embassy in Nairobi, Kenya, August 7, 1998.**

**Figure C1.F4. The U.S. Embassy bombing in Dar es Salaam, Tanzania occurred five minutes after the attack in Nairobi, Kenya.**

C1.1.5. On August 7, 1998, nearly simultaneous bomb explosions at the U.S. Embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, resulted in significant loss of life. The two explosions killed more than 300 people, including 12 U.S. Government employees and family members, and injured more than 4,000 Kenyans, Tanzanians, and Americans. These attacks brought attention to gaps in the physical security and construction standards in our U.S. Embassies overseas. It also highlighted the improved capabilities of terrorists to plan for and strike at two different targets simultaneously. As a result, the U.S. invested resources to reduce the vulnerability of U.S. diplomatic missions around the world to terrorist attacks.

**Figure C1.F5. An explosive laden boat detonated aside the USS COLE on October 12, 2000 killing 17 and wounding 42 in the Port of Aden.**

C1.1.6. On October 12, 2000, the USS COLE was attacked in the Port of Aden when an explosive-laden boat detonated abeam her port side. This tragic event resulted in the death of 17 and wounding of 42 sailors.

**Figure C1.F6. World Trade Center towers and the Pentagon moments after being struck by hijacked airliners on September 11, 2001.**

C1.1.7. The morning of September 11, 2001 marks the worst terrorist strike against the United States to date. Within minutes of each other, three sky-jacked commercial airliners, piloted by suicidal Islamic extremists, crashed into both towers of the World Trade Center in New York City and the Pentagon in Washington DC. Although the exact number of casualties as a result of the September 11 terrorist attacks shall never be known, 3044 people are presumed dead.

C1.1.8. All these major attacks, as shown in Table C1.T1., demonstrate that terrorism continues to evolve, striking at the gaps and seams in our AT defense. The Department of Defense's AT effort is outlined in DoD Directive 2000.12 and DoD Instruction 2000.16 (references (a) and (e)). Together with this Handbook, these three cornerstone documents form a family of documents designed to provide commanders and antiterrorism officers (ATOs) at all levels with guidance on AT policy, standards, tactics, techniques, and procedures. Service, Combatant Command, DoD Agency and local directives complement cornerstone documents and enhance AT programs at every echelon. The capstone for an echelon's AT program is the sound leadership and judgment provided by that echelon's military commander or civilian equivalent.

**Table C1.T1. Matrix identifying nature of seven major terrorist attacks against the United States.**

| | Beirut | World Trade Center | Oklahoma City | Khobar Towers | East Africa | USS COLE | WTC & Pentagon |
|---|---|---|---|---|---|---|---|
| Perceived Threat | Sniper | None | None | Small Bomb | Small Bomb | Pierside Attack | Truck Bomb |
| Destructive Mechanism | Vehicle Bomb | Vehicle Bomb | Vehicle Bomb | Vehicle Bomb | Vehicle Bomb | Vehicle Bomb | Sky-jacked Airliners |
| Delivery Method | Truck | Van | Truck | Truck | Vans | Boat | Airplane |
| Place of Attack (Origin) | Mid East | NYC (Mid East) | Oklahoma | Mid East | Africa (Mid East) | Mid East | U.S. (Mid East) |
| Intel Assessed Threat (Threat Level) | General Threat (High) | None (Negligible) | None (Negligible) | General Threat (High) | General Threat (High) | General Threat (High) | None (Negligible) |
| Key Lesson | ROE Application | International CONUS Attack | Domestic CONUS Attack | Counter-surveillance & Standoff | Transnational Regional Threat | Determine Hostile Intent | Anticipate Out-of-the-box Threats |

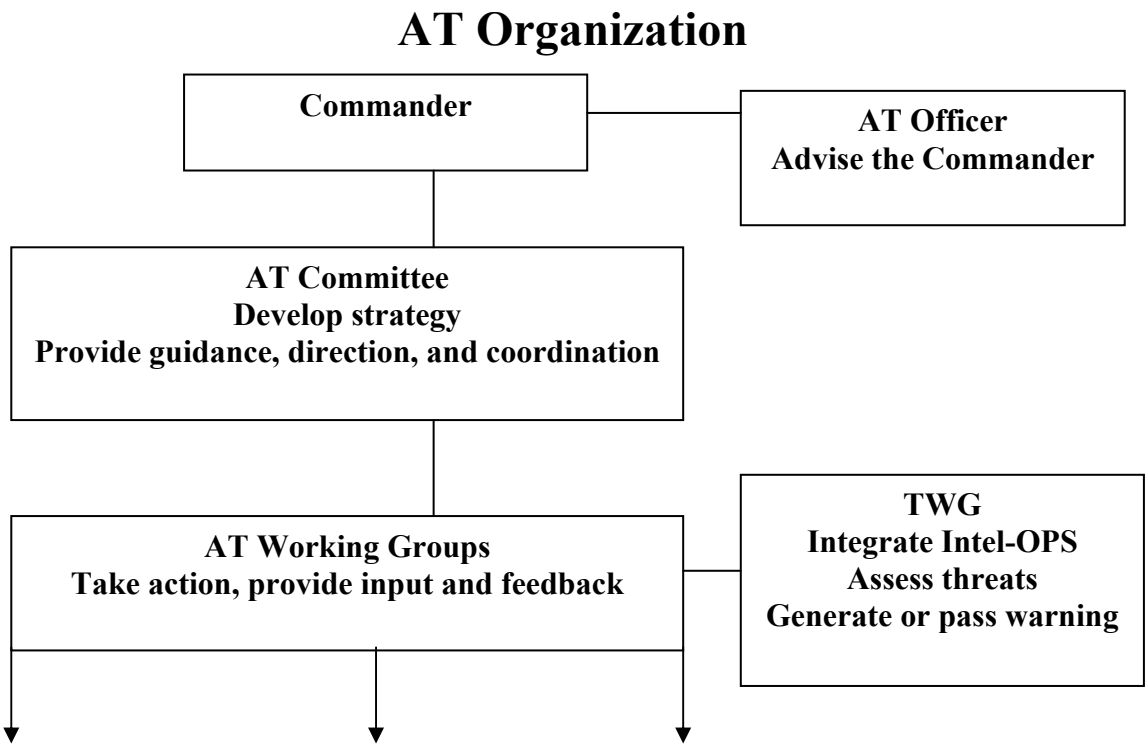
## C1.2. THE DoD ANTITERRORISM PROGRAM

C1.2.1. The DoD AT program is a collective effort that seeks to reduce the likelihood that DoD affiliated personnel, their families, facilities, and materiel shall be subject to a terrorist attack, and to prepare to respond to the consequences of such attacks should they occur. Reference (e) Standard 14 describes a Commander's major requirements and responsibilities for implementing an AT program.

C1.2.1.2. The AT program incorporates all defensive measures used to reduce the vulnerability of individuals and property to terrorist acts to include limited response and containment by local forces.

C1.2.1.3. It's essential to stress from the beginning that the effectiveness of any program is directly impacted by a commander's emphasis of the importance of his or her program, regardless of the level of command. The checklist found at Appendix 1 helps commanders and ATOs in determining the effectiveness of their AT program.

**Figure C1.F7. Sample Antiterrorism Organizational Concept**




C1.2.2. The figure above depicts a typical Antiterrorism organization at the installation level, though the need for both an AT Committee and AT Working Groups depends on the size and complexity of the facilities being protected. Regardless of size, every program needs a proactive Threat Working Group (TWG). Terms such as Antiterrorism Committee (ATC) are generic and differ from one theater to another, but their functions remain similar independent of labels.

C1.2.3. ATC. The ATC meets at the Commander/Senior Executive level to: address policy issues; make risk and other AT decisions; supervise and steer subordinate AT efforts; and review the AT program.

C1.2.4. Antiterrorism Working Group (ATWG). The ATWG meets at the Action Officer level to: develop and recommend policy; prepare planning documents; conduct criticality, vulnerability, and risk assessments.

C1.2.5. TWG. The TWG consists of the ATO, Counterintelligence (CI) representative, Law Enforcement representative, Information Operations representative and the Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE) representative. Larger installations may include additional personnel as assigned by their commander. Installation commanders that take an active role engaging local, state and federal law enforcement officials can obtain their input for the installation's TWG. In the United States and its territories, local installations must obtain local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, and other Federal Agencies. All members shall need applicable security clearances and access (unlike the remainder of the ATC or ATWG). The TWG meets periodically and/or as required to:

C1.2.5.1. Integrate all sources of threat with locally collected information.

C1.2.5.2. Complete the annual installation's AT Threat Assessment.

C1.2.5.3. Update the installation's AT Threat Assessment when threats change.

C1.2.5.4. Provide updated AT Threat Assessment information to the installation commander and to the ATWG.

C1.2.5.5. Process and report emergent threat information to the installation commander and ATO, who shall convene an emergency session of the ATWG (to include Federal Law Enforcement and intelligence counterparts). Some installations shall not have organic capabilities in all these areas and their TWGs must identify and designate intelligence and CI providers and maintain a robust dialogue with them.

C1.2.6. Commanders and their staffs should realize that every available resource must be considered when developing or reviewing an AT program and its associated plan. Often overlooked are the tenant organizations on an installation. To understand the relationship between the AT program and the AT plan, one can view the program as a collection of all ingredients while the plan is the detailed recipe (one complements the other) when separated, both shall fail.

C1.2.7. The AT program concept can be viewed as having two phases: Proactive and Reactive (crisis management).

C1.2.7.1. The proactive phase encompasses the planning; resourcing, preventive measures, awareness, education, training, and exercising that take place prior to a terrorist incident. During this phase, consideration is given to research and development, and

implementation of preventive measures. Commanders and directors must consider the installation infrastructure critical to mission accomplishment; integration of physical assets; funding requirements; security forces to detect, assess, delay, and respond to a threat; awareness education; and training (specialized skills proficiency training and exercising plans).

C1.2.7.1.1. The proactive phase begins with a deliberate application of the AT Risk Management process (Chapters 4 through 8). The steps of the AT Risk Management process (Threat, Criticality, Vulnerability, and Risk Assessments (TA, CA, VA, RA)) are conducted locally and lay the foundation for the Commander to make decisions and commit scarce resources. Determining the AT risk is essential since a Commander must understand the threat, what assets are most important to protect, and which of those important assets are most vulnerable. Assessing AT risk provides the value of an asset in relation to the AT threats and the vulnerabilities associated with it. This aids the Commander in balancing threats to vulnerabilities and the degree of risk that the Commander is willing to accept by not correcting, or perhaps being unable to correct, a vulnerability. For any vulnerability, the Commander shall manage risk by developing a strategy to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

C1.2.7.1.2. The Commander's strategy provides direction for developing the rest of the AT program (operational, personal, and physical security, training, exercising, reviewing, and planning). The AT plan is the mechanism for detailing this strategy and coordinating and executing the AT program.

C1.2.7.1.3. Continuous review is essential to ensure program improvement and evolution. Assessments (TA, CA, VA, and RA) and overall program review shall occur annually as a minimum. Exercise and incident feedback provide valuable insight into program improvement areas.

C1.2.7.2. The reactive phase includes implementation of crisis response plans, limited response and initiation of the appropriate response to a terrorist incident (military police and/or security forces, fire department, hazardous material (CBRNE), mass casualty, etc.). During the reactive phase the installation Commander conducts crisis AT risk management (see paragraph C4.3.1.).

C1.3. DoD AT POLICY AND THIS HANDBOOK

C1.3.1. This Handbook, while applicable at all levels, targets commanders and their ATOs in an effort to promote the AT awareness and security posture necessary to defend against acts of terrorism. Its structure aligns with AT program standards defined in reference (e) and is intended to help ATOs in fulfilling DoD requirements.

C1.3.2. This Handbook is suggestive in nature, providing recommendations for developing or improving an AT program. However, when directed by reference (a) or reference (e), the application of this Handbook's recommended actions become mandatory. The commander's authority to enforce security measures and responsibility to protect persons and property remains paramount. Nothing in this document shall detract from or conflict with the authorities and responsibilities of the Commanders and the Heads of the DoD Components.

C1.3.3. This Handbook, where necessary, directs readers to additional references that provide subject matter depth beyond the scope of this document. Additionally, Appendix 9 offers numerous website links for further reference.

C1.4. DEFINITIONS

C1.4.1. Reference (d) provides approved DoD terminology for general use by all DoD components. The following definitions supplement reference (d) until updated.

C1.4.1.1. Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

C1.4.1.2. AT Officer (ATO). The installation, base, regional, facility, or deploying unit AT advisor charged with managing the AT Program.

C1.4.1.3. AT Plan. The specific measures taken to establish and maintain an AT Program.

C1.4.1.4. AT Planning. The process of developing specific guidance and execution-oriented instructions for subordinates.

C1.4.1.5. AT Program. One of several security-related programs that fall under the overarching Combating Terrorism (CbT) programs that is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families,

facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource generation, and program reviews.

C1.4.1.6. AT Resource Generation. The process used to identify and submit requirements through existing DoD Planning, Programming, Budgeting and Execution (PPBE), CbT-Combating Terrorism Readiness Initiatives Fund (CbT–RIF), and other funding mechanisms. Central to success of resource generation is tracking, and then funding identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

C1.4.1.7. AT Risk Management. The process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. The end products of the AT program risk management process shall be the identification of areas and assets that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (TA, asset criticality assessment, and VA), the Commander must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or lessen the severity of the outcome of an attack. The Commander must decide on how best to employ given resources and AT force protection measures to deter, mitigate, or prepare for a terrorist incident.

C1.4.1.8. AT Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. Also, it is a product of a threat analysis for a particular unit, installation, or activity.

C1.4.1.9. AT Training. The development of individual, leader, and collective skills as well as conducting comprehensive exercises to validate plans for antiterrorism, incident response, consequence management, and continuity of essential military operations.

C1.4.1.10. AT VA.

C1.4.1.10.1. A DoD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a

terrorist attack. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

C1.4.1.10.2. The process the commander uses to determine the susceptibility to attack from the full range of threats to the security of personnel, family members, and facilities, which provide a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.

C1.4.1.11. Combating Terrorism (CbT). In the Department of Defense all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent (preempt), deter (disrupt), and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of chemical, biological, radiological, nuclear materials, or high-yield explosive (CBRNE) devices.

C1.4.1.12. Combating Terrorism Readiness Initiatives Fund (CbT–RIF). Program established by Congress and managed by the Joint Staff (J-3) that provides funds for emergency or unforeseen high priority Force Protection projects or equipment submitted by the Commanders of the Combatant Commands and approved by the Chairman of the Joint Chiefs of Staff.

C1.4.1.13. Commander. Any commanding officer, installation commander, or other command authority, or civilian supervisor in a comparable position.

C1.4.1.14. Consequence Management. Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to Governments, businesses, and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the States to respond and the Federal Government through the Department of Homeland Security as the primary Federal Agency to provide assistance as required. The Department of State is the primary Federal Agency for Foreign Consequence Management.

C1.4.1.15. Critical Asset. Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical assets may be DoD assets or other government or private assets,

(e.g. industrial or infrastructure critical assets), domestic or foreign, whose disruption or loss would render DoD critical assets ineffective or otherwise seriously disrupt DoD operations. Critical assets include traditional "physical" facilities and equipment, non-physical assets (such as software systems), or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

C1.4.1.16. Critical Infrastructure. Infrastructure deemed essential to DoD operations or the functioning of a Critical Asset.

C1.4.1.17. Critical Infrastructure Protection. DoD program to identify and protect assets critical to the Defense Transportation System. Loss of a critical asset would result in a failure to support the mission of a combatant commander. Assets include worldwide DoD, commercial, and civil physical and command, control, communications, computers, and intelligence infrastructures.

C1.4.1.18. Defense Contractor. Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies, or both, including construction. Thus, Defense contractors may include U.S. nationals, local citizens, or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DoD Component or foreign corporations wholly owned by foreign governments.

C1.4.1.19. Defense Criminal Investigative Organizations (DCIO). The U.S. Army Criminal Investigation Command (USACIDC), the Naval Criminal Investigative Service (NCIS), the Air Force Office of Special Investigations (AFOSI), and the Defense Criminal Investigative Service (DCIS) are the four DoD law enforcement organizations that make up the DCIOs. These agencies have law enforcement investigative responsibilities for federal felony offenses committed against the DoD and its Military Branches and are all members of the regional Joint Terrorism Task Forces (JTTF) and the National-JTTF.

C1.4.1.20. Duress System. A system that can covertly communicate a situation of duress (hostile, hostage, security compromised) to a security control center, or to other personnel who can notify a security control center.

C1.4.1.21. Emergency CbT-RIF Requirement. An unanticipated requirement created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act.

C1.4.1.22. Emergent CbT-RIF Requirement. A newly formed, unexpected requirement resulting from a logical consequence of unforeseen circumstances calling for prompt action.

C1.4.1.23. Family Member. Individuals defined as "dependent" in Section 1072(2) of 10 U.S.C (reference (f)). Includes spouses, unmarried widows, unmarried widowers; unmarried legitimate children, including adopted children or stepchildren, who are under 21, incapable of self-support or under 23 and enrolled in a full time education institution.

C1.4.1.24. Force Protection (FP). Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

C1.4.1.25. FP Conditions (FPCONs). A DoD-approved system that standardizes the Departments' identification and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principle means for a commander to apply an operational decision on how to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities.

C1.4.1.26. High-Risk Billet. Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

C1.4.1.27. Law Enforcement and Counterintelligence Community (LECIC). The USACIDC, U.S. Army Military Intelligence (MI), NCIS, AFOSI, and DCIS include the Department of Defense's law enforcement and counterintelligence investigative community. These agencies are responsible for law enforcement liaison and interaction with local, State, and Federal law enforcement agencies, including the FBI.

C1.4.1.28. Protective Service Operations (PSO). PSO entails the protection of dignitaries and other high-risk personnel in the combatant commander's area of responsibility where significant threats exist. Those threats include assaults, kidnappings, assassinations, and attempts to embarrass the U.S. Government. These conditions may result in the requirement to provide increased safety and security through the assignment of protective service details.

C1.4.1.29. Radiological Material. Radioactive material usually found in research, industrial or medical applications or radioactive waste from such operations.

C1.4.1.30. Security Organizations. Military law enforcement, military criminal investigative organizations, and DoD contracted security personnel.

C1.4.1.31. Terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear and intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

C1.4.1.32. Terrorist. An individual who uses unlawful violence, terror, and intimidation to achieve a result in pursuit of political, religious, or ideological objectives.

C1.4.1.33. Terrorist Group. Any element, regardless of size or espoused cause, that commits unlawful acts of violence or threatens unlawful violence in pursuit of its political, religious, or ideological objectives.

C1.4.1.34. Terrorist Threat Level. An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity, and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT, and HIGH. Threat levels should not be confused with FPCONs. Threat level assessments are provided to senior leaders to assist them determine the appropriate local FPCON.

C1.4.1.35. Vulnerability.

C1.4.1.35.1. In antiterrorism, a situation or circumstance, if left unchanged, that may result in the loss of life or damage to mission-essential resources.

C1.4.1.35.2. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its shall to fight diminished.

C1.4.1.35.3. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

C1.4.1.35.4. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.

C1.5. ABBREVIATIONS AND ACRONYMS

C1.5.1. Appendix A of reference (d) provides approved DoD abbreviations and acronyms for general use by all the DoD Components. This Handbook contains additional abbreviations and acronyms used in the AT field. The following abbreviations and acronyms are used in this Handbook:

| | | |
|---|---|---|
| C1.5.1.1. | AAR | After Action Review |
| C1.5.1.2. | ACIC | Army Counterintelligence Center |
| C1.5.1.3. | AFOSI | U.S. Air Force Office of Special Investigation |
| C1.5.1.4. | AM | Attack Means |
| C1.5.1.5. | AMC | Air Mobility Command |
| C1.5.1.6. | AOR | Area of Responsibility |
| C1.5.1.7. | AT | Antiterrorism |
| C1.5.1.8. | ATC | Antiterrorism Committee |
| C1.5.1.9. | ATCC | Antiterrorism Coordinating Committee |
| C1.5.1.10. | ATEP | Antiterrorism Enterprise Portal |
| C1.5.1.11. | ATF | Bureau of Alcohol, Tobacco, and Firearms |
| C1.5.1.12. | ATO | Antiterrorism Officer |
| C1.5.1.13. | ATOIC | U.S. Army Terrorist Operations and Intelligence Center |
| C1.5.1.14 | ATWG | Antiterrorism Working Group |
| C1.5.1.15. | BMM | Borrowed Military Manpower |
| C1.5.1.16. | BTS | Border and Transportation Security |
| C1.5.1.17. | CARVER | Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability |
| C1.5.1.18. | CBR | Chemical, Biological, and Radiological |

| | | |
|---|---|---|
| C1.5.1.19. | CBRNE | Chemical, Biological, Radiological, Nuclear, or high yield Explosives |
| C1.5.1.20. | CbT | Combating Terrorism |
| C1.5.1.21. | Cbt-RIF | Combating Terrorism Readiness Initiative Fund |
| C1.5.1.22. | CCTV | Closed Circuit Television |
| C1.5.1.23. | CI | Counter Intelligence |
| C1.5.1.24. | CIA | Central Intelligence Agency |
| C1.5.1.25. | COM | Chief of Mission |
| C1.5.1.26. | CONUS | Continental United States |
| C1.5.1.27. | COOP | Continuity of Operations Plan |
| C1.5.1.28. | CoS | Chief of Staff |
| C1.5.1.29. | COTS | Commercial-off-the-shelf |
| C1.5.1.30. | CT | Counter Terrorism |
| C1.5.1.31. | CVAMP | Core Vulnerability Assessment Management Program |
| C1.5.1.32. | CWG | Commercial-off-the-shelf Working Group |
| C1.5.1.33. | DASD (SO&CT) | Deputy Assistant Secretary of Defense (Special Operations and Combating Terrorism) |
| C1.5.1.34. | DCIO | Defense Criminal Investigative Organizations |
| C1.5.1.35. | DCIS | Defense Criminal Investigative Service |
| C1.5.1.36. | DD AT/HD | Joint Staff Deputy Director, Antiterrorism and Homeland Defense |
| C1.5.1.37. | DEA | Drug Enforcement Agency |
| C1.5.1.38. | DHS | Department of Homeland Security |
| C1.5.1.39. | DIA | Defense Intelligence Agency |
| C1.5.1.40. | DIPNOTE | Diplomatic Note |

| | | |
|---|---|---|
| C1.5.1.41. | DIWS | Defense Indications and Warning System |
| C1.5.1.42. | DOE | Department of Energy |
| C1.5.1.43. | DOJ | Department of Justice |
| C1.5.1.44. | DOS | Department of State |
| C1.5.1.45. | DOT | Department of Transportation |
| C1.5.1.46. | DTRA | Defense Threat Reduction Agency |
| C1.5.1.47. | ECPs | Entry Control Points |
| C1.5.1.48. | EEI | Essential Elements of Information |
| C1.5.1.49. | EOC | Emergency Operations Center |
| C1.5.1.50. | ESFs | Emergency Support Functions |
| C1.5.1.51. | FBI | Federal Bureau of Investigation |
| C1.5.1.52. | FEMA | Federal Emergency Management Agency |
| C1.5.1.53. | FP | Force Protection |
| C1.5.1.54. | FPCON | Force Protection Conditions |
| C1.5.1.55. | FPED | Force Protection Equipment Demonstration |
| C1.5.1.56. | FPTAS | Flight Path Threat Analysis Simulation |
| C1.5.1.57. | FPWG | Force Protection Working Group |
| C1.5.1.58. | GAO | Government Accounting Office |
| C1.5.1.59. | GOTS | Government-off-the-shelf |
| C1.5.1.60. | GSA | General Services Administration |
| C1.5.1.61. | HAVs | Heavy non-tactical Armored Vehicles |
| C1.5.1.62. | HAZMAT | Hazardous Materials |
| C1.5.1.63. | HRB | High Risk Billet |
| C1.5.1.64. | HRP | High Risk Persons |
| C1.5.1.65. | HUMINT | Human Intelligence |
| C1.5.1.66. | HVAC | Heating, Ventilation, and Air-Conditioning |

| | | |
|---|---|---|
| C1.5.1.67. | HSC | Homeland Security Council |
| C1.5.1.68. | IDS | Intrusion Detection Sensors |
| C1.5.1.69. | IED | Improvised Explosive Device |
| C1.5.1.70. | IICT | Interagency Intelligence Committee on Terrorism |
| C1.5.1.71. | IPL | Integrated Priority List |
| C1.5.1.72. | IPT | Installation Antiterrorism Program and Planning Tool |
| C1.5.1.73. | I&W | Indications and Warning |
| C1.5.1.74. | IRT | Incident Response Team |
| C1.5.1.75. | IVAs | Integrated Vulnerability Assessments |
| C1.5.1.76. | JITF-CT | Joint Intelligence Task Force- Combating Terrorism |
| C1.5.1.77. | JNLWD | Joint Non-Lethal Weapons Directorate |
| C1.5.1.78. | JSIVA | Joint Staff Integrated Vulnerability Assessment |
| C1.5.1.79. | JTTF | Joint Terrorism Task Force |
| C1.5.1.80. | LAV | Light non-tactical Armored Vehicles |
| C1.5.1.81. | LECIC | Law Enforcement and Counterintelligence Community |
| C1.5.1.82. | LFA | Lead Federal Agency |
| C1.5.1.83. | LIC | Low Intensity Conflict |
| C1.5.1.84. | LVAs | Local Vulnerability Assessments |
| C1.5.1.85. | MANPAD | Man Portable Air Defense |
| C1.5.1.86. | MCIA | Marine Corps Intelligence Agency |
| C1.5.1.87. | MDITDS | Migration Defense Intelligence Threat Database System |
| C1.5.1.88. | MEVA | Mission Essential Vulnerable Area |
| C1.5.1.89. | MI | Military Intelligence |

| | | |
|---|---|---|
| C1.5.1.90. | MSHARP | Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity |
| C1.5.1.91. | MTAC | Navy Multiplke Threat Alert Center |
| C1.5.1.92. | NCIS | Naval Criminal Investigative Service |
| C1.5.1.93. | NSA | National Security Agency |
| C1.5.1.94. | NSC | National Security Council |
| C1.5.1.95. | NTAV | Non-tactical Armored Vehicle |
| C1.5.1.96. | O/C | Observer/Controllers |
| C1.5.1.97. | OOD | Officer of the Deck |
| C1.5.1.98. | O&M | Operations and Maintenance |
| C1.5.1.99. | PA | Public Affairs |
| C1.5.1.100. | PAO | Public Affairs Officer/Office |
| C1.5.1.101. | PBD | Program Budget Decision |
| C1.5.1.102. | PCC | Policy Coordinating Committee |
| C1.5.1.103. | PDM | Program Decision Memorandum |
| C1.5.1.104. | POVs | Privately Owned Vehicles |
| C1.5.1.105. | PPBE | Planning, Programming, Budgeting and Execution System |
| C1.5.1.106. | PS | Physical Security |
| C1.5.1.107. | PSD | Protective Security Detail |
| C1.5.1.108. | PSEAG | Physical Security Equipment Action Group |
| C1.5.1.109. | PSO | Protective Service Operations |
| C1.5.1.110. | RA | Risk Assessment |
| C1.5.1.111. | RAM | Random Antiterrorism Measures |
| C1.5.1.112. | RDA | Research, Development, and Acquisition |
| C1.5.1.113. | RIF | Readiness Initiative Fund |

| | | |
|---|---|---|
| C1.5.1.114. | ROE | Rules of Engagement |
| C1.5.1.115. | RSO | Regional Security Officer |
| C1.5.1.116. | S&T | Science and Technology |
| C1.5.1.117. | SAF | Small Arms Fire |
| C1.5.1.118. | SDF | Self Defense Force |
| C1.5.1.119. | SECDEF | Secretary of Defense |
| C1.5.1.120. | SECSTATE | Secretary of State |
| C1.5.1.121. | SES | Senior Executive Service |
| C1.5.1.122. | SIGINT | Signal Intelligence |
| C1.5.1.123. | SJA | Staff Judge Advocate |
| C1.5.1.124. | SOFA | Status of Forces Agreement |
| C1.5.1.125. | SO/LIC | Special Operations and Low Intensity Conflict |
| C1.5.1.126. | SOPA | Senior Officer Present Afloat |
| C1.5.1.127. | SOPs | Standard Operating Procedures |
| C1.5.1.128. | SOW | Statement of Work |
| C1.5.1.129. | SSDF | Shipboard Self-Defense Force |
| C1.5.1.130. | SWAT | Special Weapons and Tactics |
| C1.5.1.131. | TA | Threat Assessment |
| C1.5.1.132. | TACON | Tactical Control |
| C1.5.1.133. | TICs | Toxic Industrial Chemicals |
| C1.5.1.134. | TIMs | Toxic Industrial Materials |
| C1.5.1.135. | TSA | Transportation Security Administration |
| C1.5.1.136. | TRB | Tactical Response Boat |
| C1.5.1.137. | TSWG | Technical Support Working Group |
| C1.5.1.138. | TTPs | Tactics, Techniques, and Procedures |
| C1.5.1.139. | TWG | Threat Working Group |

| | | |
|---|---|---|
| C1.5.1.140. | UFR | Unfunded Requirement |
| C1.5.1.141. | USACIDC | U.S. Army Criminal Investigation Command |
| C1.5.1.142. | USCG | United States Coast Guard |
| C1.5.1.143. | USTRANSCOM | United States Transportation Command |
| C1.5.1.144. | VA | Vulnerability Assessment |
| C1.5.1.145. | WMD | Weapons of Mass Destruction |
| C1.5.1.146. | WMDRF | Weapons of Mass Destruction Response Functions |

# C2. CHAPTER 2
# U.S. GOVERNMENT POLICY, STRATEGY, AND ORGANIZATION TO COMBAT TERRORISM

## C2.1. GENERAL U.S. GOVERNMENT POLICY

C2.1.1. Terrorism is a threat to our national security. The intent of the United States' national strategy for combating terrorism, as outlined in the White House report, " National Strategy for Combating Terrorism, " February 2003 (reference (g)) is to stop terrorist attacks against the United States , its citizens, its interests, and its friends and allies around the world and ultimately, to create an international environment inhospitable to terrorists and all those who support them. In support of these efforts, the United States shall:

C2.1.1.1. In concert with its partners defeat terrorist organizations of global reach by attacking their sanctuaries; leadership; command, control, and communications; material support; and finances.

C2.1.1.2. Deny further sponsorship, support, and sanctuary to terrorists by ensuring other states accept their responsibilities to take action against international terrorist threats within their sovereign territory.

C2.1.1.3. Diminish the underlying conditions that terrorists seek to exploit by enlisting the international community to focus its efforts and resources on the areas most at risk.

C2.1.1.4. Defend the United States, its citizens, and interests at home and abroad by both proactively protecting the homeland and extending defenses to ensure the threat is identified and neutralized as early as possible.

C2.1.1.5. Be victorious in the war against terror no matter how long it takes.

C2.1.2. Measures to CbT. To ensure that the United States is prepared to CbT in all its forms, a number of measures have been directed. AT measures (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (CT) measures (offensive measures taken to prevent (preempt), deter (disrupt), and respond to terrorism). These include:

C2.1.2.1. Reduce Vulnerabilities. In order to reduce our vulnerabilities to terrorism, both at home and abroad, all department and agency heads have been directed to ensure that their personnel and facilities are protected against terrorism. Specific efforts that shall be conducted to ensure our security against terrorist acts include the following:

C2.1.2.1.1. Review the vulnerability of government facilities and critical national infrastructure (AT).

C2.1.2.1.2. Expand the counterterrorism program (CT).

C2.1.2.1.3. Reduce vulnerabilities affecting military and civilian personnel and facilities abroad (AT).

C2.1.2.1.4. Reduce vulnerabilities affecting U.S. airports (aircraft, passengers, and cargo) and provide appropriate security measures for other modes of transportation (AT).

C2.1.2.1.5. Excluding or deporting persons who pose a terrorist threat (CT).

C2.1.2.1.6. Preventing (preempt) unlawful traffic in firearms and explosives and protecting the President and other officials against terrorist attack (AT and CT).

C2.1.2.1.7. Reduce U.S. vulnerabilities to international terrorism through intelligence collection and analysis, counterintelligence, and covert action (AT and CT).

C2.1.2.2. Deter (disrupt). To deter (disrupt) terrorism, it is necessary to provide a clear public position that United States policies are not affected by terrorist acts and that terrorists and their sponsors are vigorously pursued to eliminate terrorist capabilities and support. In this regard, it must be made clear that terrorism shall not be allowed to succeed and that the pursuit, arrest, and elimination of terrorists is of the highest priority (CT).

C2.1.2.3. Respond. To respond to terrorism, the United States must have a rapid and decisive capability to protect Americans, defeat terrorists, respond against terrorist sponsors, and provide relief to the victims of terrorists attacks (PDD39, "United States Policy on Counterterrorism " (reference (h)) (AT and CT)).

C2.1.3. In addition, the U.S. Government has adopted a policy that removes any benefit for terrorist behavior and threatens retaliation for such acts. The U.S. Government seeks to make it difficult for terrorists to carry out attacks on U.S. citizens. If attacks on U.S. citizens can be thwarted or minimized, terrorists shall soon rethink the benefits to their cause of assaulting U.S. citizens (AT and CT).

## C2.2. THE U.S. GOVERNMENT STRATEGY FOR COMBATING TERRORISM

C2.2.1. The basic strategy employed by the U.S. Government to CbT is one of direct and continuous action against terrorist groups, the cumulative effect of which shall initially disrupt,

over time degrade, and ultimately destroy the terrorist organizations. The strategy has several elements:

C2.2.1.1. The United States, with its ability to build partnerships and project power, shall lead the fight against terrorist organizations of global reach.

C2.2.1.2. Strike terrorist groups constantly to ensure that terrorists have no place to hide, to compress their scope, and reduce their capability.

C2.2.1.3. Adapt old alliances and create new partnerships to facilitate regional solutions that further isolate the spread of terrorism.

C2.2.1.4. As the scope of terrorism becomes more localized, unorganized, and relegated to the criminal domain, the United States shall rely upon and assist other states in eradicating terrorism at its root.

C2.2.1.5. The United States shall constantly strive to enlist the support of the international community, however the United States shall not hesitate to act alone, to exercise the right of self defense, including acting preemptively against terrorists to prevent them from doing harm to U.S. citizens.

C2.2.2. Enactment of the Antiterrorism and Effective Death Penalty Act of 1996 (reference (i)) makes it much easier for the U.S. Government to assert extraterritorial jurisdiction and seek extradition (by cooperation or coercive techniques) of alleged terrorists.

C2.2.3. The U.S. Government has implemented a "4D" Strategy (Defeat, Deny, Diminish and Defend) to prosecute the Global War on Terrorism.

C2.2.3.1. The first goal " Defeat Terrorists and their Organizations" entails defeating terrorist organizations of global reach through the direct or indirect use of diplomatic, economic, information, law enforcement, military, financial, intelligence, and other instruments of power. The supporting objectives include:

C2.2.3.1.1. Defeat terrorists and their organizations.

C2.2.3.1.2. Identify terrorists and their organizations.

C2.2.3.1.3. Locate terrorists and their organizations.

C2.2.3.1.4. Destroy terrorists and their organizations.

C2.2.3.2. The second goal "Deny Sponsorship, Support, and Sanctuary to Terrorists" focuses on the responsibilities of all States to fulfill their obligations to CbT both within their

borders and internationally. The United States shall target assistance to those States that are willing to combat terrorism, but may not have the means. When States prove reluctant or unwilling to meet their international obligations to deny support and sanctuary to terrorists, the United States, in cooperation with friends and allies (or if necessary acting independently), shall take appropriate steps to convince them to change their policies. The supporting objectives include:

C2.2.3.2.1. End the State sponsorship of terrorism.

C2.2.3.2.2. Establish and maintain an international standard of accountability with regard to combating terrorism.

C2.2.3.2.3. Strengthen and sustain the international effort to fight terrorism. By performing the following:

C2.2.3.2.3.1. Working with willing and able States.

C2.2.3.2.3.2. Enabling weak States.

C2.2.3.2.3.3. Persuading reluctant States.

C2.2.3.2.3.4. Compelling unwilling States.

C2.2.3.2.4. Interdicting and disrupting material support for terrorists.

C2.2.3.2.5. Eliminating terrorist sanctuaries and havens.

C2.2.3.3. The third goal "Diminish the Underlying Conditions that Terrorists Seek to Exploit" shall be pursued through ongoing U.S. efforts to resolve regional disputes and foster economic, social, and political development; market-based economies, good governance, and the rule of law. This shall contribute to the campaign against terrorism by addressing underlying conditions that terrorists often seek to manipulate for their own advantage. The supporting objectives include:

C2.2.3.3.1. Partner with the international community to strengthen weak States and prevent the reemergence of terrorism.

C2.2.3.3.2. Win the war of ideas. Together with the international community, wage a war of ideas to make clear that all acts of terrorism are illegitimate, to ensure that the conditions and ideologies that promote terrorism do not find fertile ground in any nation, to diminish the underlying conditions that terrorists seek to exploit in areas most at risk, and to kindle the hopes and aspirations of those in societies ruled by the sponsors of terrorism.

C2.2.3.4. The fourth goal "Defend U.S. Citizens and Interests at Home and Abroad" encompasses the nation's collective efforts to defend the United States' sovereignty, territory, and its national interests, at home and abroad. This goal includes the physical and cyber protection of the United States, its populace, property, and interests, as well as the protection of its democratic principles. The supporting objectives include:

C2.2.3.4.1. Implement the National Strategy for Homeland Security.

C2.2.3.4.2. Attain domain awareness.

C2.2.3.4.3. Enhance measures to ensure the integrity, reliability, and availability of critical physical and information-based infrastructures at home and abroad.

C2.2.3.4.4. Integrate measures to protect U.S. citizens abroad.

C2.2.3.4.5. Ensure an integrated incident management capability.

## C2.3. THE U.S. GOVERNMENT COMBATING TERRORISM STRUCTURE

The U.S. Government has developed a formal structure to provide policy guidance and programmatic coordination of efforts to combat terrorism both at home and abroad. As the DoD Components may be required to provide support to other U.S. Government agencies, knowledge of the institutional framework within which such support and cooperation must be provided shall help commanders discharge their responsibilities effectively.

### C2.3.1. The National Security Council (NSC) Policy Coordinating Committee (PCC) for Counterterrorism and National Preparedness.

C2.3.1.1. The Assistant to the President for National Security Affairs chairs the NSC PCC for Counterterrorism and National Preparedness. This PCC has a standing committee consisting of representatives of the following agencies and departments:

C2.3.1.1.1. Department of State (DOS).

C2.3.1.1.2. Department of Defense

C2.3.1.1.3. Department of Justice (DOJ) (The Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA)).

C2.3.1.1.4. Department of Homeland Security (DHS) (The U.S. Coast Guard (USCG), the U.S. Secret Service, the Bureau of Citizenship and Immigration Services, the Transportation Security Administration (TSA), and the Federal Emergency Management Agency (FEMA)).

C2.3.1.1.5. Department of Energy (DOE).

C2.3.1.1.6. Department of the Treasury (The Bureau of Alcohol, Tobacco, and Firearms (ATF)).

C2.3.1.1.7. Department of Transportation (DOT).

C2.3.1.1.8. Central Intelligence Agency (CIA).

C2.3.1.1.9. National Security Council (NSC).

C2.3.1.2. The PCC also has several subcommittees. Membership in the subcommittees may vary depending on the issue at hand. Major responsibilities assigned to permanent members of the PCC are discussed below.

C2.3.1.2.1. The DOS. The DOS has several important responsibilities concerning U.S. Government efforts to CbT. Specifically the DOS shall:

C2.3.1.2.1.1. Conduct diplomatic efforts to isolate terrorist groups and those nations that provide support or direction.

C2.3.1.2.1.2. Lead development of AT assistance programs to be provided by the Agency for International Development or the Department of Defense under various foreign assistance programs authorized by law.

C2.3.1.2.1.3. Assume lead agency responsibilities for managing overseas terrorist incidents involving U.S. Government–affiliated personnel, facilities, and material.

C2.3.1.2.1.4. Identifies security requirements and recommends appropriate security program remedies for U.S. Government officials abroad.

C2.3.1.2.1.5. Disseminates to the general public information regarding terrorist risk outside of the continental United States (CONUS).

C2.3.1.2.2. The DOJ. Several organizations within the DOJ have responsibilities for dealing with matters pertaining to terrorism. The major DOJ organizations involved are the following:

C2.3.1.2.2.1. The FBI. The lead U.S. Government agency for investigating and prosecuting criminal acts committed against U.S. Government personnel, on U.S. Government reservations, or against U.S. Government property. As a result of enactment of PDD-62 (reference (j)), the FBI is responsible for investigating attacks on Americans overseas whenever

the U.S. Government considers exercising extraterritorial jurisdiction. The FBI also carries out the following responsibilities:

C2.3.1.2.2.1.1. Maintains civilian counterterrorism capabilities, which can be used in response to criminal or terrorist incidents within the United States, its territories, and its possessions.

C2.3.1.2.2.1.2. Conducts assessments and evaluations of aviation security measures and practices with the TSA.

C2.3.1.2.2.1.3. Collects, analyzes, and disseminates domestic terrorism threat information and warning, and supports other intelligence collection and analysis organizations responsible for international terrorism threat analysis.

C2.3.1.2.2.1.4. Provides scientific, technical, forensic, and investigative assistance to other Federal and State agencies in investigating criminal acts that may be terrorist in character.

C2.3.1.2.2.1.5. Provides technical assistance to foreign law enforcement and prosecutorial agencies.

C2.3.1.2.2.1.6. Disseminates information to the general public regarding terrorist threats within CONUS, U.S. territories, and U.S. possessions.

C2.3.1.2.2.2. The DEA. Provides information on possible terrorist activity to other Federal Agencies and departments as part of its counternarcotics mission. The DEA also provides scientific and technical support to investigative activities as appropriate.

C2.3.1.2.2.3. The U.S. Marshals Service. Provides information to other Federal Agencies and departments on the movements and activities of persons in whom it takes an interest. Such persons include ex-Federal felons, Federal felons under its parole supervision, and persons participating in the Federal Witness Protection Program.

C2.3.1.2.3. The DHS. The DHS first priority is to protect the nation against terrorist attacks. DHS has five major divisions or directorates: Border and Transportation Security (BTS); Emergency Preparedness and Response; Science and Technology (S & T); Information Analysis and Infrastructure Protection; and Management. The BTS Directorate is responsible for maintaining the security of our nation's borders and transportation systems. The largest of the directorates, it is the home of agencies that guard the country's borders and airports, protect

critical infrastructure, and coordinate responses for emergencies. Beside the five directorates, several agencies are part of the DHS.

C2.3.1.2.3.1. The U.S.C.G. Generally responsible for security within U.S. ports and navigable waterways and for the development and implementation of security standards regarding terrorist attacks on maritime activities, including assaults on passenger ships, cargo vessels, and navigation aids. It is the lead U.S. Government agency whenever terrorist incidents affecting U.S. citizens on passenger or cargo vessels occur. In the event that a terrorist incident occurs on a moored U.S. Navy ship within an U.S. non-Navy port, or a Navy port without organic security forces, the Coast Guard shall form a security perimeter around the vessel both on land and in the water. The U.S. Navy shall have responsibility for regaining control of the ship and releasing hostages.

C2.3.1.2.3.2. The U.S. Secret Service. Involved in those aspects of the U.S. Government's efforts to combat terrorism related to the protection of the President, the Vice President, members of their families, and other individuals for whom it provides security. It is involved in the collection, analysis, and dissemination of information regarding potential terrorist threats. It also participates in S & T projects related to personnel protection, explosive detection, and other subjects of special interest.

C2.3.1.2.3.3. Bureau of Citizenship and Immigration Services. Provides information to other Federal Agencies and departments on international movements of persons who seek entry into the United States even though they may not be eligible for entry (for example, ex-felons). It also provides information on those individuals who have previously been denied entry into the United States, have previously been deported, or have previously been thwarted in their attempts to enter or remain unlawfully in the United States.

C2.3.1.2.3.4. The U.S. Customs and Border Patrol. The U.S. Customs and Border Patrol has multiple roles in the U.S. Government's AT efforts. It shall:

C2.3.1.2.3.4.1. Detect and prosecute unlawful importation of explosives, ammunition, and firearms into the United States and impounds the materials.

C2.3.1.2.3.4.2. Seize, detect, and prosecute unlawful export of licensed arms, ammunitions, explosives, and dual-purpose technology that could be employed by terrorists to conduct or support terrorist attacks.

C2.3.1.2.3.4.3. Participate in U.S. Government counter-narcotic enforcement activities.

C2.3.1.2.3.4.4. Conduct a modest research and development program with many applications to AT.

C2.3.1.2.3.4.5. Provide information to other Federal Agencies concerning the identity of potential terrorists as well as their methods of operation, potential targets of attack, and potential vulnerabilities or weaknesses in terrorist groups.

C2.3.1.2.3.5. The FEMA. The lead agency within the DHS for consequence management. It ensures that the National Response Plan (formerly Federal Response Plan) is adequate for consequence management activities in response to domestic terrorist attacks involving weapons of mass destruction (WMD).

C2.3.1.2.3.6. The TSA. Ensure the security of all transportation modes to ensure freedom of movement for people and commerce. This includes civil aviation security and related research and development activities. The TSA is the lead agency whenever an international terrorist incident occurs involving an aircraft in flight. For purposes of assigning responsibility in these matters, "flight" begins when the aircraft door is closed and secured and the aircraft is no longer dependent on ground service. TSA is also responsible for other modes of transportation that are used by the Department of Defense.

C.2.3.1.2.3.7. The Federal Protective Service. A law enforcement organization that provides physical and personnel security to U.S. Government officers and employees as well as visitors while they are within General Services Administration (GSA) owned or operated facilities.

C2.3.1.2.4. The Department of the Treasury.

C2.3.1.2.4.1. The Bureau of ATF. Provides technical and analytical skills in support of U.S. Government incident responses. It also provides substantial technical and scientific support to other agencies and departments involved in the development of bomb detection systems. It participates in investigations and prosecution of cases involving violation of Federal arms, ammunition, and explosive laws.

C2.3.1.2.5. The DOT. Collaborates with DHS on all matters relating to transportation security and transportation infrastructure protection. The DOT is responsible for operating the national air space system.. The DOT collaborates with the DHS in regulating the transportation of hazardous materials by all modes (including pipelines).

C2.3.1.2.6. The DOE. Collects, analyzes, and disseminates information to Federal Agencies and departments regarding risks and vulnerabilities of energy systems to terrorist attack. It also develops a wide range of specialized equipment, highly trained personnel, and other counterterrorism capabilities. These capabilities have been developed to assist the FBI and other Federal Agencies in the event that materials or products subject to Federal regulation and licensing under the Atomic Energy Act as amended and the Nuclear Nonproliferation Act (references (k) and (l)) become the target of or are allegedly used in the commission of terrorist acts at home or abroad.

C2.3.1.2.7. The CIA. Leads the national-level intelligence collection, analysis, and terrorist threat dissemination effort conducted by all members of the U.S. intelligence community.

C2.3.1.2.8. The NSC. Assists in the coordination of domestic and international responses to terrorist incidents and provides additional policy studies and analyses as directed by the President.

C2.3.1.2.9. The GSA. As the general property landlord for the Federal Government, GSA supports the development of appropriate physical security devices and procedures to protect persons and property found within Federal reservations, installations, and buildings.

C2.3.2. The Homeland Security Council (HSC). Securing Americans from terrorist threats or attacks is a critical national security function. It requires extensive coordination across a broad spectrum of Federal, State, and local agencies to reduce the potential for terrorist attacks and to mitigate damage should such an attack occur. The HSC ensures coordination of all homeland security-related activities among executive departments and agencies and promotes the effective development and implementation of all homeland security policies. The HSC is chaired by DHS and is similar in structure and function to the NSC.

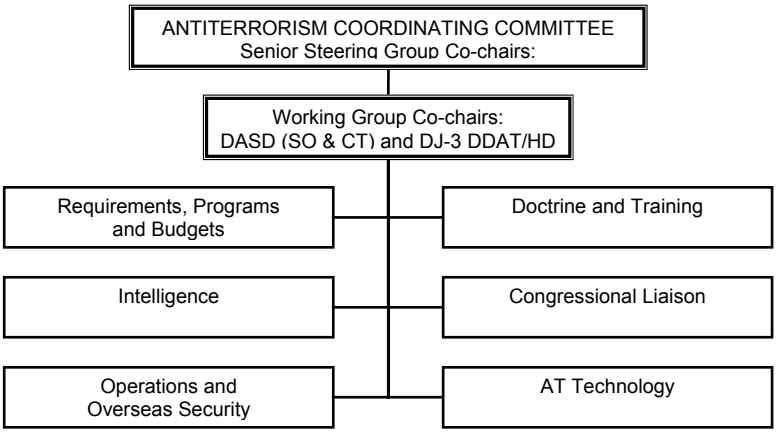
C2.4. DoD RESPONSIBILITIES FOR CbT

References (a) and (e) are two primary documents that implement the DoD AT program. Reference (a) establishes the Chairman of the Joint Chiefs of Staff as the principal military advisor and focal point to the Secretary of Defense for all DoD AT issues. It also defines the AT responsibilities of the Military Departments, the Commanders of the Combatant Commands, and the Defense Agencies for DoD activities in their respective organizations. Reference (e) provides further guidance and standards for the execution of reference (a). Specific roles and responsibilities are prescribed in detail in these directives.

## C2.5. DoD ANTITERRORISM COORDINATING COMMITTEE (ATCC)

The DoD ATCC comprises a Senior Steering Group, a Working Group, and six subgroups. The Senior Steering Group is co-chaired by the ASD (SO/LIC) and the DJ-3, Director for Operations, Joint Staff, and meets as needed. The Working Group is co-chaired by the Deputy ASD for Special Operations and Combating Terrorism (SO&CT) and the Deputy Director for Antiterrorism/Homeland Defense (DDAT/HD) and meets quarterly. There are six subgroups within the ATCC framework, which address specific facets of the DoD AT program. The six subgroups meet periodically and are organized to address topics of concern to policymakers, resource managers, and operators in the field. Representatives of other DoD Components participate on request or as appropriate for the topics of discussion. The organization structure is shown in figure C2.F1.

**Figure C2.F1. The DoD Antiterrorism Coordinating Committee**



# C3. CHAPTER 3
# THE DoD ANTITERRORISM PROGRAM: LAW AND REGULATION

## C3.1. INTRODUCTION

The DoD AT program sets forth DoD policy to deter, defeat and respond vigorously to all terrorist attacks. All terrorism acts are a potential threat to national security. The DoD AT program conforms with international and domestic law, and is based upon DoD authority and policy and is further implemented by policies issued by the Services and the Combatant Commanders.

## C3.2. AUTHORITY FOR HANDLING TERRORIST INCIDENTS

### C3.2.1. Commander's Responsibilities Inside The United States, Its Territories and Possessions.

C3.2.1.1. Although the FBI has primary law enforcement responsibility for terrorist incidents inside the United States (including its possessions and territories) and the DoD LECIC has a significant role within departmental areas of jurisdiction, commanders are nevertheless responsible for maintaining law and order on DoD installations and vessels. The Commanders' AT plans should address the use of security forces to isolate, contain and neutralize a terrorist incident within the capability of the commander's resources. The DoD Commanders have the inherent authority and obligation to defend their units and other U.S. units in the vicinity from terrorist incidents wherever they occur. Terrorist incidents involving attacks on DoD personnel, facilities, or assets are unlawful acts, which trigger the need to establish legal responsibility and authority for three separate but related activities:

C3.2.1.1.1. Immediate response, containment, and resolution of an incident.

C3.2.1.1.2. Investigation of an incident for various purposes, to include prosecuting alleged perpetrators.

C3.2.1.1.3. Prosecution of the alleged perpetrators.

C3.2.1.2. Table C3.T1. summarizes the responsibilities of the Department of Defense for response, investigation, and prosecution of all terrorist incidents that may involve DoD personnel, facilities, or assets.

**Table C3.T1. Authority and Jurisdiction in Terrorist Incident Responses**

| Authority and Jurisdiction in Terrorist Incident Responses | | | | | |
|---|---|---|---|---|---|
| Incident Location | Initial Response | Containment of Incident | Incident Resolution | Incident Investigation (Lead Agency) | Prosecution (Lead Agency) |
| DoD installation or vessel within the United States, its territories and possessions | DoD military and/or civilian security forces | Initially DoD Military and/or civilian security forces, with transition to FBI or civilian law enforcement dependent on jurisdiction | DoD Security Organizations, Military Emergency Service Team/ Special Reaction Team or FBI or other appropriate civilian law enforcement dependent on jurisdiction | FBI and DoD Criminal Investigative Task Force (CITF) for military commission crimes | DOJ and DoD Office of Military Commissions for prosecuting military commission pursuant to President's Military Order of November 13, 2001. |
| DoD Personnel Off-Base (not on installation or vessel) within the United States, its territories and possessions | Local law enforcement; FBI (Military forces retain their inherent right to self-defense) | Local law enforcement; FBI | Local law enforcement; FBI | Local law enforcement for state or local law violations; FBI for Federal law violations; and DoD CITF for military commission crimes | Local state's attorney for prosecuting state or local law violations; DOJ for prosecuting Federal law violations; and DoD Office of Military Commissions for prosecuting military commission pursuant to President's Military Order of November 13, 2001. |

| Authority and Jurisdiction in Terrorist Incident Responses | | | | | |
|---|---|---|---|---|---|
| DoD installation or vessel overseas | U.S. military and/or civilian security forces and/or host Government security forces in accordance with SOFA | U.S. military and/or civilian security forces and/or host Government security forces in accordance with SOFA | Host Government security forces supported by U.S. military in accordance with SOFA | Host Government for violation of host nation laws; DOJ for violations of U.S. law; and DoD CITF for military commission crimes | Host Government for prosecuting violation of host laws; DOJ for prosecuting Federal law violations; and DoD Office of Military Commissions for prosecuting military commission pursuant to President's Military Order of November 13, 2001. |
| DoD Personnel Off-Base (not on installation or vessel) overseas | Host Government (Military retain their inherent right of self-defense) | Host Government | Host Government with U.S. assistance on request | Host Government for investigating violation of host laws; DOJ for investigating violations of U.S. law; and DoD CITF for military commission crimes | Host Government for prosecuting violation of host laws; U.S. Attorney for prosecuting violation of U.S. laws; and DoD Office of Military Commissions for prosecuting military commission pursuant to President's Military Order of November 13, 2001. |

C3.2.1.3. In the United States, installation and vessel commanders shall provide initial and immediate response to any incident occurring on military installations or vessels to isolate and contain the incident. The use of force within the United States, its territories and possessions is governed by the DoD use of force policy contained in DoD Directive 5210.56 (reference (m)). In the event of a terrorist incident, the installation or vessel commanders must notify appropriate Federal or State civilian law enforcement authorities as soon as possible. This includes notifying the DoD Criminal Investigative Task Force regarding acts of terrorism and war crimes committed in the United States Central Command area of operations. Primary responsibility for investigating many of the most serious crimes on U.S. Government property shall normally rest with the DOJ.

C3.2.1.4. The Department of Defense may provide support to State and/or Federal law enforcement agencies in response to civil disturbances or terrorist incidents occurring outside DoD installations or vessels. Relevant regulations include DoD Directive 3025.15, DoD Directive 5525.5, and DoD Directive 5525.7 (references (n), (o), and (p)).

C3.2.1.5. DoD installation commanders may request assistance from the FBI in resolving an incident in those circumstances in which the FBI has superior tactical assets. Such assets include regional Special Weapons and Tactics (SWAT) units or the Hostage Rescue Team. In the event that FBI assistance is requested and provided, the FBI shall be the Primary Federal Agency (PFA) for the purpose of concluding the incident. If requested and subject to OSD approval, DoD commanders may provide support to the FBI. Military personnel, however, shall always remain under the command and control of the military chain of command. If military forces are employed during a tactical response to a terrorist incident, the military commander retains command responsibility of those forces. In the event that FBI assistance is requested and provided, the DoD installation commander should immediately expedite a request naming the FBI as the PFA. Command relationships should be addressed as part of the request for assistance.

C3.2.1.6. Attacks on DoD personnel or assets within the United States, its territories and possessions outside DoD facilities or vessels are to be contained and resolved by state and federal law enforcement. Limited exceptions to this rule may occur when incidents involve DoD units outside a DoD installation or vessel and immediate action is necessary to protect DoD personnel and property from immediate threat of injury before local law enforcement or the FBI can respond.

C3.2.2. Commander's Responsibilities Outside the United States, its Territories and Possessions

C3.2.2.1. For foreign incidents, the installation or vessel commander's responsibilities are the same as for domestic incidents—with the added requirement to notify the cognizant U.S. embassy. DOS notification is made at the geographic Combatant Commander level for incidents on U.S. facilities or vessels outside the United States, its territories and possessions. The commander is responsible to respond and contain the incident as quickly as possible in order to protect DoD personnel and property from immediate threat of injury. The DOS has the primary responsibility for dealing with terrorism involving Americans abroad. The installation or vessel commander should also implement any provisions of the SOFA or other agreements between the United States and the host Government relevant to the incident.

C3.2.2.2. The host Government may provide forces to further contain and resolve the incident in accordance with its obligations under international law, the SOFA and other relevant agreements. If the U.S. Government asserts a prosecutorial interest, such as extradition, the DOJ shall assume lead agency responsibilities for liaison and coordination with host nation law enforcement and prosecutorial agencies.

C3.2.2.3. The inherent right of self-defense, as reflected in the Standing Rules of Engagement, still applies in situations off-base or off-vessel in foreign areas. If U.S. forces are actually under attack, they retain the inherent right to respond with proportionate, necessary force until the threat is neutralized. This is providing that the host nation is unwilling or unable to respond to the threat in sufficient time or with appropriate means. The host Government should take appropriate action to further contain and resolve the incident in accordance with its obligations under international law as well as any applicable SOFA or other international agreement. U.S. military assistance, if any, depends on the applicable SOFA and other international agreements. Such assistance shall be coordinated through the U.S. Embassy. Unless immediate action is necessary to protect DoD personnel and property from immediate threat of injury, no U.S. military assistance may be provided to assist a host Government without direction from the Department of Defense, and in coordination with the DOS. The degree of the involvement of U.S. military forces depend on the following:

C3.2.2.3.1. The incident site.

C3.2.2.3.2. The nature of the incident.

C3.2.2.3.3. The extent of foreign government involvement.

C3.2.2.3.4. The overall threat to U.S. interests and security.

C3.2.2.3.5. The ability of U.S. forces to sustain their capability to perform assigned missions.

C3.2.3. Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)

C3.2.3.1. The 1986 Diplomatic Security Act (reference (q)) directs the Secretary of State (SECSTATE) to assume responsibility for the security of all USG personnel on official duty abroad, except those under the command of a geographic Combatant Commander and their accompanying dependents. SECSTATE discharges these responsibilities through the Chiefs of Mission (CoMs). In December 1997, the Secretary of Defense (SECDEF) and SECSTATE signed the MOU on Security of DoD Elements and Personnel in Foreign Areas (also known as the "Universal MOU"). The MOU is based on the principle of assigning security responsibility to the party—Combatant Commander or CoM—in the "best position" to provide security for DoD elements and personnel. The MOU requires delineation of security responsibilities through country specific MOAs.

C3.2.3.2. Once security responsibility has been agreed upon through the Universal MOU/MOA process, the Chief of Mission (CoM) and/or Combatant Commander (and designated AT Planning and Response Elements) enter into MOA/MOUs with local, State, and/or Federal Agencies (domestic) or Host Nation (foreign). These MOA/MOUs augment the installation's organic capabilities and/or are activated when a situation exceeds the installation's inherent capabilities, fulfilling surge requirements needed to respond to a terrorist incident. Therefore, each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs. These MOA/MOUs must be a coordinated effort between the many AT Planning and Response Elements of the installation.

C3.2.3.3. Installation specific MOA/MOUs and other special arrangements improve the resources and/or forces available to support any AT/FP Plan. These MOA/MOUs may include, but are not limited to, host nation and U.S. military police forces, fire and emergency services, medical, and Federal/State and local agencies, special operations forces, engineers, detection (nuclear, biological, radiological, chemical, and explosive), decontamination or smoke units, and explosive ordnance disposal.

# C4. CHAPTER 4
# AT RISK MANAGEMENT FUNDAMENTALS

## C4.1. INTRODUCTION

In AT, risk is viewed as the probability and severity of loss, linked to terrorist threats. Risk management assists AT decision-makers in reducing or offsetting terrorist attack effects. The risk management process is used by Commanders to identify, assess, and control risks arising from operational factors and helps in making decisions that balance risk cost with mission benefits. Commanders can use the risk management process information to determine which assets require the most protection and where future expenditure is required to minimize risk of attack, or lessen the severity of the outcome of such an attack. Risk management does not replace sound decision making, nor does it remove risk altogether, or support a zero defect mindset.

## C4.2. OVERVIEW

It is beyond the scope of this Handbook to provide a consolidated multi-service process addressing risk management background, principles, and application procedures. Users needing in-depth risk management information should consult the "Risk Management Multi-service Tactics, Techniques, and Procedures for Risk Management" (reference (r)), and/or applicable Service/Combatant Command/Agency guidance. This Handbook does provide a better general understanding of the risk management concept and process, as it relates to the AT mission. Included in the AT risk management process chapters are specific procedures to help any commander or ATO reduce or offset AT risks in order to enhance operational capabilities and mission accomplishment, with minimal acceptable loss.

## C4.3. AT RISK MANAGEMENT PROCESSES.

C4.3.1. The AT risk management process generally follows multi-service tactics, techniques, and procedures for tactical level risk management in the planning and execution of operations. The process has two levels of application: deliberate and crisis action. Available time to complete the process is the basic factor that shall determine the level of application. Deliberate AT risk management allows the application of the complete process when time is not critical. Crisis AT risk management is conducted immediately previous to or after a terrorist attack, by doing a mental or verbal review of the situation using the basic AT risk management process. Key steps of the risk management process include:

C4.3.1.1. Identifying threats.

C4.3.1.2. Assessing threats to determine threat capabilities and courses of action.

C4.3.1.3. Developing controls and making risk decisions.

C4.3.1.4. Implementing controls.

C4.3.1.5. Supervising and reviewing.

C4.3.2. In addition to those steps, the AT risk management process adds steps to determine criticality and vulnerability. These steps systematically identify and evaluate assets in term of various factors such as the target's mission, significance, and vulnerability. The criticality assessment can be conducted before, after, or concurrent to assessing the threat. The VA shall be conducted after assessing the threat and the criticality to determine what critical assets are most vulnerable. All three elements together shall be used to estimate AT risk.

C4.4. AT RISK MANAGEMENT ELEMENTS.

C4.4.1. Threat Assessment (TA). The TA should identify the terrorist threat. For each group that may be a threat, the assessment provides information on the group's intent, capability, and history as well as any specific targeting information that may be available. The TA process is further discussed in Chapter 5.

C4.4.2. Criticality Assessment. This is done to determine which assets need to be protected. The criticality assessment determines the importance of each asset, the effect of a terrorist attack on the assets, and the recoverability of the asset from attack. The criticality assessment process is further discussed in Chapter 6.

C4.4.3. VA. The VA evaluates and determines the vulnerability to a terrorist attack of an installation, unit, exercise, port, ship, residence, facility, or other site. It assesses each asset and identifies shortfalls or weaknesses that make the asset vulnerable, determines if existing countermeasures are effective, and prioritizes these vulnerabilities. The VA process is further discussed in Chapter 7.

C4.4.4. Risk Assessment. The Risk Assessment combines the criticality, threat, and vulnerability rating given to each asset and unwanted event. It uses the theory that in order for there to be risk, each one of the elements (Criticality, Threat, and Vulnerability) must be present therefore Risk = Criticality x Threat x Vulnerability. Risk is based on the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is derived by combining the

relative impact of any loss or damage to an asset (Criticality) with the relative probability of an unwanted event (Threat x Vulnerability).

C4.5. MITIGATION OPTIONS.

C4.5.1. To complete the risk analysis, mitigation options must be identified in order to develop controls, make decisions, implement controls, supervise and review. Developing controls and executing the remaining elements, are essential follow-through actions of the AT risk management process. Commanders weigh risk versus benefits and make and/or implement decisions to eliminate unacceptable levels of risk. After identifying and implementing additional countermeasures or mitigation efforts, it is prudent to recalculate the risk.

C4.5.2. The cost and effectiveness of each countermeasure should be identified so that the decision-maker can see the cost and benefit of each option. Acceptable risks should be communicated to subordinates. Commanders and all individuals involved in the AT risk management process then evaluate the effectiveness of applied controls and capture lessons learned.

C4.6. AT RISK MANAGEMENT PROCESS APPLICATION GUIDELINES

C4.6.1. Apply the process in sequence. It is not possible to prioritize risk control efforts properly until threats have been identified and assessed, and the criticality of assets being determined.

C4.6.2. Maintain balance in the process. Available time should be allocated to ensure the process is completed. The objective is to assess the time and resources available for AT risk management activities and allocate them to actions in a manner most likely to produce the best overall result.

C4.6.3. Apply the process as a cycle. Supervising and reviewing the countermeasures or mitigation efforts might identify additional threats or prove the controls ineffective. The entire AT risk management process should be repeated and applied to the new threat.

C4.7. RELATIONSHIP AND INTEGRATION OF AT RISK MANAGEMENT TO OVERALL RISK MANAGEMENT.

C4.7.1. Successful risk management is underwritten by the chain of command. A facility that has embedded the risk management process into facility operations, culture, organization, systems, and individual behavior needs to input the AT risk management process into the overall mission risk management process. The ATO should work within the organization to ensure the

commander is properly advised of residual AT threats and risks that remain after implementing all available controls.

C4.7.2. When more than one threat is identified (terrorists, enemy, environment, diseases, etc.), the Overall Residual Risk must be determined. The residual risk of each threat shall have different levels depending on the assessed threat probability and the severity of the outcome if it were to happen.

C4.7.3. Overall residual risk should be determined based on the threat having the greatest residual risk. Determining overall mission risk by averaging the risks of all threats is incorrect. If the residual terrorist threat is high, the overall residual risk is high no matter how many moderate or low risk threats are present in the other categories.

C4.7.4. The Chief of Staff, Executive Officer, or Deputy Director is usually assigned responsibility for supervising the integration of risk management across the spectrum. As a means of assessing and monitoring threats, commanders may establish an ATWG or Force Protection Working Group (FPWG). The purpose of the ATWG/FPWG is to review threats, identify vulnerabilities, recommend countermeasures, recommend FPCONs and positioning of response forces, review tasks to components, monitor corrective actions, and direct special studies (force protection assessment teams). In the absence of an ATWG/FPWG, the Chief of Staff should at a minimum, integrate personnel and resources from the following areas/staff sections to facilitate the AT risk management process.

C4.7.4.1. Personnel. Obtain personnel deployment flows; estimate casualty risks, project casualty and replacement flows; determine controls for personnel related activities; and estimate risks of employed local civilian labor.

C4.7.4.2. Intelligence. Monitor and report international threats; in conjunction with law enforcement, develop regional and/or local TA s; and determine risk of loss of intelligence assets.

C4.7.4.3. Operations. Develop overall risk assessment; develop Rules of Engagement (ROE) and supplements; and prioritize controls and levels of response.

C4.7.4.4. Logistics. Recommend technology acquisition and procurement strategies; assesses the risk of critical supplies; determine storage site vulnerabilities and controls; and determine munitions storage site vulnerabilities, safety requirements and controls.

C4.7.4.5. Plans. Integrate functional and combat control measures; identify vulnerabilities during mission analysis and war-gaming; and plan controls to mitigate risk.

C4.7.4.6. Communications. Assess risk to information and services systems; and develop controls to counter their threats.

C4.7.4.7. Resources/Comptroller. Assess AT requirements for resource dollars and coordinate budget issues regarding AT issues, acquisition, and procurement.

C4.7.4.8. Special Staffs. Address AT risk management with the various special staff offices (Medical, Legal, Public Affairs Office (PAO), and Safety) as required. In addition to the above, DCIO elements and security organizations should be consulted for their role in monitoring and reporting domestic threats to Defense resources and activities, and assisting in the development of local threat assessments and a common operational picture.

# C5. CHAPTER 5
# AT THREAT ASSESSMENT

## C5.1. INTRODUCTION AND OVERVIEW

The AT Risk Management process begins with an assessment of the terrorist threat to DoD personnel and facilities. The AT Threat Assessment is used to identify the terrorist threats posed to DoD assets and/or the threats that could be encountered in executing a mission. This Chapter includes an overview of organizations that provide threat information or analysis to the DoD Components. It then describes the analytical approach for assessing terrorist threats, the DoD Threat Methodology, and concludes with a description of how the terrorist threat is assessed at installation or unit level.

## C5.2. THREAT INFORMATION AND ANALYSIS ORGANIZATIONS

The threat of terrorist targeting of U.S. Government personnel, facilities, assets, and interests has resulted in the development of an intelligence structure to collect, analyze, and disseminate information about terrorist threats.

### C5.2.1. National Level

C5.2.1.1. The Director, Central Intelligence's forum for interagency coordination and cooperation on counterterrorism is the Community Counterterrorism Board, Interagency Intelligence Committee on Terrorism (IICT). The IICT consists of seven subcommittees with representation from 45 U.S. Government agencies, including intelligence, law enforcement, regulatory, and defense agency representatives. These organizations include: the CIA, the DOJ, the FBI, the DOS, Defense Intelligence Agency (DIA), Health and Human Services, the Center for Disease Control, the Department of Homeland Security, and the National Security Agency (NSA). The Services are represented by the Army Counterintelligence Center (ACIC), Naval Criminal Investigative Service (NCIS), Headquarters U.S. Marine Corps Counterintelligence/Human Intelligence (HUMINT) Branch, and U.S. Air Force Office of Special Investigations (AFOSI).

### C5.2.2. DoD Level

C5.2.2.1. The Secretary of Defense has assigned to the DIA responsibility for establishing and maintaining an international all-source terrorism intelligence fusion center, the Joint Intelligence Task Force – Combating Terrorism (JITF-CT), DIA. The JITF-CT provides information and analytical resources to support the Combatant Commands and the Services.

C5.2.2.2. The DIA provides a wide range of terrorism intelligence for DoD Components, to include Indications and Warning (I&W), current intelligence, assessments, in-depth analysis, and the maintenance of a counterterrorism database.

C5.2.3. Combatant Commands

C5.2.3.1. All Combatant Commands have their own supporting joint intelligence centers and intelligence organizations. Each Combatant Commander, through his or her J-2 staff, draws upon information and analysis resources of the DIA, the Services and other national agency representatives, to include all U.S. Embassies in his or her area of responsibility (AOR). In addition, the Combatant Commands collect, process, analyze and disseminate terrorism-related intelligence using organic resources. The Combatant Commands all have their own watch centers, which provide indications and warning support. The purpose is two-fold:

C5.2.3.1.1. To assist the Combatant Commander in providing for the security and protection of forces under his or her control.

C5.2.3.1.2. To ensure the flow of information passing through Service lines of communication within the area of the Combatant Commander responsibility is also brought to the attention of the Combatant Commander and his or her staff and disseminated within the Command as appropriate.

C5.2.4. Military Departments Role

C5.2.4.1. 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." To accomplish this task, each Military Department Secretary appoints a lead agency to monitor foreign intelligence and counterintelligence activities focusing on terrorist groups and terrorist acts as follows:

C5.2.4.1.1. The Army Terrorist Operations and Intelligence Center (ATOIC);

C5.2.4.1.2. The Navy Multiple Threat Alert Center (NMTAC);

C5.2.4.1.3. The AFOSI; and

C5.2.4.1.4. The Marine Corps Intelligence Activity (MCIA)

C5.2.4.2. To accomplish this mission, the Service lead agency establishes, as needed, field intelligence and law enforcement offices on an area basis to collect and disseminate information to Combatant Commanders. Each Service:

C5.2.4.2.1. Coordinates with appropriate U.S. and host nation agencies.

C5.2.4.2.2. Provides overall direction and coordination of the Service CI effort.

C5.2.4.2.3. Operates a 24-hour operations center to receive and disseminate worldwide terrorist threat information to and from the Combatant Command's J2, applicable Service staff elements, subordinate commands, and national agencies.

C5.2.4.2.4. Provides commanders with information on terrorist threats concerning their personnel, facilities, and operations.

C5.2.4.2.5. Assists the FBI or host nation authorities with intelligence matters after terrorism incidents.

C5.2.4.2.6. Provides terrorist threat information briefings.

C5.2.4.2.7. Performs as the Service's liaison representative to Federal, State, and local agencies, as well as host nation agencies to exchange information on terrorists.

C5.2.4.2.8. Provides periodic international terrorism products and other threat data to supported commanders. On request, provides current intelligence data on terrorist groups and disseminates time sensitive and specific threat warnings to appropriate commands.

C5.2.5. Field Level Activities

C5.2.5.1. The DIA, the Counterintelligence Field Activity, and the Services possess information collection assets in the field that can be directed to collect information on terrorist threats to DoD personnel, facilities, and assets. Service/OSD Investigative Agencies include criminal investigative services such as USACIDC, NCIS, AFOSI, and the DCIS. Each collects and disseminates foreign and, to very limited extent, domestic terrorist-related information to supported installation and activity commanders. As appropriate, criminal investigative elements also conduct liaison with local military/security police and civilian law enforcement agencies.

C5.2.5.2. Intelligence/Counterintelligence Staff elements of DoD agencies and commanders at all echelons execute the following responsibilities:

C5.2.5.2.1. Report promptly all known or suspected terrorist incidents, activities, and early warnings of terrorist attack to supported and supporting units/activities, local intelligence field offices, Combatant Commands, and appropriate headquarters.

C5.2.5.2.2. Initiate and maintain liaison with the security forces or provost marshal offices, local military criminal investigative offices, local intelligence field offices, security offices, host nation agencies and other organizations, elements, and individuals as required.

C5.2.5.2.3. Develop and present terrorist threat awareness briefings to all personnel within their commands in cooperation with the local intelligence field offices.

C5.2.5.2.4. Report all actual or suspected terrorist incidents or activities to their immediate commander and/or supported activities, and DIA through established reporting channels.

C5.2.5.3. Law Enforcement Staff Level Elements. Law enforcement elements of DoD agencies and military commands carry out the following responsibilities:

C5.2.5.3.1. Initiate and maintain liaison with local intelligence field offices and military criminal investigative organizations.

C5.2.5.3.2. Investigate criminal activities committed within their jurisdiction to determine whether or not such activities may constitute a terrorist threat to DoD personnel, facilities, materiel, or other U.S. interests.

C5.2.5.3.3. Report all actual or suspected terrorist incidents or activities to their immediate commander and/or supported activities through established reporting channels.

C5.2.5.3.4. Maintain liaison with Federal, host nation, and local law enforcement agencies; and civil and military combating terrorism agencies as appropriate.

C5.2.5.3.5. Gather and report information on domestic activities that pose a threat to Defense resources, facilities, and activities.

C5.2.5.4. Installation, Facility, Activity, or Unit Security Officer. The foundation of the threat reporting function demanded by the DoD AT Program rests on the shoulders of installation, facility, activity, or unit security officers. These individuals may not be part of the military intelligence community in a formal sense; however, their overall security and force protection responsibilities place them in positions through which quantities of information of potential interest or concern to the intelligence and law enforcement communities pass on a recurring basis. These security officers:

C5.2.5.4.1. Report all known or suspected terrorist incidents or activities to their immediate commander, supporting security or military police office, other supported activities, local intelligence field office, and local military criminal investigation office.

C5.2.5.4.2. Conduct regular liaison visits with the supporting security or military police office, intelligence field office, and local criminal investigation office.

C5.2.5.4.3. Assist in providing terrorist threat awareness training and briefings to all personnel and family members as required by local situations.

## C5.3. TERRORIST THREAT ASSESSMENT

C5.3.1. The threat assessment system is vital to developing and disseminating terrorism warnings. Specific warning information—time, date, place, those involved and method of attack—is rarely voluntarily provided by terrorists. Careful threat analysis is required to detect and correctly evaluate pre-incident indicators of a terrorist attack, so timely warning messages can be issued.

C5.3.2. Threat analysis provides the intelligence officer with information upon which to base warnings.

C5.3.3. Threat information for AT programs is diverse and includes foreign intelligence, open source materials, domestic criminal information, and information from federal, state, and local governments.

C5.3.3.1. Open source and publicly available information may be collected, retained, and disseminated as prescribed in references E.O. 12333, DoD 5240.1-R, and DoD Directive 5200.27 (reference (s) through (u)). Organizations engaging in these activities must ensure they are properly authorized to do so. Examples of open source material include news media (print and broadcast), press releases, political tracts, handbills, posters, and leaflets, and the World Wide Web (Internet):

C5.3.3.1.1. News media may provide good information on terrorism. News organizations often are the first to report many major terrorist incidents and include in-depth reports on terrorist individuals or groups. Such reports can provide analysts with insights into terrorist group goals and objectives, the motivation of individual members of terrorist organizations, modes of recruitment, training and training methods, and tactics of attack. Terrorist groups frequently use the media to promote their cause.

C5.3.3.1.2. Scholarly publications.

C5.3.3.1.3. Unclassified U.S. and foreign government publications.

C5.3.3.1.4. Press releases.

C5.3.3.1.5. Political tracts, handbills, posters, flyers, and leaflets often distributed by organizations committing, supporting, or opposing terrorist actions may reveal their objectives, tactics, and possible targets. Such information is often placed into the public domain as part of a campaign of terror.

C5.3.3.1.6. The worldwide web provides terrorists an outlet to spread propaganda, recruit new members and aid in fundraising. In addition, the web provides a wealth of information to include: training and training methods, weapons, and weapons usage. Only specially trained counterintelligence personnel should access these sites. Terrorist organizations have shown increased sophistication in the area of information warfare and casual visits to their sites may inadvertently provide them intelligence information on who may be interested in their activities and/or expose the untrained visitor to a computer hacker attack.

C5.3.3.2. Commercial data services may offer timely information about international or military affairs that often include information regarding terrorist incidents. Such data services often rely on foreign news media. Some data services maintain their own network of sources. Information services are provided on subscription or fee-for-service basis.

C5.3.3.3. The DCIOs, military and civil law enforcement agencies collect criminal information. Since terrorist acts are criminal acts, criminal information is a lucrative source for terrorist intelligence. Local military criminal investigative offices maintain current information in accordance with DoD regulations governing retention of criminal information. Such material may assist managers and military commanders in the assessment of the local terrorist threat.

C5.3.3.4. Government information refers to materials collected, analyzed, and disseminated under official auspices. It includes, but is not limited to, scientific and technical reports, political and economic reports, crime and terrorism statistics, policy statements, legislation, and official correspondence.

C5.3.3.4.1. Some government information may be open source, available to all persons who either request or purchase it.

C5.3.3.4.2. Government information may also be restricted or have limited distribution only within government agencies. Such information might include post-conviction court records, export/import license applications, immigration records, or financial securities registration information not released to the public.

C5.3.3.4.3. Government information also includes data and analyses derived from intelligence classified sources. Exchanges with local government agencies through for example, "cooperative arrangements," can also augment regional information.

C5.3.3.5. Local information can come from individual service members, civil servants, family members, and individuals with regional knowledge such as college faculty or cultural organizations. Local crime or neighborhood watch programs can also be valuable sources of information and can serve as a means to keep individuals informed in dispersed and remote areas.

C5.3.3.5.1. Local information is often of critical importance as it is collected and passed through either law enforcement and/or intelligence channels to the national intelligence organizations. It is frequently invaluable to analysts confirming news media or other open source accounts of terrorist activities. It can provide early warning of potential terrorist activities, allowing law enforcement and combating terrorism measures to be initiated in a timely manner to thwart or minimize the effects of a terrorist attack.

C5.3.3.5.2. A critical element of local information is obtained from individual service members, their families, and civilian employees at DoD facilities who report any suspicious activity they observe. It is critical that all these personnel receive frequent, thorough training regarding the recognition and reporting of suspicious activity. Such reports, even those that may appear frivolous, must receive immediate investigation by law enforcement and counterintelligence personnel.

C5.3.4. Access to Intelligence

C5.3.4.1. Terrorist threat information flows back and forth in the field, and among the Combatant Commanders, the Services, and the DIA. At each level, it is integrated, fused, and assessed in accordance with regulations and DoD Directives governing the security and dissemination of intelligence and law enforcement information. Terrorist threat information and analytical products are also disseminated from the national, DoD, Service, Agency, and Combatant Commander levels to all echelons of command and individual Defense Agency activities as appropriate.

C5.3.4.2. The Combatant Commanders, through their Intelligence Directorates and Counterintelligence Staff Officer, and in consultation with the DIA, embassies' staffs, country team and applicable host nation authorities, assess intelligence specific to their areas of operation and issue intelligence reports, advisories and counter intelligence reports to the units within the

Combatant Commander's control or AOR. This intelligence dissemination network is the backbone for communicating intelligence information throughout the region and to the national level.

C5.4. TERRORISM THREAT LEVEL ASSESSMENT METHODOLOGY

C5.4.1. This DoD methodology assesses the terrorist threat to DoD personnel, facilities, and interests. The methodology is used by all DoD Components to determine the level of terrorist activity in a specific country, region, or locale. This methodology does not address threats from conventional forms (i.e. hostile conventional armed forces) and/or the criminal threat (if unrelated to known or suspected terrorist activity).

C5.4.1.1. Threat levels are assigned based on available intelligence and an analytical assessment.

C5.4.1.2. Threat levels describe an environment, not a probability of attack.

C5.4.1.3. Terrorist threat levels do not allocate protective resources.

C5.4.1.4. Issuance of a Terrorist Threat Level judgment is not, in and of itself, a formal warning vehicle.

C5.4.2. Threat analysis is the process of compiling and examining all available information to develop intelligence indicators of possible terrorist activities.

C5.4.3. The Department of Defense has identified several factors to identify the collection and analysis of information from all sources concerning terrorist threat(s). These factors are used in making terrorist threat analyses on a country-by-country basis.

C5.4.4. Methodology Factors

C5.4.4.1. Operational Capability is the acquired, assessed, or demonstrated level of operational capability to conduct terrorist attacks.

C5.4.4.1.1. Group Tactics focuses on the attack methods used by the group. What type of attack has the group conducted in the past? Has the group conducted large or small-scale bombings, kidnappings, assassinations, drive-by shootings, or other assaults? Has there been any indication the group has any new capabilities? Has the group been notably unsuccessful in any types of attacks?

C5.4.4.1.2. Mass Casualty Capability/Willingness. Does the group have the capability and willingness to conduct mass casualty attacks? Has the group conducted such attacks in the past? Has the group shown an interest in CBRNE material?

C5.4.4.1.3. Targeting. Does the group conduct attacks intended to maximize casualties, i.e., conducting an attack at peak business times, or placing secondary Improvised Explosive Devices (IEDs) to target first responders? Does the group attempt to limit damage to property only, by placing IEDs after business hours or in remote locations?

C5.4.4.1.4. State Sponsorship. Does the group have state sponsorship? Who is the state sponsor? What type of intelligence/logistics/training/funding is provided? Is support from one or more Governments? If so, which ones?

C5.4.4.1.5. Group's Operating Area. Is the group indigenous, regional, or transnational? Can indigenous groups operate regionally or transnationally?

C5.4.4.1.6. High Technology Access. Does the group have access to high technology? Does the group use computers? If yes, to what extent? Can the group conduct sophisticated technical surveillance or employ advanced IEDs? What type of equipment is used? Where did the group get the equipment? Who trained the group?

C5.4.4.1.7. Method of Operation. What is the group's method of operation? A group shall likely continue to use techniques and tactics that have been successful in the past.

C5.4.4.1.8. Professionalism. What is the group's overall professionalism? Has the group consistently carried out successful sophisticated attacks? Has the group demonstrated a high or low degree of tradecraft?

C5.4.4.1.9. Different Tactics Equate to Different Threats. Different tactics result in different degrees of threat. A group that conducts property attacks presents less of a threat than one that has conducted assassinations or attacks with large vehicle borne IEDs.

C5.4.4.2. Intentions are the stated and/or the actual history of attacking U.S. interests.

C5.4.4.2.1. Recent Attacks. Has the group conducted a recent terrorist attack? Type of attack? Weapons type? Were any pre-incident indicators noted? Was outside support used? Did the group claim the attack?

C5.4.4.2.2. Anti-U.S. Ideology. Does the group have an anti-U.S. ideology? Is the ideology stated publicly? What is the group's main opposing points with the U.S.? What trigger events could entice the group to act?

C5.4.4.2.3. Anti-Host Nation Ideology. Does the group have an anti-host nation ideology? Does the group consider U.S. aid/support a hindrance to its goals? At what point would the group consider attacking U.S. interests due to this support?

C5.4.4.2.4. Attacks in Other Countries. Has the group conducted terrorist attacks in other countries? Where? What type of attack? What type of support network was in place?

C5.4.4.2.5. Response to Current International Events. Has the group ever responded to an international event with a terrorist attack? What was the event? What type of response? Has the group ever publicly denounced an international event involving the U.S.? Did they threaten U.S. interests?

C5.4.4.3. Activity. A terrorist group's activity in a country may not always be related to operational planning or present a threat to U.S./host nation interests. Many groups use countries as support bases and may not want to jeopardize their status by conducting a terrorist act there. Analysts must determine the group's activity by examining influencing elements and keeping in mind that the situation is always fluid and subject to change. Some of the key elements in evaluating activity are:

C5.4.4.3.1. Presence. Is a group present but inactive?

C5.4.4.3.2. Fund-raising and Safe Haven. Does the group use the country for fund raising? What type of fund raising? How much money is generated? What is its intended use? Is any of the money funneled to other locations or groups? Does the group use a country as a safe haven?

C5.4.4.3.3. Suspected Surveillance, Threats, and Suspicious Incidents. Has the group been known to conduct surveillance? Is the group proficient at surveillance? What does the group do with the surveillance information? Has the group threatened DoD/U.S. interests? How does the group conduct surveillance? Have there been any suspicious events that could be linked to the group?

C5.4.4.3.4. Changes in Philosophy Impacting Targeting. Has the group shown any signs of changing philosophies? Does the philosophical change include targets? Is the Department of Defense affected?

C5.4.4.3.5. Level of Involvement with External Cells. How does the local leadership interact with external leadership? How much contact is normal? Does the group have connections with other cells? Do the cells train together? Do they share intelligence?

C5.4.4.3.6. Key Operative Movement. Has there been any noted movement of key operatives? If so, from where to where? Was the movement covert? Was there any reaction from other cells? What was the purpose of movement? Were code words used?

C5.4.4.3.7. Contingency Planning. Has any planning been noted? Who/what are the targets? How were past plans executed? Who conducted the planning? Was outside help used/requested? Did any attacks occur after planning was noted? How much time elapsed?

C5.4.4.3.8. Disruptions by U.S. or Host Nation Security Elements. Have U.S. or host nation security forces disrupted any of the group's activities? If host nation only, does the group perceive U.S. involvement? What caused the disruption? What was uncovered by security? How does it affect the group's operational capability in country?

C5.4.4.3.9. Identification of Weapons Caches. Have weapons caches been uncovered? What types of weapons? Are the weapons consistent with the group's past weapons usage? Who supplied the weapons?

C5.4.4.3.10. Cell Activity (Operational or Support). What type of activity does the group mainly conduct in country? Operational? Support? Size of cells? Number of cells?

C5.4.4.3.11. Credible Indications of Targeting U.S. Assets. Is there any indication the group is targeting U.S. assets? At what stage of the targeting process was the plan uncovered? Timing? Specific target? Location?

C5.4.4.3.12. Assessment of Intelligence Reporting Regarding Terrorist Activity. What type of intelligence is being reported (Signal Intelligence (SIGINT), HUMINT, etc)? Source of reporting? Reliability? Access?

C5.4.4.4. Operating Environment. How the overall environment, to include political and security considerations, influences a terrorist group's ability and motivation to conduct an attack. Influencing factors include:

C5.4.4.4.1. DoD Presence. What is the DoD presence in the country? Size? Location? Duration of stay? What are DoD personnel doing in country (training, support, security, etc.)? What is the terrorist perception of DoD significance? How politically sensitive is the DoD presence? What could entice the terrorists to attack DoD interests?

C5.4.4.4.2. External Influencing Factors. Is the host country at war? Could this influence a terrorist group to attack? Is there active insurrection? Is the terrorist group involved in the insurrection?

C5.4.4.4.3. Host Nation Security and Level of Cooperation. Can host nation security (to include national law enforcement, paramilitary and military institutions) maintain social order? How well are security forces trained to respond to terrorist incidents? Type of equipment available for security forces? How are forces dispersed around the country? Does host nation cooperate with U.S. authorities? Does host nation share information?

C5.4.4.4.4. Political Influences Affecting Motivation to Attack. What political influences are affecting the group's motivation to attack? Has host nation cracked down after previous terrorist acts?

C5.5. TERRORIST THREAT LEVEL

C5.5.1. The Department of Defense uses four threat levels to define the degree to which the environment is conducive to conducting terrorist operations in a specific country, region or locale by using the factors and elements described above. The four threat levels are Negligible, Low, Medium, High, and Critical.

C5.5.1.1. High. Anti-U.S. terrorists are operationally active and use large casualty producing attacks as their preferred method of operation. There is a substantial DoD presence and the Operating Environment favors the terrorist.

C5.5.1.2. Significant. Anti-U.S. terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method but has limited operational activity. The Operating Environment is neutral.

C5.5.1.3. Moderate. Terrorists are present but there are no indications of anti-U.S. activity. The Operating Environment favors the Host Nation/U.S.

C5.5.1.4. Low. No group is detected or the group activity is non-threatening.

C5.5.2. A Terrorism Warning is issued when credible specific targeting information is obtained and is formally linked to the methodology (see section C5.8.).

C5.5.3. Warning Report. A report issued by the DIA when a terrorist group is operationally active and U.S. interests are specifically targeted. A warning report may be issued at any threat level (see section C5.8.).

C5.6. CHANGES IN TERRORIST THREAT LEVEL DECLARATIONS

C5.6.1. Analysis of terrorism is an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to DoD-affiliated personnel, facilities, and assets begin anew with each analysis. No formal escalation ladder of terrorist threat level exists. Terrorist threat level designations for each country are applied on the basis of current information analysis.

C5.6.2. The DIA sets the DoD Terrorism Threat Level in a particular country. The Geographic Combatant Commanders can also set Terrorism Threat Levels for specific personnel, family members, units, and installations within their AOR, using the definitions established by the DIA. Terrorist Threat Level designations can change without passing through any intermediate steps. A new terrorist group could initiate a series of attacks on DoD personnel or facilities, which could cause a threat level to rise several levels or initiate a Warning Report.

C5.6.3. Terrorism Threat Levels should not be confused with FPCONs. A FPCON is a security posture promulgated by the commander in consideration of a variety of factors (e.g. a terrorism threat assessment, terrorism threat levels, etc.). Terrorism Threat Levels should also not be confused with the Threat Conditions associated with the National Homeland Security Advisory System.

C5.7. THREAT WARNINGS

C5.7.1. Terrorist threat warnings for the Department of Defense use two mechanisms: Community Alerts/Advisories/Assessments and Defense Terrorism Warning Reports. The Intelligence community system issues coordinated Terrorist Threat Alerts, Advisories, and Assessments. The DIA is a member of the national intelligence community along with the FBI, the CIA, the NSA, the Department of Energy, the Department of Treasury, the Department of Homeland Security, and the Department of State. The Interagency Intelligence Committee on Counterterrorism is authorized to provide national-level terrorism warnings to U.S. Government organizations and customers. The Department of Homeland Security is responsible for disseminating terrorist threat warnings for attacks in the homeland. DIA is charged with assessing and disseminating terrorism threat warnings concerning DoD personnel and facilities, both domestically and overseas, to DoD personnel.

C5.7.2. The DoD Defense Indications and Warning System (DIWS) comprises a second, independent system in which DoD members at any level may initiate unilateral threat warnings. These are termed Defense Terrorism Warning Reports. Warnings within the DoD system generally stay within the system and are primarily for use by the DoD Components. DoD Terrorism Warning Reports are active for a maximum 30-day period with one 30-day extension authorized.

C5.7.3. Basic Warning Report Procedures within the Department of Defense

C5.7.3.1. DIWS Terrorist Threat Warning Reports may be prepared and issued by any member of the DIWS system. DIA is required to propose a National Intelligence Community Alert or Advisory prior to issuing a unilateral DIWS Terrorism Warning Report.

C5.7.3.2. Individual DoD Components also have the right to independently notify their members of impending threats. 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 its 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 must inform DIA of its action.

C5.7.3.3. Warnings are issued when specificity of targeting and timing exist or when analysts have determined that sufficient information indicates that U.S. personnel, facilities, or interests, particularly those of the Department of Defense, are being targeted for attack. Warnings need not be country-specific. A warning may cover an entire region or the world. The key to a warning is recognition that the pre-incident indicators for an attack are present.

C5.7.3.4. DIWS Terrorism Warning Reports are specific products. When issued, they perform a number of functions. They 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—not just downward. Warnings of impending terrorist activity are likely to have national implications and shall be provided routinely to decision-makers at the policy level of the U.S. Government.

C5.7.4. No "Double Standard". Following the terrorist bombing of Pan Am flight 103 over Lockerbie, Scotland, on December 21, 1988, the U.S. Government adopted a policy of "No Double Standard" (reference (v)). No terrorist threat warning shall be issued solely to U.S. Government consumers 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 only to government targets. The DOS, overseas, is the sole approving authority for releasing terrorist threat information to the public

## C5.8. INSTALLATION LEVEL AT THREAT ASSESSMENT REQUIREMENTS AND ACTIVITIES

C5.8.1. Commanders down to the installation or tenant level task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information. When organic intelligence/counterintelligence/law enforcement assets are not available, commanders should request support from higher authority. The full range of intelligence, counterintelligence, and law enforcement capabilities shall be utilized in support of distinct and separate threat assessment requirements: annual threat assessments and ongoing assessment of the local threat.

C5.8.2. Annual Threat Assessment. Installation Commanders shall, at least annually, prepare a terrorism threat assessment for those personnel and assets for which they have AT responsibilities. Whereas DoD Threat Methodology focuses on the degree of activity of known terrorist groups, the annual threat assessment seeks to identify the full range of feasible terrorist capabilities (weapons, tactics, techniques, and methods of attack) that could reasonably be used against the installation or its personnel. Even in the absence of a current known threat group, an assessment is a necessary input to the required annual VA and for planning physical and procedural countermeasures. Annual threat assessments should include all likely or feasible WMD including CBRNE threats.

C5.8.3. Threat Matrix. Preparation of the annual threat assessment requires careful analysis of known local threats, together with estimates of relevant national and transnational threat capabilities. Locally derived, open-source information regarding the availability of weapons and component materials in the area is also necessary in developing the range of threats. Threat analysts preparing the assessment should differentiate threats likely to be used inside the perimeter from those more likely to be used outside the perimeter to aid in the VA and development of countermeasures. The Threat Matrix unambiguously establishes the range of specific threat capabilities that shall be used to analyze vulnerabilities and plan countermeasures.

The Threat Matrix is a planning tool which ensures that security and procedural countermeasures are economically designed to counter specific threats or mitigate specific vulnerabilities, and that the risk remaining is well understood by Commanders making risk acceptance decisions (see table C5.T1.).

**Table C5.T1. Assessing Terrorist Threat Capability/ Threat Priority**

| Threat Capability | Weapon | Delivery Method | Threat Probability (Highest # is most probable) | Threat Severity (Highest # is most severe) | Threat Priority (Probability x Severity) | Threat Priority Inside Perimeter ** | Threat Priority Outside Perimeter ** |
|---|---|---|---|---|---|---|---|
| Vehicle Bomb | 220 lbs * | Vehicle (motorcycle, car, truck, boat, plane) | 13 | 6 | 78 | 1 | 2 |
| | 1000 lbs | | 12 | 7 | 84 | NA | 1 |
| | 20,000 lbs | | 4 | 12 | 48 | NA | 4 |
| Mail Bomb | 2 lbs | Package | 10 | 2 | 20 | 8 | NA |
| Sniper | 7.62 mm/ 308 Cal. | Sniper | 11 | 1 | 11 | 9 | 10 |
| Standoff Weapons | Mortar | Hasty Attack | 9 | 5 | 45 | 4 | NA |
| | RPG | Hasty Attack | 8 | 4 | 32 | 6 | 8 |
| MANPAD | SA7, SA16 | Attack against Aircraft in arrival/ departure footprint | 5 | 9 | 45 | NA | 6 |
| Pier Side Ship Ship | Surface Bomb | Boat | 7 | 10 | 70 | 2 | 3 |
| | Sub-surface Bomb | Divers | 6 | 8 | 48 | 3 | 4 |
| WMD | Anthrax | Letter | 1 | 3 | 3 | 10 | NA |
| | Nerve Agent/ Toxic Industrial Chemical | Dispersed up wind of Installation | 2 | 13 | 26 | 7 | 9 |
| | Chem/Bio Poison | Food/Water | 3 | 11 | 33 | 5 | 7 |

Example matrix is used to assess threat capabilities and determine which threats to guard against in priority. Describes threats at a notional installation that for illustration purposes has both a pier and airfield.

* Assumption that a 220 pound bomb is largest that could be concealed from security forces controlling access and transported inside the perimeter of an installation.

**Lowest number is highest priority threat inside and outside the perimeter.

C5.8.4. Both installation and unit commanders shall assess the terrorist threat for probability and severity of occurrence. Probability is the estimate of the likelihood that a threat shall cause an impact on the mission or a hazard to the installation. Severity is an estimate of the threat in terms of the degree of injury, property damage or other mission-impairing factors. By combining estimates of severity and probability, an assessment of risk can be made for each threat. A matrix may be used to assist in identifying the level of risk. The outcome of this process is a prioritized list of threats. The highest priority threat is the one that poses the most serious risk in terms of likelihood and severity. This list of prioritized threats shall be used to evaluate the acceptability of certain risks and which risks for which to make decisions concerning the employment of resources and other actions that reduce vulnerability. This assessment should be recorded as a record/baseline and updated regularly as the threat changes. If installation and unit commanders do not the resources to assess the threat for probability and severity of occurrence, they should coordinate with their next higher echelon to assist with this requirement.

C5.8.5. Unit commanders should also conduct a variation of the AT Annual Assessment described above, but apply it to the conduct of their unit mission. Threats should be listed that affect the unit as it conducts its mission. The output of this assessment is a list of terrorist threat capabilities associated with each phase of the operation.

C5.8.6. In addition to preparing an annual threat assessment, Commanders must also continuously assess local threat information so appropriate FPCON can be set. Commanders at all levels shall forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD personnel or assets for which they have AT responsibility. Threat information shall be used in the determination to raise or lower the present Force Protection Condition. Continuous threat analysis also supports the warning of suspected target facilities or personnel through the installation's mass notification system when the information relates threats of an immediate nature.

# C6. CHAPTER 6
# CRITICALITY ASSESSMENT

## C6.1. INTRODUCTION

This Chapter describes the methodology commanders and civilian equivalents can use to complete a Criticality Assessment. A critical asset, as defined by DoD Directive 5160.54 (reference (w)), is any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure their continued efficient operation; protection from disruption, degradation or destruction; and timely restoration. Both regulations and the commander's priorities and intent determine critical assets. Regulations cover items such as VIPs, ammunition storage areas, etc. The Commander's intent extends coverage to other items such as mission critical and high occupancy assets. Critical assets can be people, property, equipment, activities and operations, information, facilities, and materials.

## C6.2. CONDUCTING THE CRITICALITY ASSESSMENT

C6.2.1. The Criticality Assessment identifies assets supporting DoD missions, units, or activities and deemed critical by military commanders or civilian agency managers. For AT purposes, the Criticality Assessment should include high-population facilities, which may not necessarily be mission essential (recreational activities, theaters, or sports venues). It addresses the impact of temporary or permanent loss of assets. It examines costs of recovery and reconstitution including time, dollars, capability and infrastructure support.

C6.2.2. In military units deployed under the command of the Services or a Combatant Command, the staff at each command echelon determines and prioritizes critical assets. The Commander responsible for AT approves the prioritized list.

C6.2.2.1. The Criticality Assessment goals are:

C6.2.2.1.1. Identify installation's/unit's key assets.

C6.2.2.1.2. Determine whether critical functions can be duplicated under various attack scenarios.

C6.2.2.1.3. Determine time required to duplicate key assets or infrastructures efforts if temporarily or permanently lost.

C6.2.2.1.4. Determine priority of response to key assets, functions, and infrastructures in the event of fire, multiple bombings, or other terrorist acts.

C6.2.3. The assessment process described below is specifically designed for AT Assessment and Planning. Other DoD processes, such as the "Mission Essential Vulnerable Area" (MEVA), the "Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity" (MSHARPP) methodology, and the "Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability" (CARVER) matrix tool, offer similar types of subjective assessments but are not specifically tailored for antiterrorism assessments. While the MSHARPP and CARVER processes are included in Appendix 2 as optional methodologies for those who are familiar with their use, both have design limitations and are best used only as an adjunct to the RA and management methodology contained herein.

C6.2.4. The purpose of the Criticality Assessment process is to identify and prioritize all assets on an installation. Assets include personnel, equipment, stockpiles, buildings, recreation areas, or transportation systems that are deemed critical as defined by DoD "Antiterrorism Force Protection Installation Planning Template (reference (x)). There are many different types of assets critical to mission accomplishment and it is important not to exclude some assets because they are not necessarily mission-essential or physically located on the installation. For example, a telephone switching facility located off base may be essential to communications if alternative systems are not identified. There may also be assets on the installation which are not critical to the direct operation of the installation, but are critical to the Department of Defense.

C6.2.5. It may also be useful to link identified threat attack means to a specific time period or location. For example, a terrorist group operating in the proximity of the installation may typically target areas, such as schools or the commissary and/or exchange that contain a large number of people at certain times.

C6.2.6. When determining asset criticality, use of the following criteria shall assist in standardizing the process.

C6.2.6.1. Importance. Measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

C6.2.6.2. Effect. Measures the ramification of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

C6.2.6.3. Recoverability. Measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and

redundancies. Even if a DoD asset is injured, damaged, or destroyed, it may have future value in the accomplishment of other DoD missions or be of great symbolic value to the Department of Defense, the U.S. Government, and the American people. Consideration should therefore be given to the resources that must be expended to recover an asset and in some cases, repair it for return to service with the Department of Defense in the future.

C6.2.6.4. Mission Functionality. Measures key positions, special facilities, specialized equipment, etc., used to fulfill assigned missions.

C6.2.6.5. Substitutability. Are there substitutes available for personnel, facilities or materiel? Can assigned missions be performed using substitutes? If the substitutes are less capable, can the mission still be accomplished successfully?

C6.2.6.6. Reparability. If a DoD asset is injured or damaged, can it be repaired and rendered operable? How much time is required? How much would it cost? Could repairs be accomplished in a timely manner? Would repairs degrade asset performance, and if so, can the mission be accomplished in the degraded condition?

C6.2.7. The purpose of a Criticality Assessment Matrix is to determine the criticality of each asset, which shall also help to prioritize them. For each asset, the Assessment Team shall assign values for each criteria based on a scale, such as one to ten. The Assessment Team must determine what criteria to use. Table C6.T1. is an example of a Criticality Assessment Matrix.

**Table C6.T1. Example Criticality Assessment Matrix**

| Asset | Importance | Effect | Recover-ability | Mission Functionality | Etc. | Total |
|---|---|---|---|---|---|---|
| Base Exchange | 8 | 7 | 5 | 3 | | 37 |
| Command Post | 9 | 10 | 9 | 7 | | 57 |

C6.2.8. Once all asset values are tallied, they can be rank-ordered such that highest score is "most critical" and lowest score is "least critical." However, it is important to emphasize that not all assets in the matrix shall be "essential for mission accomplishment."

# C7. CHAPTER 7
# VULNERABILITY ASSESSMENTS (VA)

## C7.1. INTRODUCTION

VA is the process the commander uses to determine the susceptibility of assets to attack from threats identified by the AT TA. The VA answers the question "what kind of attack is the asset most/least vulnerable to?" Reference (e) provides authoritative standards regarding both installation and deploying unit Vulnerability Assessments. Vulnerabilities exist at every installation as a result of the terrorist threat faced. Vulnerabilities are always there, no matter the policies, procedures, structures and protective equipment. Although terrorist threats cannot be controlled, they can be assessed and the vulnerability of assets to those threats can be mitigated. Identifying and understanding vulnerabilities is important in determining how well an asset shall be protected from loss. Vulnerabilities are also the component of overall risk over which the commander has the most control and greatest influence. By reducing vulnerability, the potential risk to an asset is also reduced.

## C7.2. THE VULNERABILITY ASSESSMENT PROCESS.

C7.2.1. Installation or unit AT officers conduct a VA using key AT Working Group members in a collaborative effort as the assessment team. Teams should include representation from operations, security, intelligence, counterintelligence, law enforcement, communications, fire department, engineers, medical services, housing, emergency planning and WMD planning and response. The VA must comply with reference (e).

C7.2.2. The end-state of the VA process is the identification of physical characteristics or procedures that render critical assets, areas, or special events vulnerable to a range of known or feasible terrorist capabilities. Determination of vulnerability is partly a function of the commander's desired level of protection for the asset, area, or special event. Although performing a detailed VA is not simple, the results quantifying and rating the effectiveness of an installation's current protective measures are invaluable and provide a major tool for developing AT countermeasures. The VA methodology should follow the below sequence:

C7.2.2.1. List assets and the threats against those assets.

C7.2.2.2. Determine criteria to be used to assess assets against.

C7.2.2.3. Train assessment team on assessment intent and methodology.

C7.2.2.4. Assessment Team conducts assessment.

C7.2.2.5. Consolidate and review assessment results.

C7.3. PROCESS TOOLS

C7.3.1. The Department of Defense has created several tools to assist conducting Vulnerability Assessments to include the Joint Staff Core Vulnerability Assessment Management Program (CVAMP); Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (MSHARPP) and Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) (see Appendix 2). The Defense Threat Reduction Agency (DTRA) AT VA Team Guidelines are another excellent tool available for Local (Base) Vulnerability Assessments. This is a comprehensive checklist that is directly linked to reference (e) AT Standards and produces a product similar to a Joint Staff Integrated VA (JSIVA).

C7.3.2. Vulnerability Rating Example using "CARVER" criteria. CARVER (Appendix 2) provides a sample of criteria that can be used for the Vulnerability Assessment. Although criticality is covered in the CARVER method, it should not be used as a criterion for vulnerability. Criticality is covered separately during the Criticality Assessment process discussed extensively at Chapter 6.

C7.3.2.1 Accessibility. The ease with which an asset can be reached, either physically or by standoff weapons. Consider all means of attacks found in the TA.

C7.3.2.2. Recuperability. A measure of time required to replace, repair or bypass the destruction or damage inflicted on the target. Recoverability should also consider redundant systems where not all redundancies are required for mission accomplishment. Such as having five satellite radios but only two are required for mission accomplishment.

C7.3.2.3. Vulnerability. A measure of the ability of the threat to damage the target using assets available to the threat. Consider type of construction and internal placement of assets.

C7.3.2.4. Effect on Population. The positive or negative influence on the population as a result of the action taken. Effect considers public relations in the vicinity of the target, but also considers the domestic and international reaction as well.

C7.3.2.5. Recognizability. The degree to which a target can be recognized under varying weather, light, and seasonal conditions without confusion with other targets or components. Camouflage can reduce the vulnerability of an asset by making it harder to recognize.

C7.4. VULNERABILITY MATRIX.

C7.4.1. A VA matrix is useful to determine the vulnerability of each asset. For each asset, the assessment team shall assign values for each criteria based on a scale, such as one to ten, 10 being most vulnerable and 1 being least vulnerable. The assessment team must determine what criteria to use. Table C7.T1. below, is an example of a VA Matrix using the CARVER criteria.

C7.4.2. Once all asset values are tallied, they can be rank-ordered such that highest score is "most vulnerable" and lowest score is "least vulnerable." Even though an asset is very vulnerable, that does not necessarily mean that it is the highest risk. For example, equipment located in a storage warehouse near the perimeter of an installation may be very vulnerable to a vehicle bomb on an adjacent public access road. However, the criticality of the equipment and/or likelihood of it being a terrorist target may be very low, resulting in low risk.

**Table C7.T1. Example Vulnerability Assessment Matrix**

| Asset | Accessibility | Recoverability | Effect on Population | Recognizability | Etc. | Total |
|---|---|---|---|---|---|---|
| Base Exchange | 8 | 7 | 8 | 6 | | 33 |
| Command Post | 4 | 10 | 9 | 4 | | 31 |

# C8. CHAPTER 8
# RISK ASSESSMENT (RA)

## C8.1. INTRODUCTION

As discussed in Chapter 4, the RA combines Criticality, Threat, and Vulnerability assessments in order to provide a more complete picture of the risks to an asset or group of assets. This Chapter describes the methodology commanders and civilian equivalents can use to assess risk.

## C8.2. RA METHODOLOGY

C8.2.1. RA. The RA is a logical, step-by-step method, and shall require the participation of the entire staff. In starting the RA process, commanders should examine three elements: threat, criticality, and vulnerability.

C8.2.1.1. Threat. The threat is determined through a proper and thorough TA. The TA should identify the likelihood and severity of the terrorist to inflict injury to a person or damage to a facility or asset by considering terrorist capability, intent, and objectives. To enable commanders to focus their analysis, the TA should also specify the type of weapon(s) or act(s) the terrorist shall use to initiate the event (assassination, bomb, etc.).

C8.2.1.2. Asset Criticality. Critical assets are determined by both the term and the measure of importance to the installation's mission. Areas that encompass multiple critical assets are referred to as critical areas. The criticality assessment provides information to prioritize assets and allocate resources to special protective actions.

C8.2.1.3. Vulnerability. A thorough VA shall highlight the susceptibility of a person, group, unit, facility, or asset to a damaging incident. VAs should also address the capabilities of response elements to plan those activities that support the installation's ability to either deter and/or respond to terrorist threats and incidents. For example, a VA might reveal weaknesses in an organization's security systems, financial management processes, computer networks, or unprotected key infrastructure such as water supplies, bridges, and tunnels.

C8.2.2. During the RA process, the commander must consider all of the aforementioned elements, to make well-informed decisions when planning FPCON measure implementation, and terrorist incident response measures. The RA and management process described here does not dictate how to conduct the assessment, nor does it discuss how to identify deficiencies and vulnerabilities. It outlines what type of information to collect and how to organize and display

that information for decision-making. If the installation does not have the resident expertise to conduct an AT RA, consider using a JSIVA, and/or Combatant Commander or Service AT assessment reports. Vulnerabilities and deficiencies gathered from these useful reports can be plugged directly into the methodology outlined in this Chapter.

C8.2.3. Given the resource-constrained environment in which installations now operate, installation commanders or their civilian equivalents require a method to assist them in making resource allocation decisions to protect the installation from possible terrorist threats (FPCON measure implementation and other mitigation efforts) and to most effectively respond should a terrorist incident occur (response measures). Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits. The risk management process allows installation commanders to use representative (operational) risk as one of the principal factors in their decision-making process. In this context, representative risk shows the relative impact on an installation's assets, given a stated attack. Representative risk is NOT a prediction that a terrorist incident shall occur.

C8.2.4. The example below shall focus on vulnerabilities of critical assets. This same methodology can be applied to other areas of interest such as response capability. It is also important to emphasize that this methodology is merely a tool to assist commanders and civilian equivalents in assessing and managing risk.

C8.3. ASSESSING RISK -- A PRACTICAL EXERCISE

C8.3.1. This example presumes that a Commander has completed the threat, criticality, and VAs (Chapters 5 through 7). The process begins by creating an Asset RA Table. In addition to isolated assets, areas can be assessed in terms of the criticality of the assets located within it and its vulnerability to specific threats. The installation assessment team shall rate each asset for every type of threat identified in the TA.

C8.3.2. To complete the RA Table, begin by determining the asset to be examined. Create and label the table with the asset and label each column as illustrated in the Table C8.T1.

C8.3.2.1. Attack Means. Method by which asset would be attacked. Different groups may present several different attack methods based on what weapons they possess and the methods they use. Sample attack means include small arms fire, car/truck bomb, chemical weapons, biological weapons, etc. Use the information from Chapter 5.

C8.3.2.2. Criticality. Obtained from the information gathered in Chapter 6.

C8.3.2.3. Vulnerability. Obtained from the information gathered in Chapter 7.

C8.3.3. An Example. Consider a command post located in a building on a military installation. The building is constructed of 12" concrete walls, has no windows and the ventilation system is not filtered. A redundant command post exists; however, several hours would be required before it could be fully operational. Because the command post is necessary to carry out the mission, criticality is a 9 out of 10. The vulnerability is a 1 from small arms fire because small arms are unlikely to penetrate 12" of concrete and no windows exist to shoot into. The vulnerability from a car/truck bomb is higher because there is no traffic flow control around the building. The CW and BW attack means are both high vulnerabilities because the ventilation system is unfiltered.

**Table C8.T1. Example Asset Risk Assessment Table**

| Asset: Command Post | | | | |
|---|---|---|---|---|
| Attack Means | Criticality (C) (1-10) | Vulnerability (V) (1-10) | Threat Probability (TP) Y Value (1-10) | Risk Assessment (C x V x TP) |
| Small Arms Fire (SAF) | 9 | 1 | 9 | 81 |
| Car/Truck Bomb (C/TB) | 9 | 8 | 6 | 432 |
| CW | 9 | 8 | 1 | 72 |
| BW | 9 | 8 | 1 | 72 |

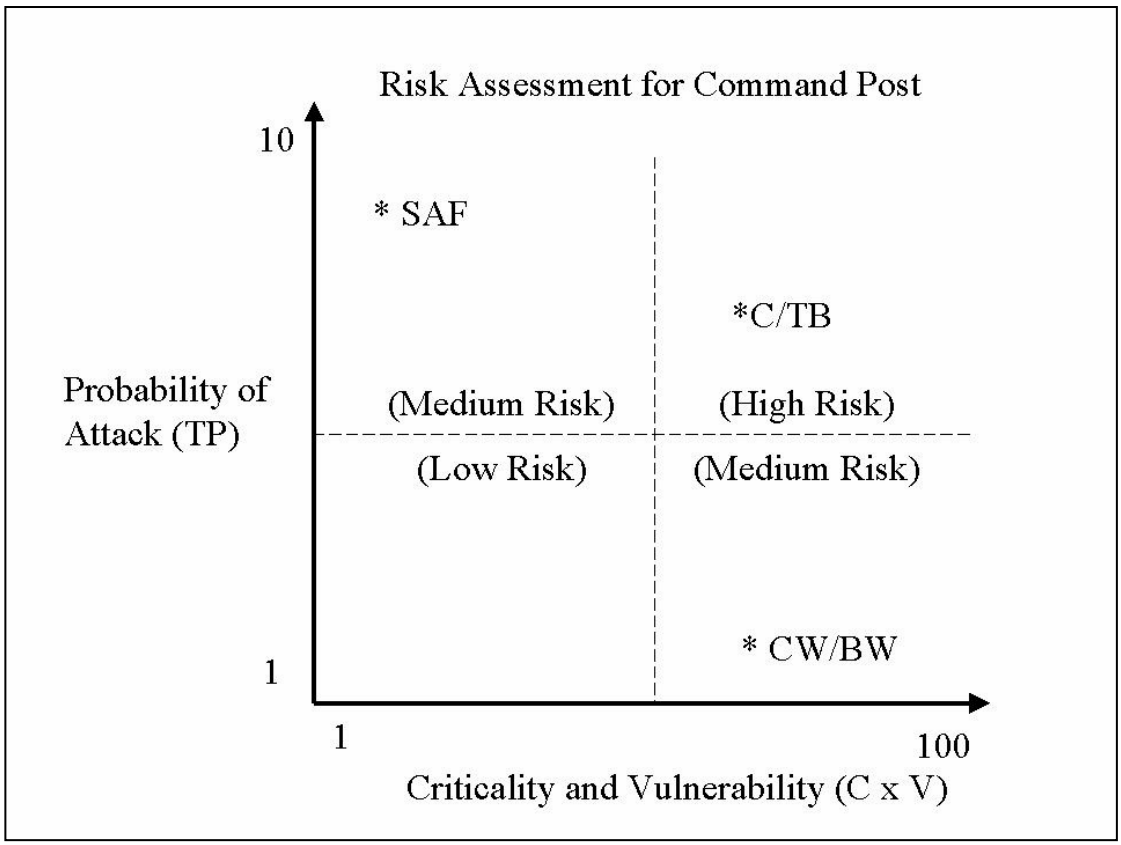
C8.3.4. It is important to note that this rating system is not meant to be a precise science. It is one method of quantifying a subjective decision, in order to generally prioritize areas in terms of risk.

C8.4. RA.

C8.4.1. Table C8.T1. gives the final RA for each asset. The assets can be prioritized based on the RA. The decision-maker is required to determine the maximum amount of risk that is acceptable.

C8.4.2. The risk can also be represented graphically using The RA Graph, Figure C8.F1. The graph shall combine the Criticality/Vulnerability/Attack Means (the x-axis) and the Threat Probability (the y-axis) to represent the risk. The representative risk is an expression of the relative impact on an asset or a planning and response element, given a stated attack means. Representative risk does NOT attempt to forecast risk (e.g., assign predictability or likelihood).

**Figure C8.F1. Example of Risk Assessment**



C8.4.3. No standard methodology exists for establishing risk levels and their determination shall vary from installation to installation, based on the commander's judgment. Although this process is subjective, commanders can focus their decision on where to establish the minimum risk by considering the following questions:

C8.4.3.1. What is the installation's mission? How important is that mission to overall U.S. military objectives in the region? (Criticality Assessment)

C8.4.3.2. What resources are available for AT activities on the installation? (VA)

C8.4.3.3. Where are the nearest available resources that could augment the installation, should an incident occur? Does the Commander have tasking authority for those resources? (VA)

C8.5. COMPLETING THE PROCESS -- RISK MANAGEMENT

C8.5.1. The end products of the above process shall be the identification of areas and assets that are vulnerable to the identified attack means and the development of associated assessment tables. From the information developed from all assessments (criticality, threat, vulnerability, and risk and the RA Graph), the Commander shall make a decision on how best to employ given resources and force protection measures to deter, mitigate, or prepare for a terrorist incident. In accordance with reference (e), installation commanders should document their risk management methodology.

C8.5.2. There are several ways to reduce risk. The decision-maker does not easily control two of those methods, reducing the threat and reducing the criticality. The one method that is controllable is reducing the vulnerability of an asset.

C8.5.3. Looking at the above example and considering only the command post, it is apparent that the highest risk is from a car/truck bomb. What are some ways of reducing the vulnerability?

C8.5.3.1. Set up barriers to control traffic flow around the command post. The further away a prospective car/truck bomb detonation, the less impact it will have on the intended target. Another alternative is to control the traffic coming onto the installation. If several buildings exist that require protection from car/truck bombs then cars and trucks can be searched more thoroughly at the entrance to the facility. If bombs aren't allowed to enter the facility, then the risk is greatly reduced.

C8.5.3.2. Determine why it takes several hours to place the redundant command post in full operation. This may only require a simple policy change or pre-positioning of equipment but the result shall be less vulnerability due to redundancy.

C8.5.4. At the end of the RA and risk management process, the commander must engage and concur with the entire assessment in order to focus the next steps in risk management process (taking action).

C8.5.5. The use of CVAMP (appendix 2) shall assist commanders and ATOs in this effort.

# C9. CHAPTER 9
# INTRODUCTION TO THE AT PLANNING PROCESS

## C9.1. INTRODUCTION

Protection of DoD personnel and assets from acts of terrorism is one of the most complex challenges for all Commanders. Planning to confront this challenge requires a comprehensive, integrated approach and a strong, clear vision of AT program requirements. AT planning is critical to deterrence, detection, defense, and response to terrorist incidents. A plan shall be written at the Combatant Commander, Service, and DoD Agency level, down to the installation level for permanent operations or locations, and incorporated into operations orders for in-transit units, temporary operations or exercises. This Chapter outlines the requirements of an AT plan and presents a methodology for plan development.

## C9.2. THE AT PLAN AND THE AT PROGRAM

By definition, the AT plan contains all the specific measures taken to establish and maintain an AT program that meets the standards of references (a) and (d). AT program elements include all the elements and assessments of the Risk Management process, planning, training and exercises, resource generation and a program review. Accordingly, an effective AT plan accounts for all aspects of the AT program.

## C9.3. AT PLAN REQUIREMENTS

At a minimum, the AT plan must address the key elements discussed below. These elements must be integrated into and/or support a comprehensive AT program. Stand-alone documents (e.g. Standard Operating Procedures, local regulations, or operations orders that articulate requirements for these key elements) shall be replicated in and/or referenced by the AT plan.

C9.3.1. TA. The terrorism TA is the tool that commanders use to arrive at a judgment of risk and consequences of terrorist attack. This assessment focuses on the full range of known or estimated terrorist capabilities in the commander's area of interest, including WMD. Annually, commanders integrate threat information prepared by the intelligence and law enforcement communities, technical information from security and engineering planners, and information from other sources to prepare their assessments (see chapter 5).

C9.3.2. Criticality Assessment. The criticality assessment shall provide the Commander with a prioritized list of assets based on the necessity for mission completion (see chapter 5).

Inputs from all organizations shall be required to determine what assets are required and how many. The completed information may be compiled into a criticality matrix. This information is then combined with the threat and vulnerability information to assess the AT risk.

C9.3.3. VA. This assessment provides a vulnerability-based analysis of an activity's AT program. A tool for the commander, the VA is the process to determine the susceptibility to attack by the broad range of terrorist threats against personnel and assets. The result of the assessment provides a basis for determining options to eliminate or mitigate vulnerabilities. Commanders shall conduct a dedicated local VA at least annually, but there should be a means to adjust the assessment as the threat changes (see chapter 7).

C9.3.4. Risk Assessment. Commanders conduct a RA to integrate threat, criticality and vulnerability information in order to make conscious and informed decisions to commit resources or enact policies and procedures that mitigate or define the risk (see chapter 8). RA provides the commander with a clear picture of the current AT posture and identifies those areas that need improvement. When conducting this assessment, Commanders shall consider the threat, asset criticality, and vulnerability of facilities, programs, and systems, as well as deterrence and response capabilities (see chapters 4 through 8).

C9.3.5. AT FPCON Measures. FPCONs AT measures are the actions taken at facilities to deter and/or prevent a terrorist(s) from conducting an attack. FPCONs are the principal means through which commanders (or DoD civilian equivalent) apply an operational decision to best protect personnel or assets from terrorist attack. AT measures assimilate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal AT protection to personnel and assets. The objective is to ensure an integrated approach to terrorist threats. Well-designed AT measures direct actions that ensure threat detection, assessment, delay, denial, and notification. AT measures should include provisions for the use of physical structures, physical security equipment, chemical-biological-nuclear-radiological-explosive detection and protection equipment, Random Antiterrorism Measures, response forces, and other emergency measures (see chapter 10). AT measures should be scalable and proportional to increases in the local threat and/or unit operational capability.

C9.3.6. Terrorist Incident Response Measures. These include procedures to provide command, control, communication and intelligence with the first responders charged with the task of determining the full nature and scope of the incident, containing damage, and countering the terrorist(s) that may still be present. The objective of terrorist incident response measures is to limit the effects and the number of casualties resulting from a terrorist attack. These measures

and the strategy that ties them together can also contribute to deterring terrorist attacks if our adversaries recognize our ability to limit the effects of their attacks.

C9.3.7. Terrorist Consequence Management Measures. As detailed in chapters 11 and 12, terrorist consequence management measures should include emergency response and disaster planning and/or preparedness to recover from a terrorist attack, to include WMD. Although not an element of AT, commanders shall include terrorist consequence management preparedness and response measures as an adjunct to the organization's AT plan. In addition, special circumstances imposed by terrorist attacks utilizing WMD shall require immediate close coordination with higher command and host nation, and/or Federal, State, and local authorities.

C9.3.8. Coverage for Off-Base Assets. In planning the coverage of off-base assets and infrastructure selected for inclusion in the facility, installation, or activity AT program, include notifications to the appropriate first responders, including law enforcement offices, and the servicing FBI field office. This shall enable integration of the facility into their response and contingency planning and provide a potential source to assist the facility in its own preparations and response. As necessary, validate and monitor the scope and viability of the coverage. If the asset is a cleared contractor facility (DoD 5220.22-M and 5220.22-R (references (y) and (z)), provide for reporting to the servicing Defense Security Service (DSS) Industrial Security Field Office (see reference (z)) of information that indicates classified information under facility control is or could be at risk. Promptly notify the servicing DSS office of any security requirements which the installation or activity intends that the cleared industrial facility implement.

## C9.4. AT PLAN DEVELOPMENT

C9.4.1. The organization's Commander is responsible for the development of the AT plan. The ATO is normally assigned the task of actually writing the plan. The ATO should leverage the capabilities of the organization's AT Working Group to assist in the process. Using the AT Working Group ensures the participation, input, and "buy-in" of the necessary subject matter experts and others with key responsibilities.

C9.4.2. There is no directed methodology for developing an AT plan. The responsibility to achieve thorough integration and avoid a "stovepiped" information flow rests with the ATO. Everyone involved in developing the plan must be familiar with all applicable AT directives and instructions. References (x) and (aa) detail the steps necessary to produce an AT plan.

C9.4.3. The following three phases are offered as a means to logically develop an AT plan:

C9.4.3.1. Phase 1: Risk Assessment. Conduct the RA only after completing the criticality, threat, and VAs. Any plan that does not start with these assessments shall be too reactive, misdirect resources, and result in wasted efforts and resources.

C9.4.3.2. Phase 2: Build AT FPCON Measures Matrices, Terrorist Incident Response Measures Matrices and Terrorist Consequence Management Measures Matrices. This phase produces the heart of the AT plan and represents the "Concept of Operations" in the five-paragraph operation order format. The end products of this phase shall be matrices of integrated pre-incident action sets to implement each FPCON security measure at the five distinct FPCONs. Each integrated action set shall identify who shall act, when they shall act, where they shall act, what the action is and the resources to be used, and how these actions shall occur at the various FPCONs. See Figure C9.F1 for an example.

**Figure C9.F1. Sample portion of a pre-incident action set matrix for FPCON NORMAL.**

| FPCON | Measure #7 | Action Set | Coordination |
|---|---|---|---|
| NORMAL | Conduct Threat Assessment | The installation senior intelligence officer shall use all available means to determine the existence, capability, intentions, history, targeting, and security environment of terrorist groups that might threaten the installation. If capabilities are listed, the threat assessment shall likely be classified. The classified threat assessment shall be maintained at the unit's XXXX office by XXXX. Dissemination shall be based on a strict need to know basis, with appropriate security clearances. | Interface with local law enforcement agencies.<br><br>Conduct interagency coordination to obtain terrorist capabilities and intentions.<br><br>Coordinate with diplomatic missions, as applicable.<br><br>Coordinate with MI and security personnel to establish the appropriate security controls and need to know. |

There should be similar matrices for each type of terrorist incident response and consequence management event. This section also contains detailed Physical Security measures. Physical Security measures are an outcome of developing the AT FPCON and Terrorist Incident matrixes.

C9.4.3.3. Phase 3: Writing the AT Plan. The challenge for the ATO responsible for writing the plan is to select a format that best suits the organization's ability to understand the plan, and to execute it quickly and decisively when required. While there is no mandated format, it is recommended that organizations use the standard five-paragraph order outlined in JP 5-002 (reference (ab)). Sample installation AT plans are also provided in Appendix 4 and in reference (x). Each level of organization shall necessarily produce an AT plan consistent with their mission and responsibilities. For example, at the installation level, the AT plan shall have a very tactical perspective and provide minute details for actions to be taken locally. A geographic Combatant Commander's plan, on the other hand, shall be at the operational level and shall provide descriptive guidance rather than prescriptive solutions.

# C10. CHAPTER 10
# THE DoD FORCE PROTECTION CONDITION (FPCON) SYSTEM

## C10.1. INTRODUCTION

C10.1.1. The FPCON System describes the progressive level of protective measures implemented by all DoD Components in response to terrorist threats. It is the principal means through which a military commander or DoD civilian exercising equivalent authority applies an operational decision on how to best guard against the threat. These guidelines shall assist commanders in reducing the effect of terrorist and other security threats to DoD units and activities.

C10.1.2. Creating additional duties and/or watches, and heightening security enhance Command's personnel awareness and alert posture. These measures display the Command's resolve to prepare for and counter the terrorist threat. These actions shall convey to anyone observing the command's activities that it is prepared and an undesirable target, and that the terrorist(s) should look elsewhere for a vulnerable target.

C10.1.3. The DoD system is generally not applicable to DoD elements that the Chief of Mission (COM) has security responsibility for and may have limited application to DoD elements that are tenants on installations and facilities not controlled by U.S. military commanders or DoD civilian exercising equivalent authority. Still, Commanders of U.S. elements on non-U.S. installations can execute many FPCON measures that do not involve installation level actions, at least to a limited degree. The terminology, definitions, and specific recommended security measures are designed to facilitate interservice coordination and support for the combating terrorism efforts of the DoD Components.

## C10.2. FORCE PROTECTION CONDITIONS (FPCONs)

There are five FPCONs. Supporting measures for each condition are listed in Appendix 3. The circumstances that apply and the purposes of each protective posture are as follows:

C10.2.1. FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

C10.2.2. FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

C10.2.3. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

C10.2.4. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

C10.2.5. FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

C10.3. FPCON RESPONSIBILITIES

C10.3.1. Per references (a) and (e) Geographic Combatant Commanders shall ensure that FPCONs are uniformly implemented and disseminated with their AOR.

C10.3.1.1. All military commanders and DoD civilians exercising equivalent authority are responsible for ensuring that their subordinates fully understand FPCON declaration procedures and FPCON measures.

C10.3.1.2. While there is no direct correlation between threat reporting and FPCONs, such information assists Commanders in making prudent FPCON declarations. Existence of threat reporting in and of itself should not be the only factor used in determining FPCONs. FPCON declaration should be based on multiple factors that may include, but are not limited to, threat, target vulnerability, criticality of assets, security resource availability, operational and physiological impact, damage control, recovery procedures, international relations, and planned U.S. Government actions that could trigger a terrorist response.

C10.3.2. The DoD FPCON system allows all military commanders and DoD civilians exercising equivalent authority the flexibility and adaptability to develop and implement AT measures that are more stringent than those mandated by higher authorities whenever FPCONs are invoked. Each set of FPCON measures is the minimum that must be implemented when a change in local threat warrants a change in FPCON or when higher authority directs an increase in FPCON. Authorities directing implementation may augment their FPCON by adding measures from higher FPCONs as necessary.

C10.3.2.1. Military commanders or DoD civilians exercising equivalent authority may implement additional FPCON measures from higher FPCONs on their own authority, develop additional measures specifically tailored for site-specific security concerns, or declare a higher FPCON for their AOR/installation.

C10.3.2.2. Subordinate military commanders or DoD civilians exercising equivalent authority at any level may not lower a FPCON or implement measures that are less rigorous than those appropriate for the declared FPCON. Waivers for not complying with prescribed FPCON measures may be obtained by following the procedures in section C10.6.

C10.3.2.3. It is essential for military commanders and DoD civilians exercising equivalent authority to implement formal analytical processes that result in a set of AOR or locality-specific terrorist threat indicators and warnings for use when transitioning from lower to higher FPCONs. Threat credibility, and if known, duration, operational environment (both H/N and DoD), asset criticality, mission impact and measures in place that contribute to mitigating the current threat are but a few of the important elements commanders should consider when calibrating FPCON postures. Such processes and measures should be harmonized to the maximum degree possible, taking fully into account differences in threat, vulnerability, criticality, and risk of resources requiring protection.

C10.3.2.4. Military commanders, DoD civilians exercising equivalent authority, and their staffs shall examine the threat, physical security, terrorist attack consequences, and mission vulnerabilities in the context of specific DoD activities and the declared FPCON. When factors are combined and the collective terrorist threat exceeds the ability of the current physical security system (barriers, surveillance and detection systems, security forces, and dedicated response forces) to provide the level of asset protection required, then implementation of higher FPCONs or additional measures is appropriate.

## C10.4. FPCON MANAGEMENT AND IMPLEMENTATION

Implementation of FPCONs does not come without adverse effects on day-to-day operations; the additional costs can be measured and described both quantitatively and qualitatively. The DoD FPCON system acknowledges cost as a significant factor bearing on the selection and maintenance of FPCONs. FPCONs ALPHA and BRAVO include measures that can be sustained for extended periods, consistent with the terrorist threat.

C10.5. RANDOM ANTITERRORISM MEASURES (RAMs) MANAGEMENT AND IMPLEMENTATION

C10.5.1. Commanders and Directors should randomly change their AT tactics; techniques and procedures so that they ensure a robust security posture from which terrorists cannot easily discern patterns or routines that are vulnerable to attack. An effective RAM program shall enable security to appear not only formidable but also unpredictable and ambiguous to instill uncertainty in terrorist planning. The basic approach for random antiterrorism measures (RAMs) program is to select security measures from higher FPCONs, as well as other measures not normally associated with FPCONs (Command developed measures, or locally developed site-specific measures) that can be employed in a random manner to supplement the basic FPCON measures already in place. Using a variety of additional security measures in a normal security posture prevents overuse of security forces, as would be the case if a higher FPCON were to be maintained for an extended period of time. Selected RAMs offer an alternative to full implementation of a higher FPCON level. This is particularly important when terrorist threat estimates suggest that lower FPCONs may not, for the moment, be adequate in view of the risk, vulnerability, and criticality of DoD assets at the installation or facility.

C10.5.2. To enhance the overall effectiveness of a given FPCON, unit commanders shall develop and implement a RAMs program as an integral part of their AT program. RAMs should be implemented in a strictly random manner, never using a set time frame or location for a given measure. RAMs should be visible (to confuse surveillance attempts) and should involve the command as a whole, not just the security forces. To be effective, tenant and transient units must be fully integrated into and support the installation or facility RAM program. Advantages of implementing RAMs include, but are not limited to:

C10.5.2.1. Executing a comprehensive, RAM program enables commanders/directors to maintain/sustain lower FPCON without compromising security effectiveness. Also, it maximizes scarce security resources and minimizes security force burnout and degradation in command AT awareness.

C10.5.2.2. Making it more difficult, through variations in our security routines, for terrorists to target important assets, build detailed descriptions of significant routines, or predict activities by a specific asset or within a targeted facility or installation.

C10.5.2.3. Helping to mask our capabilities to respond to, and defeat, terrorist attacks through unannounced, unpredictable, and visible security measures.

C10.5.2.4. Increasing AT awareness for DoD personnel, their family members, visitors, and neighbors.

C10.5.2.5. Providing additional training and increasing alertness of assigned security personnel and other participants through mental stimulation by changing their routine.

C10.5.2.6. Validating the installation or facility's capability to execute individual measures from higher FPCON.

C10.5.2.7. Enabling Commanders/Directors to more rapidly transition between FPCONs.

C10.5.3. Commanders/directors of defense agencies/facilities and their AT officers should keep the following tenets in mind when developing and executing their RAM program.

C10.5.3.1. The installation ATO is in charge of the RAM program, not the Provost Marshal or Security Officer if a separate entity/individual. However, the ATO should coordinate with the Provost Marshal/Security Officer regarding RAM measures that require utilization of security personnel. The ATO should monitor, track, and analyze RAM implementation efforts.

C10.5.3.2. A RAM program is part of a proactive and dynamic AT program.

C10.5.3.3. RAMs should be visible (to confuse surveillance attempts) and should involve the command as a whole, not just the security forces.

C10.5.3.4. To be effective, tenant and transient units must be fully integrated into and support the installation or facility RAM program.

C10.5.3.5. RAMs should be used throughout all FPCON levels and should include other measures not normally associated with a FPCON level such as Command developed measures, or locally developed site-specific measures.

C10.5.3.6. To confuse terrorist surveillance attempts, RAMs should be implemented in a strictly irregular fashion, never using a set time frame or location for a given measure.

C10.5.3.7. Local random antiterrorism measures should:

C10.5.3.7.1. Assess local threat capabilities and identify effective RAMs Countermeasures.

C10.5.3.7.2. Mitigate installation/facility vulnerabilities.

C10.5.3.7.3. Be conducted both internally to the installation and externally in coordination with local authorities.

C10.5.3.7.4. Be compatible/coordinated with ongoing approved surveillance detection and security measures.

C10.5.3.7.5. Not be limited to security force personnel.

C10.5.3.7.6. Incorporate analysis of time and space considerations to allow security forces to maintain sufficient standoff while determining hostile intent.

C10.5.4. A dynamic and proactive RAM program visibly communicates a Command's resolve to prepare for and counter the terrorist threat. A RAMs program shall make it difficult for terrorist planners to discern security, defense and operational patterns. The terrorists should be compelled to look elsewhere for a more static and therefore more vulnerable target.

## C10.6. DEVIATIONS FROM DIRECTED FPCONs

If it is determined that certain FPCON measures are inappropriate for current operations, or for proper threat mitigation, military commanders or DoD civilians exercising equivalent authority may request a waiver. The first general/flag officer exercising Tactical Command (TACON) for force protection or DoD civilian member of the senior executive service (SES) exercising equivalent authority in the chain of command is the approval authority for waiver of specific FPCON measures. Geographic combatant commanders, their deputies, or DoD civilians exercising equivalent authority may delegate this authority below the general/flag officer level on a case-by-case basis. Any senior military commander having TACON for force protection or DoD civilian member of the SES exercising equivalent authority may withdraw first general/flag officer or DoD civilian authority and retain this authority, at his or her discretion. Waiver authority for specific FPCON measures directed by a higher echelon (above first general/flag officer or DoD civilian member of the SES) rests with the military commander or DoD civilian exercising equivalent authority directing their execution. Nothing in this waiver process is intended to diminish the authority or responsibility of military commanders or DoD civilians exercising equivalent authority, senior to the waiver authority, to exercise oversight of FPCON and RAMs program execution.

C10.6.1. To ensure a consistent force protection posture is maintained, tenants on CONUS installations and facilities shall coordinate waiver actions with the host installation before submitting them to their chain of command.

C10.6.2. All waiver requests shall be directed to the waiver authority. Information copies shall be sent to the Combatant Command's joint operations center, major/fleet command's operations center, service operations center, or DoD civilian operations center, as applicable.

C10.6.3. Approved waivers, to include mitigating measures or actions, must be forwarded to service, combatant command, major command, fleet, or DoD civilian equivalent command-level recipients within 24 hours.

# C11. CHAPTER 11
# CONSEQUENCE MANAGEMENT PLANNING
# AND
# TERRORIST USE OF WEAPONS OF MASS DESTRUCTION (WMD)

## C11.1. INTRODUCTION

WMD are those weapons capable of a high order of destruction and/or of being used in such a manner as to kill/injure large numbers of people. WMD can be any device, material, or substance used in a manner, in a quantity or type, or under circumstances evidencing intent to cause death or serious injury to persons or significant damage to property. WMDs can be CBRNE devices. This Chapter provides an overview of the potential use of weapons of WMD by terrorists and broad guidance for achieving reference (e) standards.

## C11.2. TERRORIST USE OF WMD

C11.2.1. The threat of terrorist use of WMD poses great challenges for military organizations. Previous concerns regarding WMD use focused on battlefield employment against warned and protected military personnel. The threat has expanded in recent years as many terrorist organizations have grown in sophistication and now have the ability to acquire and employ WMD. Numerous groups and organizations have determined that acquiring and using WMD may further their cause. Paramilitary groups, antigovernment organizations, political splinter groups, religious cults, and terrorist organizations have all attempted to use some type of WMD against U.S. interests or those of our allies.

C11.2.2. Recent events have demonstrated the reality of terrorist acquisition and employment of all types of WMD. The ease with which these organizations obtained material and technology to manufacture and disseminate WMD clearly shows that even small, previously unknown groups can pose significant threats to DoD organizations. The documented use of biological agents, toxins, chemical agents, and/or the efforts to obtain radiological material serve to illustrate the growing concern over terrorist use of WMD.

## C11.3. CONSIDERATIONS

C11.3.1. WMD Threat. WMD related events have increased in number and lethality in a relatively short time. The probable use of this asymmetrical threat requires specific planning on the part of not only combat forces, but peace time forces and noncombatants as well.

C11.3.2. WMD Planning Considerations. Existing military doctrine has expanded from Chemical, Biological, and Radiological (CBR) terminology to include Nuclear and High-yield Explosives (CBRNE). Planning factors for battlefield use of these weapons may have direct application when planning for terrorist use of WMD. Table C11.T1. summarizes planning considerations in existing joint doctrinal publications on the use of CBRNE weapons. Section C11.6. addresses planning considerations for possible terrorist use of WMD.

**Table C11.T1. Doctrinal CBRNE Planning Considerations**

| Considerations | Include |
|---|---|
| Awareness Training | Agents, Delivery Methods, and Symptoms |
| Contamination Avoidance | Contamination Control, Detection and Warning, Identification and Marking, Setting perimeters, and Passive Defense Measures |
| Protection | Individual Protection and Collective Protection |
| Decontamination | Immediate, Operational, and Thorough Decontamination |
| Medical Aspects | Treatment; Intervention/Countermeasures; Medical Surveillance; Triage; Quarantine; and Casualty Evacuation and Handling |
| Other Considerations | DoD dependents, Civilians and Contractors; Visitors; Host Nation and Multinational Forces and Personnel |

C11.3.3. Chemical Agents. The traditional categories of chemical agents include blister agents, nerve agents, blood agents, and choking/respiratory agents. These agents have been studied extensively. Their physical properties, physiological effects to the human body, treatment, and methods of employment are well documented in military doctrinal publications. It is important to remember that most military planning concerns large-scale use of the weapons against troops in a tactical environment. Threat from terrorist use may well be from the release of relatively small quantities in highly populated areas where the potential for exposure is greatest. Table C11.T2. lists some of the most common military chemical agents and their properties. Army FM 3-11.9 (reference (ac)) provides more information on various Chemical and Biological warfare agents.

**Table C11.T2. Examples of Chemical Agents**

| TYPE AGENT | EXAMPLE | MECHANISM OF ATTACK | TIME TO ONSET OF SYMPTOMS | SYMPTOMS |
|---|---|---|---|---|
| Blister | Mustard (H) | Skin and tissue destruction on contact | 2-12 hours | Redness of skin, skin blistering, eye irritation, blindness, and lung damage |
| Nerve | Sarin (GB) and VX | Nervous system disruption on inhalation or contact | Seconds to minutes | Dim vision, muscular twitching, salivation, difficulty breathing, nausea, and convulsions |
| Blood | Cyanogen chloride (CK)<br>Hydrogen cyanide (AC) | Blocking of blood and oxygen on inhalation | Seconds to minutes | Dizziness, nausea, vomiting, headaches, and convulsions |
| Choking | PHOSGENE (CG)<br>Chlorine | Lung damage on inhalation | Minutes for initial symptoms, several hours for later symptoms | Eye and airway irritation, tightness in the chest, shortness of breath, and fluid in the lungs |

C11.3.3.1. While much is known about these categories of chemical agents, terrorists are also capable of using a wide variety of toxic industrial chemicals and toxic industrial agents. Planning for this type of attack against unwarned, unprotected personnel presents great challenges to DoD organizations. These toxic industrial chemicals (TICs) and toxic industrial materials (TIMs) may exist in large quantities on/near military installations and provide potential weapons of opportunity. Additionally, current detection equipment may not be able to adequately warn of an incident or to properly identify the type of substance used. Medical personnel may not be able to rapidly diagnosis or treat casualties. Decontamination and contamination control procedures may not adequately address techniques to minimize and mitigate the effects of the incident. To minimize the uncertainty of these situations, a thorough assessment of the range of possible threat agents and potential vulnerabilities is essential.

C11.3.3.2. For any type of chemical agent attack, procedures must be in place to allow for the rapid recognition and warning of the incident. Unlike biological agents, chemical agent exposure generally results in the sudden onset of symptoms. Emergency responders should be trained to recognize symptoms of chemical contamination. Emergency medical responders should be trained to recognize and treat victims of toxic chemical exposure. Detection and

identification of the agent or agent properties will need to occur at the site and be conducted by an appropriate first response team.

C11.3.4. Biological Agents. A major problem posed by biological weapons is the lack of adequate quantities of responsive and sensitive biological detectors. If an area is not covered by detectors , there shall be a significant lag-time between employment and on-set of symptoms. Biological weapons may be more insidious than chemical weapons. Current biological detectors are "detect to treat," providing information on the type of agent after exposure. Research, development, and acquisition (RDA) efforts are underway to develop and field "detect to warn" detectors, but deployment of such devices shall not occur for several years. Once exposure has occurred, most of the biological agents have an incubation period of one to seven days before the onset of symptoms. Potential agents such as anthrax, cholera, plague, smallpox, tularemia, and viral hemorrhagic fevers, such as Ebola virus, Lassa fever, and Yellow fever, have delayed symptoms following initial exposure. The lag time from employment until detection has the potential to allow for widespread contamination and the dispersion of affected personnel across a very large area. Table C11.T3. shows some potential biological agents, their incubation periods, and potential lethality.

**Table C11.T3. Example Biological Agents**

| **Error! No index entries found.** | Causative Agent | Incubation Period (Days) | Fatalities (%) |
|---|---|---|---|
| Anthrax | Bacillus anthracis | 1-5 | >90 |
| Plague | Yersinia pestis | 1-3 | 90 |
| Tularemia | Francisella tularensis | 1-10 | 5-20 |
| Cholera | Vibrio cholerae | 2-5 | 25-50 |
| Venezuelan Equine Encephalitis | VEE Virus | 2-5 | <1 |
| Q Fever | Coxiella burnetti | 12-21 | <1 |

C11.3.4.1. One method terrorists may use to spread biological agents is through dispersal of the agent as an aerosolized spray containing bacteria, viruses, or spores. This method is hard to detect and is effective in covering large areas with minimal amounts of agent and equipment. Other methods of agent dispersal include introducing the agent into food and water sources or releasing animals (vectors) that have been infected or are carrying the pathogenic organism. Detection of attacks is usually delayed, allowing for significant dispersion of the agent and greatly increased casualties. The following examples demonstrate how terrorists could disperse

biological agents using very common means that would be difficult to detect and attract little attention from security personnel.

C11.3.4.1.1. Individuals posing as workers in utility uniforms spraying vegetation along the perimeter fence line of an installation or headquarters. The sprayers could contain biological agents that were being aerosolized by the commercial weed sprayers.

C11.3.4.1.2. A small boat passing through a port area on a slow meandering course. A commercial generator and compressor could be concealed in the boat and disperse a significant quantity of agent material over a large area.

C11.3.4.1.3. A small commercial aircraft with an advertising banner attached flying repeatedly over an outdoor sporting event or over a housing area. The plane could easily conceal a spray tank that was dispersing agent over a very large area.

C11.3.4.2. Two key factors limiting the effects of a potential biological agent attack are a comprehensive vaccination policy and the active medical surveillance program. Vaccination programs offer the best defense against agent exposure but are limited by a lack of vaccines for all potential agents. To help compensate for this shortfall, it is important to involve medical personnel in assessing the threat from indigenous diseases and establishing an active preventive medicine program. In contrast to naturally occurring diseases in which incidence of the disease increase slowly over a period of weeks or months, a deliberate biological attack shall peak in a few days. Timely identification and communication of the attack is essential in treating and controlling the disease and limiting the effect on personnel. An active medical surveillance program is essential to this process.

C11.3.4.3. Preventive medicine services shall be in great demand upon the onset of an attack. Demands for medical support and service shall likely exceed their availability. Preventive medicine specialists shall be required to assist Commanders with identifying safe food and water sources and in determining when to use treatment, immunization, and other preventive measures. Preventive medicine personnel must be continually aware of the biological threat in order to update their database on diseases, potential vectors, and the susceptibility of troops to diseases.

C11.3.5. Toxins are a relatively new threat and pose a difficult problem in detecting an attack. Toxins are chemical compounds, obtained from biological sources. Botulinum and ricin are in the toxin category. As with biological agents, medical personnel must provide assistance in identifying and treating personnel that are exposed to toxin agents. Toxins may be dispersed

by methods similar to those used for biological agents and are more rapid acting. Other than immediate decontamination, there are no fielded first aid or treatment options for toxins; casualties must be taken to a medical facility for diagnosis and treatment. Table C11.T4. lists examples of toxins and the time frame from exposure to onset of symptoms.

**Table C11.T4. Toxin Agents and Onset of Symptoms**

| TOXIN | Exposure Lag/Onset of Symptoms |
|---|---|
| Trichothecene Mycotoxins (T2) | Minutes |
| Ricin | 18-24 Hours |
| Staplylococcal Enterotoxin B | 3-12 hours |
| Botulinum Toxin | 24-36 hours |

C11.3.5.1. Toxins are non-volatile and tend to be more toxic than chemical agents. For example, botulinum toxin is 15,000 times more lethal than nerve agent GB. Their volatility means that they would not be a persistent battlefield threat and would not likely be spread by secondary or person-to-person exposures.

C11.3.5.2. For toxins, both incapacitation and lethality must be considered. Several toxins cause significant illness at levels much lower than the level required for lethality and are militarily significant in their ability to incapacitate military force and civilian populations. Recovery rates for exposed personnel tend to be slow, even when they are provided continuing medical treatment.

C11.3.6. Radiological Materials. While it is unlikely that non state sponsored terrorists shall develop nuclear weapons, they have shown that they can procure radioactive material. The most likely source of this material is from industrial and medical applications. Nuclear research facilities, nuclear reactors, medical research and treatment centers, and construction engineering activities are all potential sources of radioactive material. Low-level radioactive material and radioactive waste could be used to contaminate food and water sources as well as public areas and facilities. Equipment to detect radiation is available to most units, but normally is not in continuous use. Because low-level exposure to radiation does not have a noticeable immediate effect, an attack may go undetected. An exception to this would be the use of an improvised explosive device to spread radiation upon detonation. Radiation, regardless of its intensity, has the potential to produce harmful effects on unprotected personnel and have significant

psychological impact. Effects may be the result of external exposure to a radioactive source or inhalation or ingestion of radioactive particles.

C11.3.7. Recent events have forced a greater awareness of the vulnerability of U.S. personnel and facilities to attack from terrorist elements, both in the US and abroad. The suddenness and severity of the attacks has reinforced the need to anticipate and plan for the threat and consequence of terrorist attacks against U.S. personnel. The remainder of this Chapter addresses reference (e) standards to assist in the analysis, planning, crisis management, and consequence management of the possible use of WMD by terrorist organizations.

C11.4. POTENTIAL THREAT OF TERRORIST USE OF WMD

C11.4.1. The potentially devastating effect of terrorist use of WMD mandates that organizations conduct a thorough analysis of the threat in their areas of interest. Chapter 5 provides detailed discussions on guidelines and procedures to follow when conducting terrorist threat estimates. The unique aspects of the terrorist threat to acquire and employ WMD should be considered as a distinct element of the overall TA.

C11.4.2. The Combatant Commanders should ensure an integrated collection and analysis program is established that draws detailed threat data from all available sources. Deployed forces should also establish close relationships with diplomatic missions and supporting country teams within their AOR; they are an excellent source of information on the political and psychological background of local terrorist organizations.

C11.4.3. Collection plans should address the terrorist capability to acquire and use WMD. This information should be part of the Commander's Essential Elements of Information (EEI). EEI should be integrated into subordinate elements' collection plans and reviewed as new or evolving threats emerge. The plan should consider terrorist threats from commercial, industrial and medical source material as well as the traditional military nuclear, biological and chemical weapons and agents.

C11.4.4. New or changing terrorist capability to acquire or deploy WMD must be rapidly disseminated through command channels. Units should include procedures for immediate reporting of changing terrorist threats or actual use of WMD. Notification should be sent through chains of command, lines of authority, intelligence agencies and similar organizations. As appropriate, it must also be passed to diplomatic missions or local U.S. authorities to assist them in their preparation and response for a potential incident.

C11.5. VA FOR TERRORIST USE OF WMD

C11.5.1. Organizations shall assess the vulnerability of installations, facilities, and personnel in their AOR to terrorist use of WMD. VAs shall be based on the TAs derived from reference (e) standards and on the principles of VAs.

C11.5.2. As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, Explosive Ordnance Disposal, and CBRNE staff elements. The entire range of potential terrorist WMD use should be considered when conducting assessments. As previously mentioned, threats from commercial chemical, biological, nuclear, high-yield explosive and radiological sources should be included as well as traditional military agents. Commanders should consider the following when conducting VAs and possible mitigation options:

C11.5.2.1. Availability of individual protective clothing and equipment.

C11.5.2.2. Availability of collective protection equipment and facilities.

C11.5.2.3. Medical response and emergency services capability.

C11.5.2.4. Training of personnel.

C11.5.2.5. Physical security and protective barriers.

C11.5.2.6. Facility design and construction.

C11.5.2.7. Early warning and detection capability.

C11.5.2.8. Alarms and attack warning.

C11.5.2.9. Threat intelligence.

C11.5.2.10. Sustainment operations and follow on support.

C11.5.2.11. Force health protection strategy.

C11.5.2.12. Storage of bulk hazardous material.

C11.5.2.13. Explosive Ordnance Disposal response capability and availability.

C11.6. PLANNING FOR CONSEQUENCE MANAGEMENT

C11.6.1. DoD Instruction 2000.18 (reference (ad)) provides DoD guidance for the establishment of a CBRNE preparedness program for emergency responders at all DoD installations. DoD installation emergency responders must be prepared to respond to the effects

of a CBRNE incident to preserve life, prevent human suffering, mitigate the incident, and protect critical assets and infrastructure. Reference (e) standards require commanders to "include terrorist consequence management preparedness and response measures as an adjunct to the installation AT Plan." The planning must focus primarily on mitigating the effects of, and immediate recovery from, a terrorist incident and address all factors included in emergency response and disaster planning doctrine for the installation. To ensure completeness, plans should address the nine weapons of mass destruction response functions (WMDRF), as discussed later in this Chapter. As in all AT planning, the WMD portion of the AT plan should be a product of a working group comprised of the representatives from the installation or unit functional areas. More assistance for WMD planning can be found in the WMD Appendix to the AT/FP Installation Planning Template or the Installation Antiterrorism Program and Planning Tool, both produced by the Joint Staffs Deputy Directorate for Antiterrorism and Homeland Defense, J3 DD AT/HD.

C11.6.2. According to reference (e), commanders must develop estimates for potential terrorist use of WMD in their AOR. This forms the basis for all facts and assumptions that drive the planning and preparation for any use of WMD by potential threat organizations.

C11.6.3. Likewise, reference (e) directs that Commanders must conduct a vulnerability assessment for terrorist use of WMD. Identification of the most likely and vulnerable targets enables more detailed planning, which drives organizations to improve security measures.

C11.6.4. Chapter 12 contains detailed crisis planning/incident response and execution guidelines for dealing with a terrorist incident. Organizing the WMD portion of the AT plan by WMD response functions ensures all functional areas of the installation or unit are addressed. WMDRFs are derived from the National Response Plan Emergency Support Functions (ESFs). The following contains the nine WMDRFs and additional planning considerations that should be included in addressing terrorist use of WMD.

C11.6.4.1. Information and Planning. This area focuses on preparing the installation to respond to a terrorist attack. In the event of a terrorist incident, the installation must coordinate large contingencies of internal and external support organizations for an effective incident response. The subtasks are MOUs/MOAs, command and control, emergency operations center, and public information.

C11.6.4.1.1. MOUs/MOAs. During the "baselining" process, the Commander identifies shortfalls in capability to detect, deter and respond to an incident. The shortfalls from

the response functions may be filled through MOAs/MOUs with local, State, and Federal authorities or the host nation. Coordination with local authorities is essential when planning for a WMD event. An attack on either the DoD facility or the local civilian populaces shall most likely affect both communities. Thorough coordination between DoD organizations and local officials provides a means to improve the response time and offers the opportunity to share critical resources needed to mitigate the effects of an incident. MOUs/MOAs are discussed in more detail in Chapter 3.

C11.6.4.1.2. Command and Control. Command and control is the process Commanders use to plan, direct, coordinate, and control forces to ensure mission accomplishment. The facility Commander has overall authority and direction over the WMD incident through his on site incident commander, unless further delegated, or assumed by the FBI. In the event the FBI assumes jurisdiction, the facility Commander retains control of military assets. For off-facility CBRNE events in foreign countries, the DOS is designated as the primary Federal Agency for foreign consequence management operations in support of foreign governments.

C11.6.4.1.3. Emergency Operations Center (EOC). The purpose of the EOC is to provide overall command and control (on behalf of the commander) of a WMD or other type of incident. The EOC should be organized and equipped to coordinate information flow between the on-scene Commander and facility Commander. Standard Operating Procedures (SOPs) should be documented and procedures refined as needed. EOCs normally have only a small staff on duty and shall require immediate augmentation when an attack occurs. EOCs may be unmanned and are activated (partial or full) depending on the incident scope. Staff elements should be fully trained and prepared to implement the appropriate plan to reduce the effects of a WMD incident. Based on criticality and VAs, installation planners should identify areas on the installation that could serve as alternate command posts/EOCs. The EOC facility may need to have special design and construction so it can operate during a CBRNE incident.

C11.6.4.1.4. Intelligence/Threat. The intelligence staff must provide the commander with timely and accurate intelligence. Intelligence assessments should consider all sources of intelligence, to include local law enforcement, FBI, and U.S. Embassy (if applicable), in determining terrorist WMD intentions and capabilities. In the U.S. and its territories, Commanders can obtain local terrorist threat information by querying the FBI through the installation law enforcement liaison, local law enforcement, or other Federal Agencies.

C11.6.4.1.5. Public Affairs (PA). Principal PA objectives of a WMD plan are to ensure that accurate information is provided to the public and to communicate a calm, measured, and reasonable reaction to the ongoing event. When the EOC is activated, operations include the activities of the Public Affairs Officer (PAO) and media center. The media center is located in a separate location from the EOC. The PAO is represented in both the EOC and media center and prepares media releases and conducts briefings at the media center during the incident, using information obtained by the PAO and cleared by the EOC and the commander or his or her designated representative. The PAO must be fully apprised of the situation as it develops. The media representatives should not have direct access to terrorists, victims, and communications nets, or anyone directly involved in a terrorist incident unless the PAO has cleared such contact with the EOC. DoD experience with media representatives has shown that bringing them in early under reasonable conditions and restrictions commensurate with the risk and gravity of the event and providing them thorough briefings maintains DoD credibility and preserves freedom of information. PA efforts should focus on informing the public of possible dangers and reinforcing public confidence in the installations' capabilities to respond to an event.

C11.6.4.1.6. Training and Exercises. Training is the means to achieve the tactical and technical proficiency that individuals, leaders, and units must have to enable them to accomplish their missions. Training must focus on the techniques and procedures of integrated response operations. Exercises should include all response functions, to include local, State, Federal, or host nation resources, required to support AT and consequence management operations. AT training should be incorporated into unit-level training plans and pre-deployment exercises. Lessons learned must be documented (after action review (AARs)) and used to develop training plans and assess the overall effectiveness of the AT plan.

C11.6.4.2. Communications. A crucial aspect of implementing the WMD plan is establishing and controlling communications among the forces in the incident area, the EOC, and the Incident Response Team (IRT). Communications personnel must be able to respond to changing needs during the incident and be able to maintain, over a prolonged period, control of all incoming and outgoing communications as well as the communications channels included in the WMD plan. Use of appropriate secure emergency communication equipment is paramount to successful management of the incident. Interoperability with all response entities, military or civilian is necessary. Back up communication plans and equipment (layers of capability) should be planned for and available if needed.

C11.6.4.3. Hazardous Materials (HAZMAT)/CBRNE. The HAZMAT/CBRNE WMDRF refers to expertise necessary to respond to the release of a CBRNE agent on the installation. All installation personnel should be trained to notify the proper authorities of a suspected or actual CBRNE release. The proper authorities shall then activate the response element. The response element may consist of the WMDRF leads and associated teams of each functional area, such as detection, security, safety, medical, transportation, logistics, fire fighting, decontamination, and any personnel having CBRNE expertise. This response element should be able to arrive immediately on the incident site, assess the situation, advise the EOC, mitigate the situation and have reach-back capability to follow-on forces/expertise, as the situation dictates. The response element acts as the forward command at the incident site. This element should ensure the actions at the incident site are properly coordinated. A staff member in the EOC with CBRNE expertise shall greatly add to the support of the CBRNE response at the incident site.

C11.6.4.4. Security. The security forces of an installation must provide physical security of the incident site and conduct post-incident investigations. This force consists of persons specifically organized, trained, and equipped to protect the physical security interests of the command. The site of a CBRNE terrorist incident is a crime scene. Witness testimony, physical evidence, and photographic evidences are important in pursuing leads on suspected terrorists. Security forces must maintain a continuous chain of custody on evidence obtained during an incident by documenting the location, control, and possession of the evidence from the time of custody is established until presenting the evidence to other authorities or in court. Training and exercises for security forces should include self-protection measures and tactical operations in a CBRNE environment to protect strategic or other critical assets.

C11.6.4.5. Fire Fighting. Fire fighting response functions include detecting and suppressing fires, effecting rescue, rendering life saving first aid, and providing water to decontamination efforts.

C11.6.4.6. Health and Medical Services. Health and medical services should provide for adequate public health and medical care following a WMD incident, both at the incident site and in hospitals. The use of CBRNE weapons or systems may create large numbers of casualties in short periods; compromise both the quality and quantity of health care delivered by posing a serious contamination threat to medical personnel; constrain mobility and evacuation; and contaminate the logistical supply base. These factors have the potential of severely degrading health care delivery and require detailed planning.

C11.6.4.7. Resource Support. Resource support should provide operational support to obtain, maintain, store, move, and replenish material resources required to respond to a WMD incident on the installation. Transportation support is required to move all assets, both human and materiel, in response to a WMD incident. This includes the ability to protect the means and the operators during the response support. A CBRNE environment shall increase the importance of alternative modes and routes. This makes centralized movement control imperative. Based on incident and intelligence reports regarding contaminated routes, it may be necessary to divert supply convoys or use alternate routes for evacuation.

C11.6.4.8. Mass Care. The purpose of mass care is to coordinate efforts to provide sheltering, feeding and emergency relief supplies following a CBRNE incident. The provision of emergency shelter for disaster victims includes the use of pre-identified shelter sites in existing structures; creation of temporary facilities such as tent cities, or the temporary construction of shelters; and use of similar facilities outside the disaster-affected area, should evacuation be necessary. There may be a need to provide food to victims and emergency workers. This can be done through a combination of fixed sites, mobile feeding units, and bulk food distribution.

C11.6.4.9. Public Works. Public works should ensure all facilities remain operational if possible, ensure damage is remedied or mitigated, and ensure full recovery of affected elements in a timely manner to allow for the recovery of the installation.

C11.6.5. It is highly recommended that the installation planners prepare a Response/Synchronization Matrix. The Response/Synchronization Matrix consists of response measures that must be carried out in response to a WMD incident by each functional area. These measures shall be developed into action sets. Since there are no WMD-specific measures, Commanders, civilian equivalents, and installation planners must create their own. For the purpose of the plan, planners must create both pre-incident and post incident measures. The end product of a completed synchronization matrix is a comprehensive picture of all actions occurring (often simultaneously) during pre-incident and post-incident. An example of a Response/Synchronization Matrix is at Table C11.T5.

**Table C11.T5 Example Response/Synchronization Matrix**

| WMD RESPONSE FUNCTION | WMD MEASURES | WMD ACTION SETS | WMD COORDINATION REQUIRED |
|---|---|---|---|
| WMDRF #1 Information & Planning | | | |
| MOA/MOU | | | |
| Pre-Incident | Baseline the installation for WMD Response; identify required equipment for WMDRFS 1-9; identify resources available through augmentation. | The Installation Commander shall use the Antiterrorism Working Group (ATWG) to assess the installation's ability to respond to a WMD incident. This assessment shall address shortfalls and vulnerabilities. The installation director of support shall obtain equipment required for WMD incident response. | The installation director shall coordinate with WMDRF leads for equipment<br><br>Coordinate with WMDRF #2-9 leads for content requirements |
| | Establish MOA/MOUs with Host Nation government and WMD response elements. | The installation Chief of Staff (CoS) or administrative equivalent, shall determine from each installation WMDRF lead the desired content of each MOA/MOU; write the MOA/MOUs; staff/coordinate the content with command legal, and applicable civilian agencies and provide staff oversight for formalization of agreements. | Coordinate and sign MOA/MOUs with local Host Nation government. |
| | Monitor MOA/MOU status periodically to ensure support is available to respond to WMD incident. | The installation CoS or administrative equivalent, in conjunction w/each WMDRF lead shall conduct a semiannual review of each WMDRF for sufficiency and update, as necessary. | Coordinate with WMDRF #2-9 leads for changes in content requirements.<br>Update MOA/MOUs with local Host Nation government. |
| | Request funds for unprogrammed requirements | Once coordination is complete with external elements, the CoS or administrative equivalent shall identify at the remaining shortfalls and report these shortfalls to the | |

| WMD RESPONSE FUNCTION | WMD MEASURES | WMD ACTION SETS | WMD COORDINATION REQUIRED |
|---|---|---|---|
| | | applicable service's higher headquarter as unprogrammed requirements. | |

C11.6.6. The matrix above is only an example. Each installation must prepare its own action sets and coordination based on the installation's Combatant Commander/Service/DoD Agency specific requirements, structure, expertise, location and resources. Reference (aa) provides greater details on the Response/Synchronization Matrix.

# C12. CHAPTER 12
# TERRORIST INCIDENT RESPONSE MANAGEMENT

## C12.1. INTRODUCTION

C12.1.1. Terrorist Incident Response Management is a sequence of command, staff and first responder actions to respond to a terrorist incident or other unique event and restore AT capability. The primary objective of Terrorist Incident Response Management is to limit the effects and number of casualties resulting from a terrorist attack. Commanders develop response measures to save lives, preserve health and safety, secure and eliminate the hazard, protect property, prevent further damage to the installation and maintain public confidence in the installation's ability to respond to a terrorist incident.

C12.1.2. A Commander's responsibility to enforce security measures and to protect persons and property is paramount during any level of conflict. As such, it is incumbent upon the Commander to plan for, and be capable of reacting to a terrorist attack. If the attack involves a chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) device, the number of casualties and the extent of the areas involved may quickly overwhelm organic resources. This situation is covered in more detail later in section C12.6.

C12.1.3. This Chapter addresses management of a terrorist incident. The focus of incident management is on the organic assets of an installation, ship, or base and the ability to cope with the situation using organic assets until outside assistance arrives. Reference (e) requires all commanders to prepare installation-wide terrorist incident response measures and include them in the AT plan. The terrorist incident response measures should include procedures for determining the nature and scope of incidence response; procedures for coordinating security, fire, and medical first responders; and steps to reconstitute the installation's ability to perform AT measures.

C12.1.4. There are an unlimited number of potential terrorist incidents requiring a response. Developing separate courses of action for each is an unrealistic task. To prepare for the most probable, or likely threats, AT Plans should address (at an absolute minimum) each potential threat identified through the TA Process.

C12.2. TERRORIST INCIDENT MANAGEMENT PLANNING

C12.2.1. The establishment of a mechanism to respond to a terrorist incident is an essential element of the DoD CbT Program. Normally, the installation, base, or unit commander identifies an office or section, or designates personnel from various sections, who act as the principal planning agency for special threats and who comprise the Emergency Operations Center (see paragraph C12.3.4.) during an actual crisis. One effective method for determining what areas should comprise the planning and execution of the response is to use the WMD response functions.

C12.2.2. There is no requirement to have a separate terrorist incident management plan. However, reference (e) requires that the AT Plan address terrorist incident response measures. Appendix 5 identifies items that should be considered for inclusion into the crisis management plan.

C12.3. INITIAL RESPONSE

C12.3.1. Onset of a Terrorist Incident: The onset of a terrorist incident begins with the detection of an unlawful act of violence or threatened violence. Detection may result from routine surveillance performed by an installation or facility intrusion detection system, guard or security force, or aware DoD-affiliated persons. Once detection of a criminal act occurs, first responding security or law enforcement personnel must perform an initial assessment.

C12.3.2. Initial Response Force

C12.3.2.1. On-duty Security Forces/Military Police patrols or guard personnel usually provide initial response to a terrorist attack. The initial response force is usually under the control of the on-scene senior officer or noncommissioned officer assuming responsibility. At facilities controlled by the Defense Agencies, the initial response force may be under the control of a senior civilian security or DoD law enforcement official. Once the initial response force has responded to the incident and determined the circumstances, the installation Commander should activate required forces and begin notification procedures for military and civilian authorities.

C12.3.2.2. The initial response force should immediately identify and report the nature of the situation, isolate the incident, and contain the situation until relieved by the reaction force commander. Initial response force actions are critical. Each shift of the daily security force must

have trained personnel who are aware of the threat and are capable of reacting promptly to any new development.

C12.3.2.3. For example, if the attack is a bombing, ambush, assassination, or firebombing, the terrorists may escape before additional forces arrive. In these cases, the initial response force should provide medical aid, seal off the crime scene, and secure other potential targets in case the initial attack was a diversionary tactic. If the event is a hostage/barricade situation, the initial response force should seal off and isolate the incident scene to ensure no one enters or leaves the area. The initial response force must also be prepared to locate witnesses and direct them to a safe location for debriefing. For foreign incidents, the initial response force must also be prepared to interface with host nation police or military forces that may also be responding to the incident.

C12.3.3. Installation/Base Commander

C12.3.3.1. The installation/base commander, depending upon established SOPs should activate the installation's EOC. Additionally, the commander should notify specialized response forces, and immediately report the incident to the appropriate superior military command EOC, military investigative agency, FBI, civilian authorities, and if a foreign incident, to host nation authorities and the U.S. Embassy, as required.

C12.3.4. The Emergency Operations Center (EOC)

C12.3.4.1. The EOC serves as the command post at a predetermined location. Communications are established immediately with the initial response force containing the situation, the specially trained operational response force preparing to take over or augment the initial response force, and other critical participants as pre-designated in the EOC's SOPs. There are usually three standard secure communications circuits: command net (administrative matters, support, routine traffic), tactical net (operations), and intelligence net. If necessary, a dedicated net for negotiations may be necessary if a landline cannot be established with the terrorist.

C12.3.4.2. The EOC should distribute responsibilities into four basic functions:

C12.3.4.2.1. Operations. Responsible for First Responders (fire, security, and medical); hazardous materials; bioenvironmental; safety; and public affairs (PA).

C12.3.4.2.2. Logistics. Responsible for service (communications, power, food) and support (shelters, supplies, etc.).

C12.3.4.2.3. Planning. Responsible for amending and developing plans to address the changing circumstances.

C12.3.4.2.4. Administration. Responsible for tracking personnel casualties or fatalities, notifications, report, and contracting services as necessary.

C12.3.5. Confirmation

C12.3.5.1. Since jurisdiction depends on whether the incident is terrorist related, it is important for the response force to identify the type of incident as quickly as possible. If the FBI or host nation assumes control, then the response force must be prepared to coordinate the operational handover and assist as needed.

C12.3.5.2. The initial or specialized response forces may be required to provide outer perimeter security as well as be prepared to manage the entire event. They must also be prepared to turn over responsibility for resolving the incident to host government security forces if overseas or the FBI if within the United States and in the event that the FBI seeks to exercise jurisdiction over the containment and resolution phases of the incident. These installation/base forces must always prepare for the most resource-demanding contingency. This level of readiness requires considerable sustainment training.

C12.4. FOLLOW-ON RESPONSE

The response to a terrorist incident varies depending on the nature and location of the incident. Generally there are three distinct phases through which an incident may evolve although many incidents do not develop beyond the first phase.

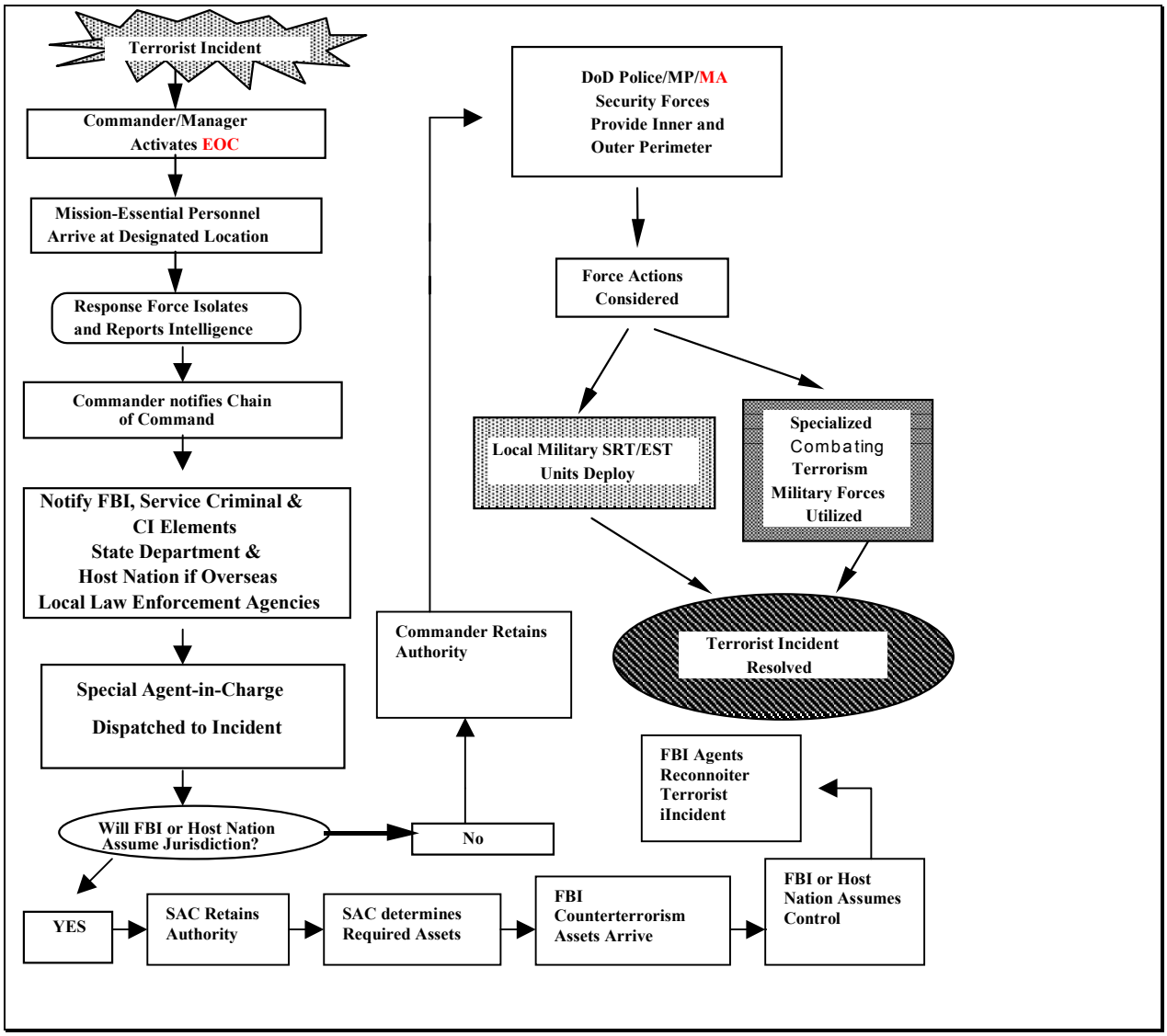
C12.4.1. Phase I: Locally Available Resources. Phase I is the commitment of locally available resources, including available Security Forces/Military Police patrols or guards and available backup units. Civilian contract guard services should not be used as part of an initial response force for a terrorist incident unless there is no Federal law enforcement or Security Forces/Military Police available. Civilian contract guard services should generally be restricted to perimeter security duties, traffic control, and crowd control activities. Ideally, all law enforcement or security personnel are familiar with local SOPs for terrorist incidents and have practiced these procedures as part of their unit-training program. They must be prepared to secure, contain, and gather information at the scene until the beginning of Phase II. While securing and containing the incident scene, response forces must be alert to the fact terrorist incidents often include diversionary tactics. The evacuation of threatened areas is a high priority function.

C12.4.2. Phase II: Augmentation of Initial Response Force. Phase II is the augmentation of the initial response force by additional law enforcement/security personnel and/or a specially trained response force, such as Special Reaction Team (SRT)/Emergency Service Team (EST), FBI hostage rescue teams, or host nation tactical units. On many installations, the initial response force and the augmentation force are essentially the same. This phase begins when the EOC is activated. During this phase, either the FBI or the host nation may assume control jurisdiction over the incident. If that occurs, installation forces must be ready to support the operation. The installation specially trained response force must be ready for employment in this phase of the operation. In any country that a terrorist incident against an American facility/unit occurs, the DOS and the U.S. Embassy shall play the key role in coordinating the U.S. Government and host country response to such an incident.

C12.4.3. Phase III: Commitment of Counter-Terrorist Resources. Phase III is the commitment of a specialized the FBI, the Department of Defense, or host nation counter-terrorist force. In this phase steps are taken to terminate the incident. Incident termination may be the result of successful negotiations, assault, or other actions including the surrender of the terrorists. Because identifying the terrorists, as opposed to the hostages, may be difficult, it is important that the capturing forces handle and secure all initial captives as possible terrorists.

C12.4.4. Response Sequence. Figure C12.F1. shows a typical response sequence to a terrorist incident. It addresses the straightforward case within the exclusive jurisdiction of the United States, its territories, and its possessions; where the DoD Components perform all three phases of terrorist incident crisis management—initial response, containment, and crisis resolution. Also, it shows the process to those instances overseas, where SOFA permits the DoD Components to manage terrorist crises on their own authority. The following section addresses those situations in which host Governments or the FBI assume responsibility for managing the containment and resolution phases of a terrorist incident.

**Figure C12.F1. DoD Management of Terrorist Incident**




## C12.5. TERRORIST INCIDENT RESPONSE: SHARED AUTHORITIES AND JURISDICTIONS

C12.5.1. It is customary and usual for military commanders and civilian managers to assume responsibility for initial response, containment, and resolution of criminal incidents that occur on DoD facilities within the United States, its territories, and its possessions. The FBI has lead agency responsibilities for investigation and prosecution of alleged violations of U.S. Code that occur on DoD installations or within DoD facilities. It also has the responsibility for

investigating those incidents that an installation commander declares to be "terrorist" in nature. In addition, the FBI has lead agency responsibilities for investigation and prosecution of individuals alleged to have violated Antiterrorism Act of 1990, Pub. L. 101-519, Sec. 132, November 5, 1990 (reference (ae)) by committing prohibited acts against Americans abroad.

C12.5.2. DoD installation military commanders and civilian managers have responsibility and authority for making an initial response, containing, and resolving criminal incidents occurring within their installation. If needed they may ask the FBI for assistance if the FBI has superior tactical assets available, such as regional SWAT or Hostage Response Teams (HRT).

C12.6. INITIAL RESPONSE TO A CBRNE ATTACK

C12.6.1. Installations have the requirement for an immediate response capability to ensure critical mission continuity and save lives during a CBRNE incident and to mitigate the situation (see reference (ad)). National-level responders may not be immediately accessible or available to respond to an installation's needs. Therefore, each installation must plan for the worst-case scenario by tailoring its response for each functional area, based on its organic resources and available local support through MOAs/MOUs. The situation may dictate that the installation not only conducts the initial response, but also sustains response operations.

C12.6.2. In the event of a terrorist CBRNE incident, the commander should direct the following complementary sets of actions:

C12.6.2.1. Activate the installation's initial response elements and local MOAs/MOUs.

C12.6.2.2. Initiate the DoD notification process; and

C12.6.2.3. Request resources to augment the installation's response capabilities.

C12.6.3. Installation commanders are responsible for ensuring their first responders have a plan and are equipped, trained, and exercised on the plan for responding to an incident involving CBRNE.

C12.6.4. Installations are required to have incident management plans. One effective way to develop these plans is by the use of WMDRFs. As detailed in Chapter 11, the WMDRFs parallel the national-level FEMA Emergency Support Functions (ESFs) to the greatest degree possible. This parallelism shall ensure that if there is a need for Federal assistance, incoming support can easily transition into the appropriate functional areas on the installation. The Installation Antiterrorism Program and Planning Tool (IPPT) uses the WMDRFs to systematically address each of the installation response functional areas. From these Response Measures, the

installation planners should create installation specific action sets or implementation instructions. These action sets should include who, what, when, where, and how the lead staff element shall carry out the response measure. Once planners have carefully prepared discrete actions sets, it is recommended they be placed in a response matrix.

C12.6.5. Terrorist CBRNE incidents, or threats of terrorist CBRNE acts, may overwhelm an installation's minimum capability to adequately detect, assess, or contain the threat. The Department of Defense, like most other local, State, or Federal entities, has neither the authority nor the expertise to respond unilaterally to all aspects of terrorist CBRNE threats or acts. The tenets of the National Response Plan shall help an installation develop its response based on crisis and consequence management.

C12.7. SPECIAL CONSIDERATIONS DURING CRISIS RESPONSE

C12.7.1. Establishing Communications. A crucial aspect of implementing the AT plan is establishing secure communications among the forces in the incident area and the EOC. Once this is done, all other elements of the communications plan are activated. Communications personnel must be able to respond to changing needs during the incident and be able to maintain, over a prolonged period, the communications channels included in the AT plan.

C12.7.2. Evidence. Although the primary goal is ending a terrorist incident without injury, another goal is the successful prosecution of terrorists. Witness testimony, photographic evidence, etc., are important in achieving a successful prosecution. Maintaining the continuous chain of custody on evidence obtained during an incident requires documenting the location, control, and possession of the evidence from the time custody is established until presenting the evidence in court. Failure to maintain the chain can result in exclusion of the evidence. Types of evidence for which the chain must be established include, but are not limited to:

C12.7.2.1. Photographs taken during the incident.

C12.7.2.2. Physical evidence, including any item(s) used by the terrorists.

C12.7.2.3. Tape recordings of conversations between terrorists and hostage negotiators.

C12.7.2.4. Demand notes or other messages recorded by written, audio, or video means prepared by the terrorists.

C12.7.3. Disposition of Apprehended Personnel. Apprehended military personnel must be handled according to Service regulations and applicable installation SOPs. In the U.S., civilian detainees must be released to the FBI or U.S. Federal Marshals for disposition. In foreign

incidents, civilian detainees may be processed according to the SOFA, diplomatic note (DIPNOTE) or other agreements with that particular country. The Staff Judge Advocate (SJA) should be consulted prior to releasing any individual to Host Nation authorities. In coordination with the SJA, an after-action report should be prepared within 7 working days after termination of the event.

C12.7.4. Reports. Reporting to higher headquarters is an important element in any special threat or terrorist situation. Each Service and command have a reporting procedure that requires a timely report of the incident to higher military authorities. The crisis management plan should dictate required reports and timelines for notification. An after-action report should be prepared within seven working days after termination of the event. This should include all staff journals and other documentation to include detailed information concerning disposition of evidence and captured individuals. The SJA and law enforcement personnel should ensure this report is in sufficient detail to meet prosecution requirements.

C12.7.5. PA. Principal PA objectives of a terrorist incident crisis management plan are to ensure accurate information is provided to the public (including news media) and to communicate a calm, measured and reasonable reaction to the ongoing event.

C12.7.5.1. PA programs should attempt to:

C12.7.5.1.1. Identify terrorist activities, as criminal acts not worthy of public support.

C12.7.5.1.2. Reiterate U.S. policy on terrorism that identifies all terrorist acts as criminal acts, mandates no concessions to terrorists, refuses to pay ransom, and isolates those nations identified as encouraging, supporting or directing terrorism; and

C12.7.5.1.3. Support DoD PA strategy on releasing information pertaining to antiterrorism plans, operations, or forces involved in antiterrorist operations.

C12.7.5.2. The DOJ has lead PA responsibility for incidents occurring on U.S. territory if the FBI assumes jurisdiction for resolving the incident. The Office of the Assistant Secretary of Defense (Public Affairs) (OASD (PA)) supports the DOJ in providing specific PA support.

C12.7.5.3. When U.S. military security or combating terrorism forces are employed, the Department of Defense provides a spokesman for dealing only with security or combating terrorism forces military operational matters.

C12.7.5.4. The DOS coordinates PA during terrorist incidents overseas. The DOS may delegate the PA responsibility to a designated DoD representative.

C12.7.5.5. The OASD (PA) is the single point of contact for all PA aspects of U.S. military CbT actions. While there is no mandatory requirement to release information, installation commanders are advised to exercise prudent judgment on such matters and coordinate actions through PA channels, to OASD (PA).

C12.7.5.6. When the EOC is activated, it should include the activities of the PAO and media center. The media center should be located in a separate location away from the EOC. The PAO shall prepare media releases and conduct briefings at the media center during the incident. The PAO shall use information obtained from EOC activities. PA shall coordinate with EOC personnel, and clear all information with the commander, prior to release. The PAO must be fully knowledgeable of the situation as it develops. The media representatives should not have direct access to hostages, hostage takers, communications nets, or anyone directly involved in a terrorist incident unless the PAO has cleared such contact with the EOC. DoD experience with media representatives has shown that bringing them in early under reasonable conditions and restrictions commensurate with the risk and gravity of the event, providing them thorough briefings, maintains DoD credibility and preserves freedom of information. Refer to Chapter 19 for additional PA guidance.

C12.7.6. Immediate Post-Incident Actions. During the immediate post-incident phase, medical and psychological attention, along with other support services, should be given to all personnel involved in the operation, including captured terrorists. A final briefing should be given to media personnel; however, they should not be permitted to visit the incident site. Because of the criminal nature of the terrorist event, the site must be secured until the crime scene investigation is completed by the appropriate investigative agency. It is also imperative to record every action that occurred during the incident.

# C13. CHAPTER 13
# EXERCISING THE ANTITERRORISM PLAN

## C13.1. INTRODUCTION

C13.1.1. Preparing for AT exercises is an important task that requires dedication and planning. Exercises are conducted to give leaders, staffs and personnel realistic experiences to better accomplish their wartime or special mission tasks. Realistic exercises allow personnel to be placed in fluid environments where critical decision making is practiced to broaden experience base and to identify areas or plans that need improvement. Reference (e) directs that Commanders at all levels shall conduct field and staff training to exercise AT plans, at least annually. Additionally, the standard requires the following portions be exercised, at a minimum; AT Physical Security measures, Terrorist Incident Response measures, and Terrorist Consequence Management measures. Exercising AT plans is an important part of an AT Program as it provides the following benefits:

C13.1.2. Assists the organization/installation to maintain operational readiness.

C13.1.3. Provides the organization with a means to document and measure operational readiness.

C13.1.4. Validates capabilities identified in plans.

C13.1.5. Confirms adequacy of training.

C13.1.6. Provides a means to assess and identify vulnerabilities and resources.

C13.1.7. Demonstrates a commitment to continuous AT improvement.

C13.1.8. Increases antiterrorism awareness.

C13.1.9. Provides a means to identify and prioritize needed force protection resources.

C13.1.10. Enables all participants to fine-tune their respective applicable skill-sets.

C13.2. TYPES OF EXERCISES

C13.2.1. AT exercises are similar in planning, preparation, execution and evaluation to other training events and exercises conducted by our services at the unit/installation level. These types of exercises include Tabletop, Drills, and Full-Scale exercises and generally increase in level of involvement and cost.

C13.2.2. Tabletop Exercises. Also known as a rock drill, this type of AT exercise involves the key leaders and staff officers of an organization or installation gathered in one room or area. It is a scenario driven discussion led by a facilitator and can be used to exercise specific portions of an AT plan or the entire plan itself. This type of exercise, depending on the scenario, can be one hour or last a full day. A tabletop exercise should be used when an AT plan is new, as refresher training, or to familiarize new leaders with the AT plan.

**Figure C13.F1. Players start a tabletop exercise.**

C13.2.3. Drills. Drills are collective training events that focus on selected functions, procedures, or portions of an AT plan. Example portions of an AT plan that can be exercised to achieve limited objectives are command post exercises, notification drills, first responder drills, or evacuation drills. Drills are scenario driven events usually limited to specific organizations or functions in order to test, assess and validate specific portions of a plan. These also can last anywhere from 1 to 8 hours, or even longer, if necessary.

**Figure C13.F2. Security Forces conduct a drill.**

C13.2.4. Full-Scale Exercise. A full-scale exercise is the most complex of AT exercises and most likely shall involve the entire organization and installation as the installation AT plan is exercised. For many key organizations and tenant units, this training event shall be the major focus of training for the days and weeks leading up to the event as units shall activate portions or all parts of their AT plan. The day-to-day functions of the installation shall most likely be impacted. To ensure a successful full-scale exercise, commands are encouraged to conduct a tabletop exercise and appropriate drills prior to conducting a full-scale exercise. This exercise requires the most planning and should be used to validate the AT plan and timelines, assess functional capabilities and skills, and test equipment. This type of exercise can be as long as several days.

C13.3. PREPARING FOR AN EXERCISE

C13.3.1. A successful AT exercise, like any other exercise or training event, requires thorough planning. Commanders and their staffs should use their service specific doctrine to plan an AT exercise. It is important to plan the training event far enough in advance as to ensure it is de-conflicted with other mission requirements, deployments, and training events. If the event is to achieve worthwhile training objectives, the Commander must be involved in key decision points in the planning process, the first of which is to get the training event(s) placed on the long range training calendar.

C13.3.2. Characteristics of an AT Exercise.

C13.3.2.1. Successful tabletop and full-scale AT exercises are threat scenario driven, guided by white hat controllers, and have Commander involvement and support.

C13.3.2.2. Drills may or may not have a threat scenario depending on which function or portions of an AT plan are being exercised. Commands must examine which key functions or portions of an AT plan are key tasks needing to be

**Figure C13.F3. Observers/Controllers discuss an exercise with player personnel.**

exercised. They must then ensure tenant organizations, staffs, or subordinate units have properly trained and equipped those organizations to accomplish their tasks using their service specific training methodology. Drills are excellent tools to train and evaluate those key functions and to validate that portion of the plan.

C13.3.2.3. Observer/Controllers (O/C). O/Cs are key players during exercises and should be identified and trained prior to the event. O/Cs should be able to move about freely during an exercise, to ensure participants stay focused on the scenario, abide by the exercise rules, and assist in meeting the exercise objectives. In playing the role of the white hat, O/Cs shall be in an excellent position to capture lessons learned and facilitate the AAR process.

C13.3.3. Design of the AT Exercise. In order to have a successful AT exercise, commanders and planners should gather a planning team, designating an officer in charge. This team should receive commander's guidance to develop the scope of the exercise, and the training objectives. Once the objectives are determined, the team should develop a work plan with milestones to accomplish the preparation. The format of the exercise, with corresponding staff and organizational responsibilities should be tasked as early as possible in order to allow time to prepare for success. It is very important to plan the assessment process and means during the planning stages so that shortcomings can be identified and improvements can be tracked and accomplished.

C13.3.4. Scenario Development. The operations officer and intelligence officer need to work together to develop a realistic scenario which shall set the conditions to achieve the training objectives. The threat scenario must be realistic and pertinent to the local threat assessment. Participation of the local law enforcement community is essential. DoD and civilian law enforcement can make significant contributions to scenario and threat development. Ensuring valuable AT injects are developed is probably the most important task for the identified action officer during the planning phase so that the training audience experiences a fluid operation requiring key AT staffing and decisions by leaders. The current threat assessment should be utilized to develop a realistic scenario. For full-scale exercises, commands should consider a Red Team to fill the role of a terrorist organization. Identifying the Red Team early is also critically important so that they can properly prepare and train for the event.

C13.3.4.1. The scenario development phase should produce several products, including a narrative, a timeline, and injects. Injects can be in many forms, some of which are messages, phone calls, radio calls, or even physical actions. Creativity limited by realism during the inject development process shall lead to a well thought out, challenging, and worthwhile exercise.

C13.3.4.2. Once the vision for the exercise has been established, making it happen is the next step. This requires a great deal of logistics and administrative coordination and is essential to the success of the exercise. The staging of the event may require resources not normally on-hand or may require initiative to acquire. Arrangements for rooms, vehicles for O/C and key leaders, along with other white hat requirements need to be locked in. Staging of events and the logistics associated with a "terrorist act" need to be considered and planned for. Visual/audio support, access control to key O/C areas, and the control cell set up should be arranged. Finally, it is important to plan for basic items such as food, water and latrine facilities for players and O/Cs. All of these requirements should be tasked to subordinate organizations or staff.

C13.3.5. The scenario should be articulated into a well-written exercise directive, with identified purposes of clear, focused tasks with pre-defined evaluation criteria. The directive shall be the foundation of the exercise and must be produced far enough in advance for units to digest, plan and train to ensure the exercise is worthwhile.

C13.3.6. Once the scenario and directive have been developed, planners should create an exercise manual. It should contain the schedule, the scope, objectives, inject timeline/implementation schedule, ground rules and Rules of Engagement (ROE). It should also contain scenario materials, contact information for key leaders and participants, the exercise directive that task organizations and units, and any other forms and records needed. Injects and some scenario materials should not be available to player units or the exercise shall lose realism. As such, portions of this manual should become close hold documents, available only to key leaders, planners, and white hat O/Cs.

C13.3.7. Preparation for the exercise is completed when the staff prepares sufficient copies of exercise manuals and briefing material needed to conduct the exercise.

C13.4. CONDUCTING THE AT EXERCISE

C13.4.1. Exercises shall have many players. The Exercise Coordinator who is the head O/C, the other O/Cs, player units, and role players or Red Teams are key players. The Exercise Coordinator has overall responsibility for running the exercise and monitors the pace of events according to the scenario. The O/Cs observe individuals, and unit or staff players to ensure objectives are being met and to assess player responses to the scenario to compare against expected responses and the pre-defined evaluation criteria. The O/Cs should also assist in tracking AAR comments.

C13.4.2. Before the exercise starts several briefings need to occur to get everyone's head in the game. Players need to be briefed on the scope of the exercise the rules for the exercise, safety and the roles of the controllers. Control cells need to be briefed and trained to run injects by message, phone, simulators, or other pre-determined means. Finally, role players need to understand when their roles start, end and the purpose of their role-playing event.

C13.4.3. Once the briefings are accomplished, it is time to start the exercise. The injects should be initiated according to the timeline and monitored by the Exercise Controller. He shall need assistance in keeping track of time so players are continually challenged. The planned timeline may need to be slowed down or even sped up, as necessary, to keep the players constantly involved and engaged. A real AT event shall be extremely engaging and the exercise should attempt to simulate those conditions. The AT exercise ends when all injects have occurred, player units have accomplished responses, and the training objectives have been met.

C13.5. EVALUATING THE AT EXERCISE

C13.5.1. The evaluation phase actually begins concurrently with the exercise. O/Cs and players should continually be noting and tracking AAR comments for consideration later. After the exercise, each echelon should conduct its own "hotwash" to capture lessons learned and AAR comments. If the exercise lasts more than one day it is usually a good idea to have a hotwash at the end of each day.

C13.5.2. O/Cs should be responsible to facilitate the hotwash for each organization. To do so, they need to take notes throughout the day so that they capture observations, and data collection where appropriate, to use in analysis, and a written report later.

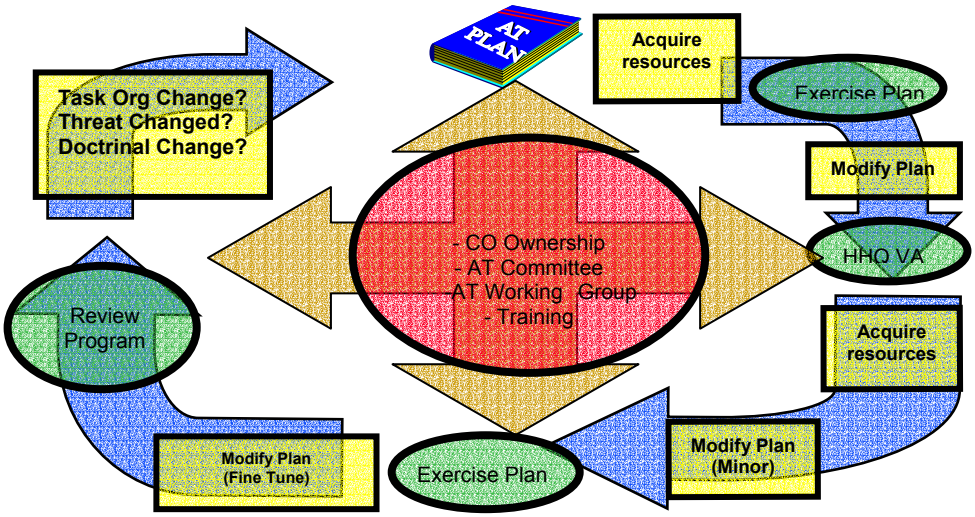
C13.5.3. The Exercise Controller is responsible to collect all O/C input for the exercise AAR. The AAR is where significant execution shortcomings of the exercise and scenario should be identified, discussed, and a concept plan of action to fix each item developed.

C13.5.4. A formal AAR should be held with all key leaders and staff present to review the issues developed for discussion. Participants should be encouraged to speak freely at this discussion to gather the best ideas that shall remedy identified shortcomings. Resource shortages should be identified, as well as procedural problems.

C13.5.5. Once the formal AAR is complete, the exercise staff officer should prepare a written AAR, complete with milestones and suspense dates to complete required retraining, revision of the AT plan, and resource acquisitions.

C13.5.6. This exercise process shall yield great benefits. Exercises are part of the AT program life cycle depicted below. They assist in improving the AT plan, in acquiring resources, reviewing a program and increasing awareness. Arguably, conducting an exercise is the best way to enhance installation or organization AT programs and plans throughout the life cycle. Figure C13.F4. portrays the AT program life cycle.

**Figure C13.F4. Life Cycle of the AT Exercise Program.**



# C14. CHAPTER 14

# ANTITERRORISM ASSESSMENTS

## C14.1. INTRODUCTION

Global terrorism has become a high profile concern within the DoD since the Khobar Towers terrorist bombing in 1996. The September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon indicate that U.S. national security and our military forces are increasingly vulnerable to the transnational threat of terrorism. People, mission-related facilities, and the support infrastructure are all at risk.

C14.1.1. In response to terrorism, each Combatant Commander/Service is mandated to develop an AT VA capability as prescribed by reference (a).

C14.1.2. VA help determine the vulnerability of a facility to a terrorist attack and identifies areas of improvement to withstand, mitigate or deter the attack.

C14.1.3. This Chapter describes the three types of assessments available to the installation commander:

C14.1.3.1. Joint Staff Integrated Vulnerability Assessments (JSIVAs).

C14.1.3.2. Combatant Commander/Service Integrated Vulnerability Assessments (IVAs).

C14.1.3.3. Local Vulnerability Assessments (LVAs).

## C14.2. JSIVAS

C14.2.1. The Chairman of the Joint Chiefs of Staff, as the principal military advisor to the Secretary of Defense for AT issues, is tasked to assess the DoD Component policies and programs. To accomplish this task, the Chairman of the Joint Chiefs of Staff executes the JSIVA program through the DD AT/HD Division.

C14.2.2. The Combatant Commanders and Services are required by reference (a) to assess their installations and AT programs to reference (e) standards. Combatant Commanders and Services can request JSIVAs to meet their assessment responsibilities. DD AT/HD allocates

assessments based upon threat, mission of the installation, and criticality. Specially tailored JSIVAs are performed when requested by the Combatant Commanders, as contingencies require.

C14.2.3. JSIVA teams provide independent assessments to assist the Commanders in meeting AT responsibilities. JSIVA teams identify installation vulnerabilities and present options (procedural and programmatic) for the Commanders to mitigate those vulnerabilities. The ultimate goal of a JSIVA is to assist commanders in enhancing the AT programs.

C14.2.4. In response to USS COLE and Government Accounting Office (GAO) report findings, the scope of the JSIVA process shall be expanded to include higher headquarters, strategic sea and airports, and the Joint Chiefs of Staff exercises.

## C14.3. COMBATANT COMMANDER/SERVICE INTEGRATED VULNERABILITY ASSESSMENTS (IVAS)

C14.3.1. Combatant Commander/Service Level AT Vulnerability Assessments. Reference (e) standards outline higher headquarters level AT Vulnerability Assessments. The team composition and individual member duties remain the responsibility of each Combatant Commander/Service. Reference (e) states, "Combatant Commanders and/or Military Departments and/or Services and/or DoD Agencies shall ensure lower level AT programs receive a Higher Headquarters Vulnerability Assessment at least once every 3 years to ensure unity of AT efforts throughout their AORs or subordinate commands.

C14.3.2. To provide essential visibility, commanders shall prioritize, track, and report vulnerabilities identified during vulnerability assessments to the next general officer/flag officer or equivalent. Note that Higher Headquarters Vulnerability Assessments satisfy the annual requirement for a Local Vulnerability Assessment.

## C14.4. LOCAL VULNERABILITY ASSESSMENTS (LVAS)

C14.4.1. Local Vulnerability Assessments. Reference (e) standards outline Local Vulnerability Assessments as follows, "Local Commanders shall conduct a local Vulnerability Assessment for facilities, installations, and operating areas within their area of responsibility. The Local Vulnerability Assessment shall address the broad range of physical threats to the security of personnel and assets and shall be conducted at least annually".

C14.4.2. The DTRA AT/FP Vulnerability Assessment Team Guidelines is an excellent tool available to help conducting vulnerability assessments. This tool is a comprehensive checklist that incorporates reference (e) guidelines and produces a product similar to DTRA's JSIVA.

C14.5. ASSESSMENT AREAS

C14.5.1. Assessment Areas. According to reference (e) standards, a vulnerability assessment shall address the following areas:

C14.5.1.1. AT Plans and Programs. The assessment shall examine the installation AT program and its ability to accomplish appropriate standards contained in reference (e) and those established by the appropriate Combatant Command, Service, or DoD Agency.

C14.5.1.2. Counterintelligence, Law Enforcement Liaison, and Intelligence Support. The assessment shall focus on the installation's ability to receive threat information and warnings from higher headquarters and local resources, actively collect information on the threat (when permitted and in accordance with applicable law and regulations), process that information to include local fusion and analysis, and develop a reasonably postulated threat statement of the activity. Further, the assessment shall examine the ability to disseminate threat information to subordinate commands, tenant organizations, assigned to or visiting DoD personnel (including military members, civilians, and contractor employees, and dependents), and how that process supports the implementation of appropriate force protection measures to protect military personnel, DoD civilians and family members.

C14.5.1.3. AT Physical Security Measures. The assessment shall determine the installation's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying, or defending against acts of terrorism. Physical security techniques include procedural measures such as perimeter security, security force training, security surveys, medical surveillance for unnatural disease outbreaks, and armed response to warning or detection as well as physical security measures such as fences, lights, intrusion detection devices, access control systems, closed circuit television cameras, personnel and vehicle barriers, biological, chemical and radiological agent detectors and filters, and other security systems. The assessment should also consider commercial-off-the-shelf (COTS) AT technology enhancements and potential

solutions for those circumstances where existing technology or procedural modifications are inadequate.

C14.5.1.4. Vulnerability to a Threat and Terrorist Incident Response Measures. The assessment shall examine the installation's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices, to include WMD. The assessment shall further examine the ability to provide structural or infrastructure protection against terrorist events. The ability to respond to a terrorist event, with emphasis on a mass casualty situation, shall also be examined.

C14.5.1.5. VAs for Terrorist Use of WMD. The assessment shall assess the vulnerability of installations, facilities, and personnel within their AOR to terrorist use of WMD, to include the potential use of CBRNE.

C14.5.1.5.1. The assessment shall examine written plans and/or programs in the areas of counterintelligence, law enforcement liaison, intelligence support, security and post-incident response (the ability of the activity to respond to a terrorist incident, especially a mass casualty event, to include a disease outbreak caused by terrorist use of biological weapons).

C14.5.1.5.2. The assessment shall focus on the most probable terrorist threat for the facility and appropriate countermeasures. In cases where no identified threat exists, units shall be assessed on their ability to implement AT measures under increasing FPCONs in response to an increase in the Terrorist Threat Level or terrorist threat warning.

C14.5.1.5.3. The assessment shall examine the availability of resources to support plans as written and the frequency and extent to which plans have been exercised. The assessment shall also examine the degree to which plans complement one another and support the assessed unit's ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate AT measures and provide an appropriate response should a terrorist event occur.

C14.5.1.5.4. Host Nation, Local Community, Inter-Service, and Tenant Support. The assessment shall examine the level and adequacy of support available to the activity from the

host nation, local community, and where appropriate, inter-service and tenant organizations to enhance force protection measures or respond to a terrorist incident.

C14.5.1.5.4.1. The assessment shall determine the status of formal and informal agreements with supporting organizations via MOU or MOA, Inter-Service Support Agreements, Host Tenant Support Agreements, or other models.

C14.5.1.5.4.2. The assessment shall determine the integration and feasibility of plans with the host nation, local community and inter-service and tenant organizations to provide security, law enforcement, fire, medical and emergency response capability in reaction to a terrorist event with emphasis on mass casualty situations.

C14.5.1.5.4.3. The assessment shall determine the adequacy of resources available to execute agreements and the extent and frequency to which plans are exercised.

C14.5.1.6. Team Composition and Level of Expertise. As a minimum, the level of expertise and team composition must support the assessment of the functional areas described above. Team membership shall have expertise in the following areas: physical security; civil, electrical, or structural engineering; special operations; operational readiness; law enforcement and medical operations; infrastructure, and intelligence/counterintelligence. In exceptional cases, Commanders may be required to tailor team composition and scope of the assessment to meet unique requirements of a particular site, but must meet the intent of providing a comprehensive assessment.

C14.5.1.6.1. Specific size and certification of expertise shall be as directed by the Combatant Commander and/or Service and/or DoD Component creating the team. However, team members must be functionally orientated and have experience in the assessment area to be considered for team membership.

C14.5.1.6.2. Based on site specific factors such as Terrorism Threat Level, terrorist characteristics, geography and security environment, assessment teams may be augmented by personnel with expertise in the areas of linguistics; chemical, biological, radiological weapons effects; AT technology; Explosive Ordnance Disposal; special warfare; communications; information assurance or operations; and other specialties as determined by the Combatant

Commander and/or Military Departments and/or Service and/or DoD Agency sponsoring the assessment.

# C15. CHAPTER 15
# ANTITERRORISM (AT) PROGRAM REVIEW

## C15.1. INTRODUCTION

C15.1.1. This Chapter is designed to assist installation or unit AT Program managers in performing an AT Program review. In order to be successful, an AT program must be implemented in a methodical, coordinated manner. Although your installation or unit may already have some elements in place, all program areas should be reviewed thoroughly on at least an annual basis. It cannot be stressed enough that the AT Program is the ultimate responsibility of the commander or, in the case of a DoD Agency, the civilian equivalent. As such he and/or she has the authority and responsibility to alter or add to the AT program as deemed necessary to accommodate the local situation. The AT Program elements described below are merely the minimum recommended issues that should be addressed.

C15.1.2. It is not the purpose of this Chapter to supplant the guidance provided by appropriate OSD/Chairman of the Joint Chiefs of Staff/Service/Combatant Commanders directives, but to complement them by illuminating the grand strategy that should govern the development of installation AT Programs.

C15.1.3. Essential Program Elements. References (a and d) defines essential elements of an AT Program. These elements are:

C15.1.3.1. All the elements and assessments of the Risk Management process.

C15.1.3.2. Planning.

C15.1.3.3. Training and exercises.

C15.1.3.4. Resource generation

C15.1.3.5. Program Reviews.

C15.2. RISK MANAGEMENT PROCESS.

C15.2.1. TA Standards. Reference (e) standards, as highlighted below, provide guidance for conducting a threat assessment. Although multiple standards are identified, they each contribute to the overall TA process. Chapter 5, "Terrorist Threat Assessment," provides a detailed discussion of recommended processes to conduct Terrorist Threat Assessments.

C15.2.1.1. Development of AT Standards.

C15.2.1.2. Coordination in Overseas Locations.

C15.2.1.3. Application of DoD Terrorism Threat Analysis Methodology.

C15.2.1.4. Threat Information Collection and Analysis.

C15.2.1.5. Threat Information Flow.

C15.2.1.6. Potential Threat of Terrorist Use of WMD.

C15.2.2. TA Development. In order to develop a site-specific TA that satisfies reference (e) standards, ATOs should refer to Combatant Commander/Service directives supplementing this document. Consider using the J-34 Installation Antiterrorism Program and Planning Tool (IPT) as it shall facilitate what would otherwise be an extremely time consuming process. The tool assists directly in the development of the installation's AT Plan, using pre-incident FPCON measures and post-incident response measures—providing a methodology for implementing the explicit guidance found in reference (e).

C15.3. CRITICALITY/VULNERABILITY/RISK ASSESSMENTS

C15.3.1. Assessment Standards. Chapter 6, "Criticality Assessment," Chapter 7, "Vulnerability Assessment," and Chapter 8, "Risk Assessment," provides detailed discussions on recommended processes on conducting these assessments. Much like the Threat Assessment, multiple reference (e) standards address conducting VA and program reviews. Some standards are program centric while others focus on VAs. These standards are:

C15.3.1.1. Comprehensive AT Program Development, Implementation, and Assessment.

C15.3.1.2. ATOs.

C15.3.1.3. AT Program Review.

C15.3.1.4. VAs of Installations.

C15.3.1.5. Pre-deployment AT Vulnerability Assessment.

C15.4. PLANNING

C15.4.1. Planning Standards. Reference (e) provides guidance for the development of AT-related plans. Some standards deal with the specifics of plan writing, while others address FPCON issues. FPCONs are actually a derivative of the Operations and Intelligence fusion process. The following highlighted standards affect the AT planning process:

C15.4.1.1. Development of FPCONS.

C15.4.1.2. FPCON Measures Implementation.

C15.4.1.3. Threat Response Measures.

C15.4.1.4. Comprehensive AT Program for AOR.

C15.4.1.5. Terrorism TA.

C15.4.1.6. Physical Security Measures.

C15.4.1.7. Terrorism Incident Measures.

C15.4.1.8. Terrorist Consequence Management.

C15.4.2. Planning Integration. The J-34 Installation Planning Tool, particularly Part III, provides an integrated approach to fulfilling the requirements of the above standards.

C15.5. TRAINING

C15.5.1. Training Standards. Reference (e) provides guidance for the conduct of AT-related training to include eligibility, course content for training levels I through IV, and requirements for High Risk Personnel. The individual standards are:

C15.5.1.1. General requirements for AT Training.

C15.5.1.2. Level I AT Awareness Training.

C15.5.1.3. AOR Specific Training Requirements for All DoD Personnel.

C15.5.1.4. Level II ATO Training.

C15.5.1.5. Training for High Risk Personnel and High Risk Billets.

C15.5.2. Filling In the Gaps. The DoD AT Standards give a reasonably complete picture of training requirements. The following discussion provides further analysis of the training process and the selection of a training source.

C15.5.3. Analyze Training Requirements. Training is absolutely vital to the success of any AT program. The requirements for Level I and II training are fairly straightforward. In AT, success rests on the foundation of awareness. However, some supporting skills, such as how to conduct an assessment, constitute a hidden set of necessary training. ATOs must take an exacting look at the current inventory of skills, determine which are needed and develop a strategy to close the gap.

C15.5.3.1. Training Strategy Development. The solution is to let your AT working group do the development work. This solution shall make use of their varied expertise as well as giving them ownership of the strategy. Instead of imposing the training externally, this approach allows for a process of internal adoption. From an organizational viewpoint, this shall greatly speed the rate at which training occurs.

C15.5.4. Leverage AT Training and Expertise. The most obvious source of Level II trained personnel is your Service school. However, other options can be found in the toolbox. Cost and availability figure most heavily in selecting the supplier for each category. Quite often, organizations like the Interagency OPSEC Support Staff shall conduct MTTs at your location to train large numbers of individuals at a relatively low cost.

C15.6. EXERCISES

C15.6.1. Exercise Standards. Commanders at all levels are required to exercise their AT plans at least annually.

C15.6.2. Incremental Approach. Success is often achieved through steady, incremental progress (crawl before walking, walk before running). With this mindset, it is wise to begin by

conducting staff exercises. Although the exercise requirement is an annual one, during the initial phases of a program, you may have to conduct a separate staff exercise, a communications/logistics exercise, and a field exercise all in 1 year. Remember that AT Plans ARE NOT considered to be valid or executable until they have been exercised. However, there is no requirement to exercise AT plans in a vacuum. AT scenarios/injects can be incorporated into a larger exercise in order to extract the maximum training benefit for all concerned.

C15.6.3. Psychological Effect. An active exercise program can create an impression of strength. Remember that people react to their perceptions as though they are reality. Terrorists are no exception. If terrorists can see that the US is prepared for their attacks, they shall shift their efforts elsewhere, thus fulfilling your AT Program's goal of deterring terrorist acts.

C15.6.4. Identifying Shortfalls. Exercises Identify Resource Shortfalls. This presupposes a mechanism for capturing lessons learned. Once the command identifies shortfalls, the process of covering the gaps can begin. The answer shall not always be an external provision of additional resources. Often, the answer shall be the reprogramming of internal resources.

C15.6.5. Joint Exercises/Operations. Nearly all combat operations, now and in the future, shall be joint operations. Unless our forces practice AT procedures during joint operations to resolve interoperability issues, soft spots shall be created. Since terrorists specialize in asymmetric attacks, failure to conduct joint AT exercises is a high-risk proposition.

C15.7. RESOURCE GENERATION

Chapter 16, "Resource Requirements and Funding Sources," provides a detailed description of the minimum essential elements of generating resource requirements for AT Programs. AT Program reviews shall include an assessment of the following:

C15.7.1. Generating requirements.

C15.7.2. Documenting resource requirements.

C15.7.3. Prioritizing resource requirements.

C15.7.4. Funding sources.

C15.7.5. Unfunded requirement submissions.

C15.8. PROGRAM REVIEWS

VAs support the AT program review by identifying shortfalls in the program itself. Areas to focus the assessment should include, but not be limited to, the following:

C15.8.1. AT Plans and Programs.

C15.8.2. CI, Law Enforcement Liaison, and intelligence support.

C15.8.3. AT Physical Security Measures.

C15.8.4. Vulnerability to a Threat and Terrorist Incident Response Measures.

C15.8.5. VAs for Terrorist Use of WMD.

C15.8.6. Host Nation, Local Community, Inter-Service, and Tenant Support.

# C16. CHAPTER 16
# RESOURCE REQUIREMENTS AND FUNDING SOURCES

## C16.1. OVERVIEW

C16.1.1. From the perspective of many terrorists, there is little difference between installations or activities owned, operated, and manned by DoD civilian personnel, military personnel, or contractor personnel. The goal of an AT program is to protect military service members, the DoD civilian workforce, family members, facilities, and other vital mission-related assets from terrorists. In order for an AT program to obtain this goal, it is essential to ensure resources are available to execute the AT plan and achieve the four over-arching objectives to deter, detect, defend, and respond. However, generating resource requirements and acquiring additional resources to mitigate identified vulnerabilities is an important step in the solution to reducing risk. It is imperative to continue to educate and increase AT awareness; engage with the local community for assistance and information; follow, implement, and improve existing security tactics, techniques and procedures; and maximize protective benefits from existing resources. The AT plan must be complete and effective, a TA conducted, critical assets identified, and a higher Headquarters VA conducted assessing current AT plan/program effectiveness for these critical assets against identified threats. Once threat, asset, vulnerability, and AT effectiveness information is gathered, data needs to be analyzed, and the likelihood of the threat and the nature and scope of potential harm to all assets (people and facilities) assessed. This analysis lays the foundation for resource determination and risk management.

C16.1.2. Once resources are determined to be necessary and an unacceptable level of risk exists, it is important to ensure appropriate resources (manpower, operations, and equipment) are available to execute the AT plan and achieve the four objectives mentioned above. However, before activities/installations/units can successfully compete and acquire these resources, requirements must be documented, well defined, prioritized, and clearly articulated. Once AT requirements have been established and appropriately documented, there are two principal avenues to obtain funding for required resources. The first is the DoD PPBE process. The second source of funding is through the Combating Terrorism Readiness Initiatives Fund (CbT RIF) designed to quickly provide funds to the Combatant Commanders for the purpose of emergency or emergent high-priority CbT requirements.

C16.2. GENERATING REQUIREMENTS

C16.2.1. To assess resource requirements, the development of an executable AT plan is critical. It is important to identify and document in the plan who, what, when, where, and how resources are needed to mitigate AT threats and vulnerabilities. Given limited resources and budgetary constraints, the plan should provide commanders with alternatives for timely, cost-effective remedies to allow for tradeoffs. A well designed, integrated systems approach is essential to achieving these tradeoffs. A typical physical security systems approach should include resources capable of performing early threat and weapons detection, classification and assessment, delay, communications, and response. The physical security measures should be a combination of active and passive systems, devices, and personnel. All these resources are necessary to protect designated security interests from possible threats.

C16.2.2. Once the AT plan is complete, a TA conducted, and critical assets identified, a VA must be conducted to determine the vulnerabilities of critical assets given the organization's current AT effectiveness with regard to manpower, policy/procedures/plans, equipment, and training/exercises. During integrated vulnerability assessments, a higher headquarters vulnerability assessment team (Joint Staff, Combatant Commander, Component Command or Service) shall provide both procedural and programmatic recommendations to mitigate vulnerabilities and reduce risk. The programmatic recommendations should not translate directly into a resource requirement. Based upon the analysis conducted by the unit/installation, it is the Commander's decision, with the assistance of a working group, to determine how to address these recommendations. Implementing, changing, or adding tactics, techniques, and procedures may or may not mitigate the risk. Either way, it is understood there is no zero-risk environment, and it is the commander's decision to determine if the risk is acceptable, how to address the issues, and resources that are necessary.

C16.2.3. Once threat, asset, vulnerability, and AT effectiveness information is gathered, the data must be analyzed to assess the likelihood of the threat and the nature and scope of potential harm to all assets (people and facilities). This analysis lays the foundation for risk management - the selection and implementation of effective and affordable security measures that meet prioritized security requirements. Once this analysis is complete, the plan is exercised, lessons are learned, and the level of risk identified, then it is time to determine if additional resources are required and appropriately document them. If additional resource requirements are necessary, the suitable resource must be tied to the plan and requested in order to provide a higher level of protection to meet the AT plan's objectives for a successful AT program.

C16.2.4. AT resource requirements (manpower, operations, and equipment) should be identified for all levels of force protection conditions. First, it is essential that resources are obtained to meet the minimum-security requirements needed for the baseline (day-to-day FPCON) program. Since additional security measures are required for higher FPCONs, resource requirements should be identified for each higher FPCON, to achieve the required level of security. In identifying these resource requirements, it is important that AT working groups are involved in resource determination and prioritization. These working groups need to be comprised of members from all organizations involved in the AT Plan and Program (including the financial/resource manager/comptroller). They must have the appropriate information to adequately assess threats, vulnerabilities, critical assets, AT program deficiencies/current effectiveness, and risk. This information is imperative in determining where to appropriately allocate resources and funding and must be continuously documented.

C16.3. DOCUMENTING RESOURCE REQUIREMENTS

C16.3.1. Formally, continuously, and adequately documenting resource requirements is crucial in articulating, prioritizing, and justifying the need and effectively competing for the funding necessary to acquire the resource. A formal DoD requirements process has been established by OSD and implemented through the Department of Defense. The Services, OSD, and Joint Staff use this methodology to document and prioritize requirements for the PPBE process and CbT RIF. Activities/installations/units at the lowest level, needing additional resources, should be documenting requirements using this methodology and should be forwarding requirements through their chain of command to higher headquarters. The information required is essential for the activity/installation/units and higher headquarters to track, understand, articulate, and defend requirements to compete for funding. The omission or poor quality of the justification and impact statement is often the key cause for losing budget battles.

C16.3.2. Requirements are to be annotated using a prescribed excel spreadsheet format. This spreadsheet format is available through your Component and Service AT offices. It is important the installation/unit AT POC originating the request works with their resource or financial manager (RM/FM) to fill out the spreadsheet and provide all the pertinent data. The following information is required for the spreadsheet (refer to Table C16.T1.).

C16.3.2.1. Control Number. These control numbers should be filled out by the Components and are essential to forward with all requirements for any funding/requirements data call. This is the method used to track and identify the status of numerous unfunded

requirements. The numbers also allow Joint Staff, OSD, and the Services to track the history of the initial request back to the beginning of the requirement from year to year. Once the control number is established, it should not change and should stay with the project until the project is funded. The control number shall consist of four parts: code letter(s) to identify the Combatant Commander and Component, the fiscal year (last two digits of the year) the requirement was initially identified, and a sequence number. For example, the control number P-A-02-0001 is a PACOM (P) Army (A) requirement identified in fiscal year 2002 (02) for FY04 and is project #1 (0001).

C16.3.2.2. Service/Agency. The Service/Agency responsible for funding the requirement.

C16.3.2.3. Component. The Service component affiliated with the requirement.

C16.3.2.4. Location/FPCON. The location (city and country) of the activity/installation/unit and the FPCON level.

C16.3.2.5. Priority. Prioritize each requirement based upon the justification of the threat, vulnerability, criticality, the AT plan effectiveness, and the Commander's risk in accordance with the guidelines addressed in section C16.4. (prioritizing requirements). When prioritizing, it is important to consider the short and long term effects, affordability and supportability issues, and the cost-benefit impact on life-cycle costs such as manpower and maintenance.

C16.3.2.6. Requirement Title. Identify the program requirement and be as descriptive as possible to avoid confusion with other similarly named requirements (i.e. hydraulic barriers versus barriers).

C16.3.2.7. Requirement Description. Fully describe the program requirement. The description should at a minimum, include any applicable standards, regulations, plans upon which the requirement is based. Requirements are typically equipment, personnel, or maintenance type requirements.

C16.3.2.7.1. Equipment. Identify the resource requirement and the description and name with specific quantities and unit price if applicable. For more information regarding appropriate technology refer to the Chapter on technology.

C16.3.2.7.2. Personnel Requirements. Manpower includes requirements for either guards (contract, military or civilian) or management and planning (i.e. physical security officer, AT training officer).

C16.3.2.7.2.1. Guards. Identify the requirement as either contract guards, military or civilian manpower. If contract guards are required to reduce borrowed military manpower (BMM), then identify the number of BMM that the requirement shall reduce and the total BMM present. If military manpower is required, identify the number required, officer or enlisted, and associated grades. Provide a brief duty description for each (i.e. security guard, security administration personnel). Example: 50 military positions required for security guard positions (patrols, access control) - all enlisted, 25 sergeant (E-5) and 25 staff sergeant (E-6). If civilian personnel are required, identify by grade and the number required for each. Provide a brief duty description for each (i.e. security guard, security administration personnel). Example: 50 contract guard positions (patrols, access control) (10 supervisors, 40 guards).

C16.3.2.7.2.2. Management and Planning. Identify the requirement as a contractor, military manpower, or civilian (i.e. physical security officer, AT training officer). If a contractor is required, identify the number, and provide a brief description of responsibilities. If manpower is required, specify civilian or military, identify the number required, the ranks and grades for each, and provide a brief duty description for each (i.e. physical security officer, AT training officer). Examples: 25 security personnel (E-3) required for badge/administrative duties or 5 training personnel (GS-4) required to conduct level-I AT training.

C16.3.2.7.3. Maintenance Requirements. Identify the item for which maintenance is required and the cost/year. Identify the normal life expectancy of the item, the basis for the replacement, and a projected replacement date.

C16.3.2.8. Type IVA/Date. Identify how the requirement was identified and recommended (JSIVA, Service VA, Combatant Commander VA, MACOM/MAJCOM VA, self assessment, AT plan development, exercise), and the date (month/year) the assessment was conducted. If the requirement is for additional manpower, include how the manpower position was validated.

**C16.F1. Interrelationship and Categories for Appropriate Resource Justification.**


C16.3.2.9. Justification. It is important to continuously document and justify requirements in terms of the threat, asset criticality, current AT program effectiveness, vulnerability. Therefore, the justification is composed of the following four elements: TA, VA, Asset Criticality Assessment, and AT Plan/Program Effectiveness. This information and the interrelationship between the categories become the basis for the Commander's RA. The ultimate goal is to ensure appropriate justification is provided to acquire a resource that offers a high to moderate degree of protection and provides the capability to meet all or some of the objectives of the AT plan/program.

C16.3.2.9.1. Threat. Both the threat level (High, Significant, Moderate, and Low) and specific threat (e.g. chemical/ biological/ radiological/ nuclear or improvised explosive device (IED)) should be described for the location/ unit requesting the resource. This shall give the chain of command insight (based upon intelligence information) into the anticipated terrorist's operational capability, intentions, activity, and operating environment and an understanding of the magnitude of the threat.

C16.3.2.9.2. VA. Higher headquarter VA teams assess an organization's current AT program and its effectiveness against critical assets to identify vulnerabilities in protecting these assets. These vulnerabilities are typically linked to three areas: construction deficiencies, accessibility, and recognizability. Vulnerabilities need to be described in terms of these three applicable areas. This shall enable the chain of command to understand the magnitude of the vulnerability, and shall assist in determining the appropriate level of risk. Thoroughly describing the vulnerability is important for lower threat environments where emphasis and priorities are usually lower than in higher threat environments.

C16.3.2.9.3. Criticality of Assets. The criticality of assets (personnel, facilities, weapon systems, etc.) to be protected needs to be described with regard to its importance (asset value), the effect of an incident (ramifications to area/mission), and recovery (time to restore). Describing the criticality of assets in these terms shall assist in prioritizing resources to protect the most important areas and assets first.

C16.3.2.9.4. AT Program Effectiveness. Assessing the current AT program effectiveness is essential in determining if there are deficiencies in manpower, policy/procedures/plans, equipment, and training/exercises. All attempts should be pursued to change and improve tactics, techniques, and policy/procedures/plans, and training/exercises. Typically, if resources are required, deficiencies are identified in manpower or equipment. These deficiencies need to be described to explain why existing manpower and equipment resources cannot mitigate the risk.

C16.3.2.10. Commander's RA. A Commander, with the assistance of his staff/councils/working groups, should provide a risk assessment based upon the threat, asset criticality, the program's current effectiveness, and asset vulnerability information. This RA should address the likelihood of an incident happening and describe the impact if the resource is not provided.

C16.3.2.11. Program and Budget Execution Review. Services' Program and Budget Execution Review and the President's Budget typically include a CbT exhibit that identifies funding the Services have dedicated toward CbT. Service components shall forward a copy of

their CbT Annex to their AT staff in order to ensure Combatant Commander-level visibility over dedicated AT resources. There are seven AT categories that the Services must report to OSD (see DoD 7000.14-R (reference (af)) volume 2B chapter 19).

C16.3.2.11.1. Physical Security (PS) Equipment (blast mitigation, communications, explosive devices, barriers, intrusion detection, personal protection, other equipment/sensor, patrol/harbor boats, and High Mobility Multipurpose Wheeled Vehicles).

C16.3.2.11.2. PS Site Improvement (facility modifications).

C16.3.2.11.3. PS Management and Planning (personnel who manage PS programs, resources, and assets such as, but not limited to HQ staffs).

C16.3.2.11.4. Security Forces/Technicians (personnel and operating costs associated with protective forces used to safeguard assets, personnel, or information).

C16.3.2.11.5. Law Enforcement (all personnel and operating costs associated with law enforcement).

C16.3.2.11.6. Security and Investigative Matters (defense criminal investigative resources, security and any cross-discipline security functions).

C16.3.2.11.7. Research, Development, Test and Evaluation (includes activities at Defense Threat Reduction Agency and Counterterrorism Technical Support Group).

C16.3.2.12. Integrated Priority List (IPL). The IPL is the principal mechanism by which the combatant commanders communicate their views to the Secretary of Defense on the adequacy of the defense program. This newly revised and streamlined process is designed to bolster ongoing efforts to improve capabilities-based planning. The Combatant Commander's IPL now focuses on a succinct statement of key capability gaps that could hinder the performance of assigned missions. The focus of the IPL is expressed in terms of the capability required – not on a specific programmatic solution. The IPL uses the framework established by the Joint Staff for the Functional Capability Boards as described in CJCSI 3170.01C (reference (ag)). For each item on the Combatant Commander's IPL he has to answer four basic questions:

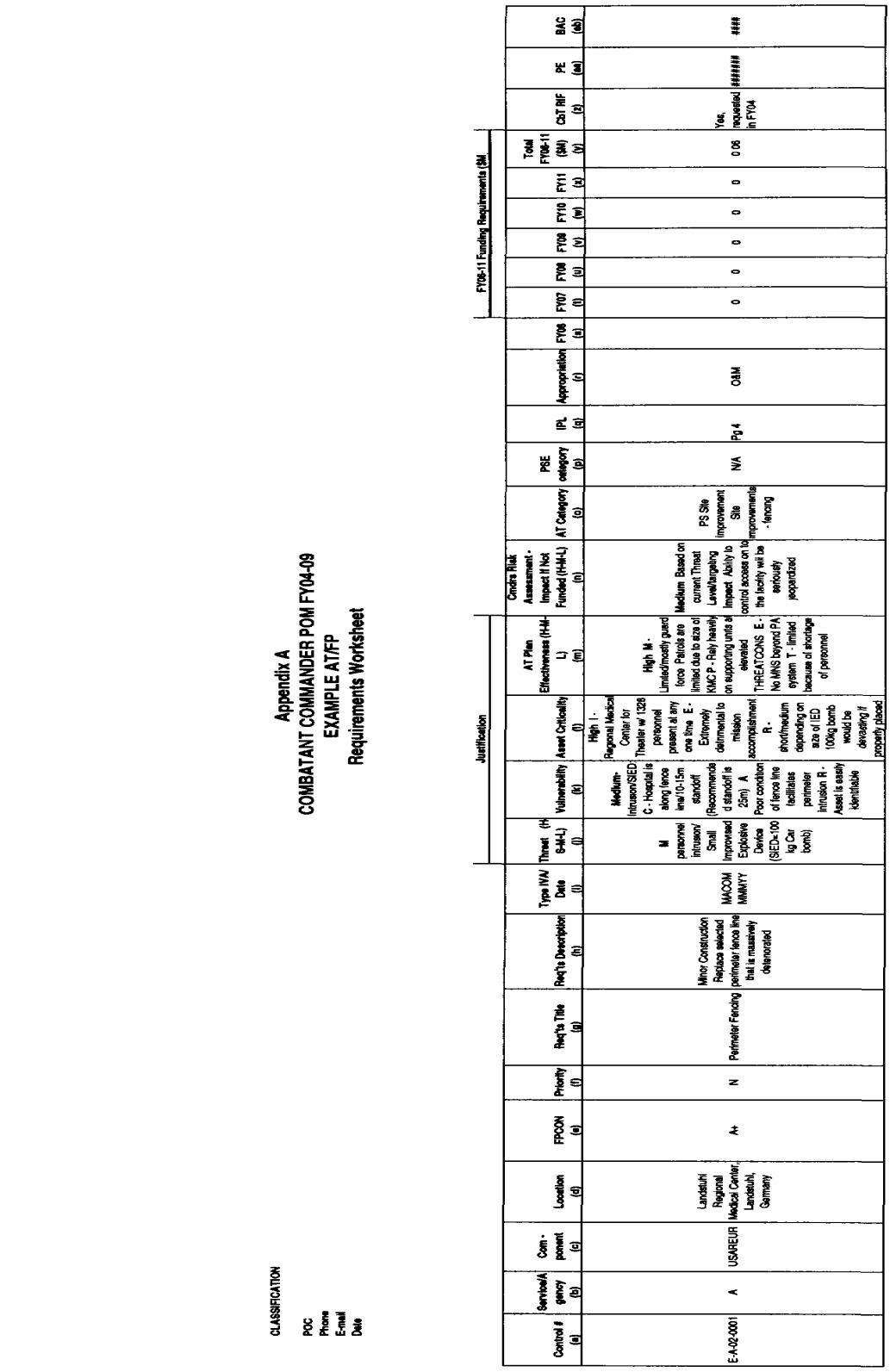
one, identify the current capability shortfall and the Joint Functional Concept it supports; two, cite the specific element of guidance (e.g. Contingency Planning Guidance, Security Cooperation Guidance, or Defense Planning) for which the capabilities fall short; three, describe the risks incurred by the capability shortfall using the Quadrennial Defense Review risk framework; and four, identify the extent to which the defense program mitigates the capability gap or shortfall. In addition to the IPL submission, the Combatant Commander is also required to brief the Secretary of Defense on their IPL's.

C16.3.2.13. Appropriation. The appropriation type must meet reference (af) guidelines and should be according to reference (ah) for MILCON projects. The activity/installation/unit resource/financial manager should determine the correct appropriation. Annotate the type of appropriation required that is associated with the funding and requirement: procurement, operations and maintenance (O&M), military construction (MILCON), or military pay. A requirement may have more than one appropriation type, for example if maintenance costs are associated with equipment purchase. The item to be purchased may require procurement funding and O&M funding to maintain the cost of the item in the future.

C16.3.2.14. Funding Requirement ($) by Fiscal Year (FY). The installation or unit resource/ financial manager should be involved along with the contracting and engineering staffs to determine the correct funding requirements. Annotate the funding requirement for each year in a dollar figure (dollars in thousands) for both the procurement of the item and the associated maintenance costs in the out years. Replacement and shelf life issues should be taken into consideration and annotated for future planning purposes.

C16.3.2.15. CbT RIF. If a CbT RIF request (See section C16.5.) has been submitted by the Combatant Commander to the Joint Staff per CJCSI 5261.01B,(reference (ai)), annotate this and the FY the request was submitted. CbT RIF is managed by the Joint Staff and is used to fund the Combatant Commander's (not Services or Agencies) emergency or emergent high-priority requirements in the year of execution. If a CbT RIF request has been submitted, indicating an emergent request, then an additional request for funding should be submitted to submitted to capture the follow-on costs.

**C16.T1. Example AT Requirements Spreadsheet**
**(Requirement Identified in FY02 for the FY04-09 PPBE Cycle)**



CLASSIFICATION

POC
Phone
E-mail
Date

Appendix A
COMBATANT COMMANDER POM FY04-09
EXAMPLE AT/FP
Requirements Worksheet

| | | | | | | | | Justification | | | | | | | FY08-11 Funding Requirements ($M) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Control # (a) | Service/Agency (b) | Component (c) | Location (d) | FPCON (e) | Priority (f) | Req'ts Title (g) | Req'ts Description (h) | Type IVA/ Date (i) | Threat (H-M-L) (j) | Vulnerability (k) | Asset Criticality (l) | AT Plan Effectiveness (H-M-L) (m) | Cmdrs Risk Assessment - Impact If Not Funded (H-M-L) (n) | AT Category (o) | PSE category (p) | IPL (q) | Appropriation (r) | FY08 (s) | FY07 (t) | FY08 (u) | FY08 (v) | FY10 (w) | FY11 (x) | Total FY08-11 ($M) (y) | CbT RIF (z) | PE (aa) | BAC (ab) |
| E-A-02-0001 | A | USAREUR | Landstuhl Regional Medical Center, Landstuhl, Germany | A+ | N | Perimeter Fencing | Minor Construction Replace selected perimeter fence line that is massively delaminated | MACOM MMMYY | M personnel intrusion/ Small Improvised Explosive Device (SIED)= 100 kg Car bomb) | Medium-Intrusion/SIED C - Hospital is along fence line/10-15m standoff (Recommended standoff is 25m) A Poor condition of fence line (facilitates perimeter intrusion R - Asset is easily identifiable | High I - Regional Medical Center for Theater w/ 1326 personnel present at any one time E - Extremely detrimental to mission accomplishment R - short/medium depending on size of IED 100kg bomb would be devasting if properly placed | High M - Limited/mostly guard force Patrols are limited due to size of KMC P - Rely heavily on supporting units a elevated THREATCONS E - No MNS beyond PA system T - limited because of shortage of personnel | Medium Based on current Threat Level/targeting Impact Ability to control access on to the facility will be seriously jeopardized | PS Site Improvement Site improvements - fencing | N/A | Pg 4 | O&M | | 0 | 0 | | | | 0.06 | Yes, requested in FY04 | ###### | ### |

C16.4. PRIORITIZING REQUIREMENTS

C16.4.1. Once requirements are generated and documented it is essential to analyze the justification data (threat, asset criticality, current program effectiveness, vulnerabilities, and commander's risk) and prioritize requirements focusing on the most critical and important needs first. Resources required to mitigate a major or a high risk situation should be given priority. Emphasis should be placed on acquiring resources to deter, detect, and defend, preventing the terrorist and threat from entering an area of significant importance. In addition, resources requirements necessary to meet minimal security requirements and to adhere to DoD or Service directives, standards, instructions, or regulations; should be given priority.

C16.4.2. To assist in the prioritization of resources, requirements should be placed into the following three categories of importance: 1 High Priority, 2 Medium Priority, and 3 Low Priority. (refer to Table C16.T2). It is recommended activities/installations/units employ working groups and councils to assist in this endeavor. This shall ensure working groups and councils responsible for making overarching decisions and recommendations to Commanders are aware of all the requirements, their significance, and the risks involved. In addition, it is not necessary for each criterion to be met within a specific category for the requirement to be identified as either 1 High, 2 Medium, or 3 Low. However, a majority of the criterion in the following table should be met.

C.16.4.3. Although a requirement is identified as a high/medium/low item/project, the resource must be affordable, supportable, reduce risk, and provide a high or moderate impact on the program to achieve the objectives identified in the AT Plan. Once the requirements have been prioritized and categorized, an acquisition strategy needs to be researched, requirements submitted, and funding sources sought.

**C16.T2. Criterion and Summary Descriptions for Prioritization Categories.**

| Criterion | 1 High | 2 Medium | 3 Low |
|---|---|---|---|
| **Typical % of Requirements** | ~10-20% | ~30-40% | ~50-60% |
| **Threat** | High-Significant | High to Moderate | All Threat Levels |
| **Asset Criticality** | Likely Target – Critical to Mission – High Impact – Significant (define significant in terms of time, e.g. hours, days) Time to Restore to Operations | Likely Target – Moderately Critical to Mission – Large # of People (define large in terms of numbers, e.g. >500) – Moderate Time to Restore to Operations | Asset Important to Mission – Wide # of People – Short Time to Restore to Operations – Redundant Capability exists |
| **Asset Vulnerability** | Significant/ Major Vulnerabilities – MILCON Standards not met – Weak Structural Protection– Extremely Accessible and Vital Recognizable Structures | Moderate Vulnerability – Accessible, Lacking Perimeter/ Access Control – Construction Protection Low – Recognizable Important and Lucrative Structures | Lower Vulnerability – Less Accessible, Enhance Perimeter/Access Control – Construction Protection Moderate – Less recognizable structures identified as vulnerable |
| **Current AT Plan/Program Effectiveness** | AT Program Ineffective/ Unexecutable – Resources Not Available for Baseline AT program or higher FPCON measures - No Other Mitigation Capability | AT Program Ineffective/ Unexecutable – Resource may be necessary to execute higher FPCON AT measures - Short-term mitigation capability available | Enhance/Improve AT Program - Resources available for FPCON baseline and baseline +1; however, may be necessary to execute higher FPCON AT measures - Longer-term mitigation capability available |
| **Commander's Risk** | Major / High Risk – Unacceptable Impact on Mission Readiness | Considerable/ Moderate Risk – Long-term Impact on Mission Readiness | Lower Risk – Short-term Impact on Mission Readiness |

C16.5. FUNDING SOURCES

C16.5.1. A realistic and affordable fiscal year budget and procurement strategy should be developed that captures all life-cycle costs (manpower needs, logistics/maintenance, replacement costs). The AT officer and the RM/FM/Comptroller should be working closely from the beginning to address these requirements. The AT officer is the expert responsible for

articulating and justifying the requirements and the RM/FM/Comptroller is responsible for identifying the correct appropriation and funding amounts, and submitting the funding requirement at the appropriate time to the affiliated agency/organization responsible for funding the requirement.

C16.5.2. Prior to submitting the requirement to higher HQ as an unfunded requirement, it is inherent upon the organization to assess the resource requirement against other organizational unfunded or funded requirements and determine if an internal reallocation of funding is appropriate and possible. If it is determined funding cannot be reallocated internal to the organization to fund the requirement; there are two potential funding options for the installation/unit to obtain funding.

C16.5.2.1. The first option is to leverage the PPBE process to compete for funding. Unfortunately, this doesn't address the need to fund requirements today, but to fund requirements in a minimum of two years from the year of execution. It is important to understand and use the PPBE process to obtain funding (information on the PPBE process can be found in Management Initiative Decision 913 (reference (aj)). However, this process does not guarantee that you shall receive funding. Adequately articulating and justifying requirements is crucial. Without thorough and proper justification, it is almost certain requirements shall not be addressed nor considered for funding. These requirements must compete with other higher HQ Service responsibilities and priorities. Even with well-documented justification it does not necessarily guarantee funding shall be provided because of this competition for limited funding; however, the unit's chances to effectively compete are substantially improved. In addition to properly documenting requirements, it is critical that requirements/funding information is provided on time and in the format requested. If this is not accomplished, then it appears the organization requesting the additional funding does not consider this a priority and therefore does not need the funding as much as another organization willing to do what it takes and follows directions.

C16.5.2.2. The second source of funding is through the CbT RIF. The purpose of the CbT RIF is to fund emergency and emergent high-priority combating terrorism requirements in the year of execution. The Joint Staff, DD AT/HD is the steward for this fund. CbT RIF

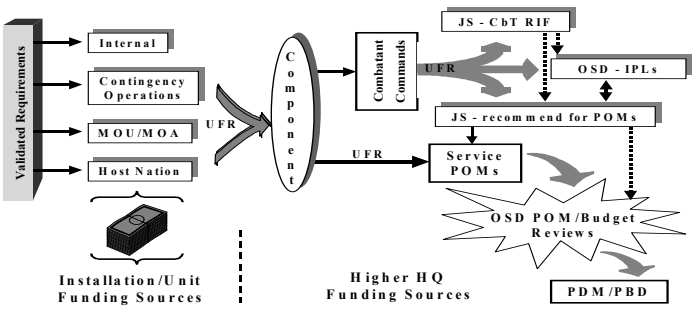
provides a means for the Combatant Commanders to react to unforeseen requirements from changes in a terrorist threat, threat levels, force protection doctrine/ standards, as well as unanticipated requirements identified as a result of VAs, tactical operations and exercising AT plans. If maintenance funds for CbT RIF projects are not programmed and provided from the parent Service, CbT RIF can be used to fund maintenance costs for those CbT RIF-funded items during the year of purchase and the subsequent year as a temporary measure to permit Services adequate time to program life-cycle costs. The fund is not intended to subsidize ongoing projects, supplement budget shortfalls, or support routine activities, which are a Service responsibility, and does not handle the majority of FP resource requirements.

C16.5.2.3. CbT RIF requests can only be submitted by the Combatant Commanders for their geographic area, AOR or for assigned forces. The Combatant Commanders must validate and forward CbT RIF requests for O&M and procurement funds to the Joint Staff, DD AT/HD in accordance with CbT RIF submission, approval, and reporting procedures in reference (ai). The use of CVAMP (appendix (2)) is required for submission of CbT RIF requests to the Joint Staff.

C16.6. UNFUNDED REQUIREMENTS SUBMISSION

C16.6.1. If it is determined funding cannot be reallocated internal to the organization to fund the validated, documented, and prioritized requirement, the unfunded requirement (UFR) must be forwarded to higher HQ (affiliated Service Component). Figure C16.F2. illustrates this process.

**C16.F2. Unfunded Requirements Submission Process.**



C16.6.2. If the Component is not able to fund the requirement(s), then the well-documented UFR(s) should be forwarded to both the Combatant Commander and Service AT staffs for consideration. The same requirement should be sent to both the Combatant Commander and the Services to ensure the Services are receiving the same requirements.

C16.6.2.1. The Combatant Commander staffs are responsible for consolidating UFRs and including them in the Combatant Commander's IPLs submitted to OSD in October through November. OSD and the Services provide guidance during the PPBE process. The Combatant Commander is also required to forward consolidated Component UFRs to the JS so they can coordinate and make priority recommendations to the Services (~ Nov–Dec) in preparation for the Services' next PPBE cycle. Combatant Commander staffs are also responsible for forwarding the Combatant Commander approved emergent or emergency UFRs to the JS to compete for CbT RIF funding.

C16.6.2.2. Service AT staffs shall assess and prioritize the well-documented UFRs provided by their Components and recommended by the Joint Staff. It is important that Services receive the appropriate mandated documentation using the specified format (refer to table C16.T1), so they can adequately champion and defend their Component's AT requirements throughout the Services corporate PPBE process. Services should ensure that funding requests are not duplicated through the two avenues (PPBE process and CbT RIF).

C16.6.3. OSD shall review the budgets proposed by the Services to meet AT objectives during the Program and Budget Execution Review (~ Jun–DEC). Unresolved issues and critical requirements may result in OSD program and funding direction to the Services and Agencies via a Program Decision Memorandum (PDM) and/or Program Budget Decision (PBD).

C16.7. AT OFFICER RESOURCE RESPONSIBILITIES

C16.7.1. Once designated as a member of the AT staff or as the single AT POC, the POC becomes the expert within the organization in generating, prioritizing, and appropriately documenting AT requirements. AT should be the primary duty of the designated person. If this is not feasible, service headquarters should request funding to hire civilian personnel to properly fill this requirement as per subparagraph C16.3.2.7.2.

C16.7.2. The AT POC is responsible for establishing and maintaining a formal documentation methodology documenting AT resource requirements in regard to threat, asset criticality, vulnerabilities, current program effectiveness, and commander's risk. Requirements must be continuously documented and ready for funding data calls for information.

C16.7.3. Once the requirements are documented, the information needs to be articulated and justified to the installation AT working groups, budget personnel, installation councils, and commander. These personnel should be involved in an appropriate risk assessment and determination as to whether funding should be provided within existing organizational funds; addressed through alternative means (e.g. sharing resources, procedural changes); requested through the chain of command as an unfunded requirement; or to do nothing and accept the risk.

C16.7.4. Work continuously with the programming, resourcing, and budgeting personnel to justify requirements and assist in determining the best source of funding and the associated data call timeline. Always expect a quick suspense with regard to funding and have requirements appropriately documented and available to never miss a suspense. Continuously forward AT requirements through the chain of command regardless of funding availability and always follow-up and track requirements status.

# C17. CHAPTER 17
# TECHNOLOGY

## C17.1. OVERVIEW

As the terrorist threat becomes more sophisticated, Tactics, Techniques and Procedures (TTPs) shall be hard pressed to be the only means to counter the threat. Technology can and should be used to augment sound TTPs in support of the program. Technology can also be a valuable tool for increasing the effectiveness of personnel while decreasing manpower requirements. The Department of Defense has several organizations that can assist in identifying an acceptable solution to a known requirement.

## C17.2. TECHNOLOGY

C17.2.1. Quite often when identifying AT requirements, Commanders do not know what technological solutions are available to fulfill AT resource shortfalls. There are organizations that can aid the Commander in identifying technology to satisfy these requirements: The Physical Security Equipment Action Group (PSEAG), the Technical Support Working Group (TSWG), and the Joint Non-Lethal Weapons Directorate (JNLWD). These organizations are separately funded to provide COTS, rapid prototyping, and research and development and/or evaluation of solutions for units in the field. They can provide information and research on technology and equipment evaluated and deemed suitable for your purpose. Additionally, they can provide field assessments to assist in identifying the optimal solutions to meet your requirements.

C17.2.2. The PSEAG objective under reference (ak) is to select or design, evaluate, and acquire the most efficient and productive security equipment at the most reasonable cost to ensure the effective protection of DoD resources, including personnel, classified information, material, and readiness. This Handbook established Service responsibilities in regards to management, operation, and support functions, including the responsibility for programming, budgeting, funding, and publication of standards, military specifications, design, and performance criteria for research and engineering. Listed in Table C17.T1. are Service responsibilities by category and the respective points of contact.

**Table C17.T1. Service Responsibilities and Points of Contact**

| CATEGORY | POINT OF CONTACT |
|---|---|
| • Interior Physical Security Equipment<br>• Lighting<br>• Tactical Security Equipment<br>• Barriers<br>• Personnel Alerting Systems<br>• Applicable Robotics | U.S. Army<br>Product Manager, Physical Security Equipment (PM-PSE)<br>Ft. Belvoir, VA<br>(703) 704-2412<br>www.monmouth.army.mil/smc/pmpse |
| • Anti-compromise Emergency Destruction Systems<br>• Waterside and Shipboard Security Systems<br>• Locks, Safes, Vaults, Seals, Containers & Related Delay Systems<br>• Applicable Robotics<br>• Explosive Detection | U.S. Navy<br>NCIS AT/FP Division (Code 24)<br>Washington Navy Yard, Washington D.C.<br>(202) 433-9138 |
| • Exterior Physical Security Equipment<br>• Access Control Systems<br>• Active Denial Technology<br>• Aerial Intrusion Detection Systems | U.S. Air Force<br>Electronic Systems Command (ESC)/ Force Protection Systems Program Office<br>Hanscom AFB, MA<br>(781) 377-5657<br>www.hanscom.af.mil/esc-fd |
| Note: The PSEAG web page is located at www.dodpse.spawar.navy.mil | |

C17.2.2.1. In order to better achieve the PSEAG objective, the COTS Working Group (CWG) was established to provide direct assistance and oversee the evaluation and integration of COTS equipment to support deployed forces. The CWG, chaired and operated on a daily basis by the Physical Security Branch of the DTRA in Alexandria, VA, consists of representatives from the four Services, DD AT/HD, DTRA, and advisory members from outside agencies. Commands may contact the CWG directly to receive Antiterrorism COTS equipment information or guidance, and discuss potential solutions directly with a working group representative. The toll free phone number is 1-800-811-7590 or DSN 221-0556.

C17.2.2.2. The Force Protection Equipment Demonstration (FPED) is held to provide leaders and decision-makers from the Department of Defense the opportunity to observe, and become familiar with Force Protection Equipment. The FPED provides unique opportunities for attendees to evaluate like pieces of force protection equipment under similar conditions and actually determine the relative merit of the demonstrated equipment.

C17.2.3. TSWG is the national interagency forum for research and development programs for CbT through rapid research, development, and prototyping. TSWG is comprised of nine subgroups consisting of: Chemical, Biological, Radiological, and Nuclear Counter-Measures; Explosive Detection; Improvised Device Defeat; Infrastructure Protection; Investigative Support and Forensics; Personnel Protection; Physical Security; Surveillance; Collection and Operations Support (which includes biometrics); Tactical Operations Support; and Training Technology Development. TSWG Agency members include the Department of Defense, DOS, Department of the Treasury, DOJ, DOE, Department of Health and Human Services, Department of Agriculture, Department of Commerce, Department of Transportation, and other agencies like the CIA, EPA, US Postal Service, and GSA - Federal Protective Services. The TSWG homepage is located at www.tswg.gov. Table C17.T2 lists TSWG points of contact by category.

**Table C17.T2. Technical Support Working Group Points of Contact**

| | |
|---|---|
| Chemical, Biological, Radiological and Nuclear Countermeasures | (703) 602-6203 |
| Explosive Detection | (703) 604-1684 |
| Improvised Device Defeat | (703) 604-1679 |
| Infrastructure Protection | (703) 602-6215 |
| Investigative Support & Forensics | (703) 604-1703 |
| Personnel Protection | (703) 601-4317 |
| Physical Security | (703) 604-1689 |
| Surveillance, Collection & Operations Support | (703) 604-1676 |
| Tactical Operations Support | (703) 601-4317 |
| Training Technology Development | (703) 604-1697 |

C17.2.4. JNLWD provides the most current and accurate information available on relative aspects of non-lethal technologies to the Services and other government activities requiring the use of restrained measures in the performance of their mission. They can provide recommendations regarding the application of Non-Lethal technologies on a global basis through a life-cycle perspective; including research, development, production, and deployment of those technologies. The JNLWD website is located at www.jnlwd.usmc.mil.

# C18. CHAPTER 18
# ANTITERRORISM TRAINING FOR DOD PERSONNEL

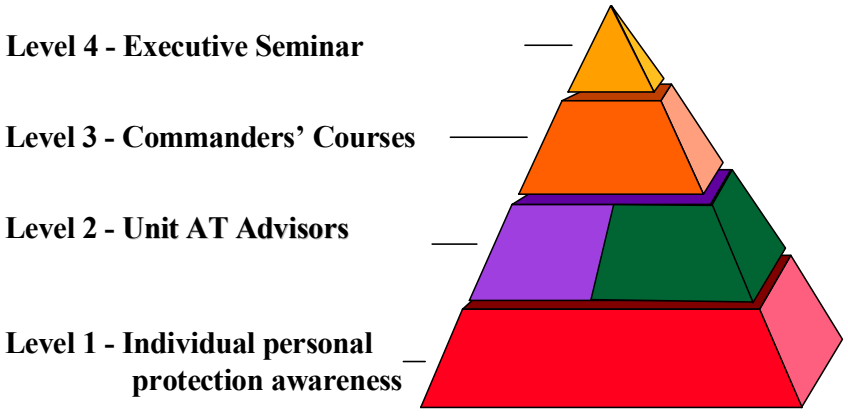
## C18.1. INTRODUCTION

The key to an effective AT program is to develop an awareness that is both sustained and reinforced from initial entry to termination of DoD service. DoD personnel must be aware of basic personal protective measures against terrorism, specific threats for the area they shall operate in or transit, and specialized training which their duty or position requires. References (a) and (e) direct the Services to incorporate and conduct antiterrorism training at all levels. The intent of this Chapter is to describe the general framework of the antiterrorism training program for all DoD Components.

## C18.2. GENERAL REQUIREMENTS FOR AT TRAINING

C18.2.1. The Chairman of the Joint Chiefs of Staff in consultation with the Commanders of the Combatant Commands, the Office of the Secretary of Defense, and the Military Departments, established requirements and minimum standards for antiterrorism training. These standards address personnel responsible for managing AT programs and training requirements for individuals, commanders, senior executive officers, high risk personnel and those assigned to high risk billets, and units preparing to deploy. Reference (e) outlines the minimum training standards and discusses specific training requirements.

**Figure C18.F1. Antiterrorism Training Concept**



C18.2.2. Level I Awareness Training. Individual security awareness and antiterrorism training are essential elements of an overall AT program. Each individual must share in this responsibility by ensuring the proper degree of alertness and employment of personal protection measures. AT awareness training begins immediately upon entry into service with the DoD and continues throughout the career of all DoD personnel.

C18.2.2.1. Awareness training requirements identify the target audience, frequency of training, who can administer training, and the qualifications necessary to provide the training. AT Officers (ATOs) play a principle role in managing this effort and for ensuring individual completion is recorded.

C18.2.2.2. In addition to providing training by a certified instructor, awareness training is also available through advanced distributed learning. Personnel may use this method to meet annual training requirements, provided Services, Combatant Commanders, or other commands have not established more stringent requirements. ATOs should contact their Component representative to obtain the web-site address.

C18.2.2.3. The Level I Awareness training requirement should not be confused with Area of Responsibility (AOR) specific training. Awareness training is conducted annually. For individuals traveling outside CONUS, in addition to completing the annual awareness training, they must also receive an AOR-specific update (see C18.4) within three months of travel.

C18.2.2.4. Individuals administering Level I training must be qualified to do so by attending a formal Service-approved Level II ATO Training Course. Commanders may qualify subject matter experts who have not attended a Service approved ATO course to administer Level I training. In the latter case, subject matter experts may be exempt from attending Level II training provided they receive AT and individual protection training that reviews current AT publications and identifies methods to obtain AOR-specific updates.

C18.2.3. Level II Antiterrorism Officer Training. Each installation and/or deploying unit (e.g., battalion, squadron, ship) must have at least one assigned ATO. Personnel identified as unit ATOs are responsible for managing the AT program, advising the commander on AT issues, and providing Level I Awareness Training. To help prepare individuals for ATO duty,

Component provided courses are available that incorporate the minimum training standards outlined in reference (e) into a program of instruction.

C18.2.3.1. Service-approved Level II ATO Training courses are listed in Table C18.T1. (not an all-inclusive list, users should check with their Service for the latest offerings). Several of these courses offer Mobile Training Teams.

**Table C18.T1. Service-Approved Level II ATO Training Courses**

| Service | Type/Location | POC |
|---|---|---|
| Army | Resident I US Army MP School, Ft Leonard Wood, M0[1] | DAMO-ODL (703) 695-8626 |
| Army | MTT / Various Locations[2] | FORSCOM (404) 464-5902 |
| Navy | Resident I EWTGLANT, Naval Station NW Annex, Chesapeake, VA | (757) 421-8059 |
| Navy | Resident I FLTRANCEN, San Diego, CA | (619) 556-7759 |
| Navy | MTT / NCIS MTTLANT, NAB Little Creek, VA[3] | (757) 462-8925 |
| Navy | MTT / NCIS MTTPAC, North Island, CA | (619) 545-8934 |
| Navy | Resident Navy Reserve, New Orleans, LA | (504) 678-7759 |
| Navy | Resident, Military Sealift Command, APMC Training Center, NJ | (732) 938-4979 (Ext. 17) |
| Air Force | Resident, ACC, Nellis AFB. NV | DSN 682-2772 |
| Air Force | Resident, AFRC, Robins USAFB, GA | DSN 497-0105 |
| Air Force | Resident, AFSOC, Hurlburt Field, FL | DSN 579-1856 |
| Air Force | Resident, AMWC, Ft Dix, NJ | DSN 944-4101, ext 187 |
| Air Force | Resident, USAFE, Sembach AB, GE | DSN 314-496-6383 |

1 The MP School will run MTTs if funding is provided.
2 FORSCOM is using the USAMPS P0I. They have a series of MTTs planned throughout CONUS
3 The Navy runs MTTs as needed using NCIS personnel from MTTLANT and MTTPAC

Units should use this training resource to satisfy individual and unit pre-deployment training requirements when timeliness or quota availability does not permit personnel from their units to participate in resident training programs. Component provided training taking place outside of these courses should continue to meet reference (e) training standards.

C18.2.3.2. Elements of an AT program include threat assessments, vulnerability assessments, planning, exercises, program reviews, and training. Instructions should relate to these elements to effectively prepare ATO's for their duties. It is understood that ATO's in many cases rely on other functional area experts to complete requirements within the overall AT program. ATO's should be familiar with the roles of other functional areas in order to manage their respective AT program.

C18.2.3.2.1. The minimum training standards identify several topics for instruction.

C18.2.3.2.1.1. The instructions should address overall ATO responsibilities and the role-played in AT program administration. The ATO should have a basic understanding of existing policy and standards and where to access information for reference. Appendix 9 offers sources for gathering AT information.

C18.2.3.2.1.2. Organizational structuring for AT highlights how units are structured to execute AT responsibilities. For example a discussion of FP Working Groups, Threat Working Groups, Intelligence Fusion Cells, and their roles in bringing together the various functional representatives may be appropriate.

C18.2.3.2.1.3. ATOs should fully comprehend the threat assessment process, to include actions taken to perform an assessment, the individuals responsible for those actions, and the application/usefulness of the assessment final product. ATOs should understand that the local threat assessment, as addressed in an AT program, is a different product than a country threat assessment produced by higher echelon intelligence organizations. This area of instruction should also include discussion of the following:

C18.2.3.2.1.3.1. DIA threat level methodology.

C18.2.3.2.1.3.2. Integration of intelligence , counterintelligence, and law enforcement functions via a threat working group-like cell.

C18.2.3.2.1.3.3. Importance of threat information flow throughout the chain of command.

C18.2.3.2.1.3.4. WMD threat.

C18.2.3.2.1.3.5. Need to conduct local threat assessments annually.

C18.2.3.2.1.3.6. Elements of a risk assessment.

C18.2.3.2.1.4. Vulnerability Assessments (VAs). ATOs should understand the baseline FP posture concept and the various requirements associated with vulnerability assessments such as local and Higher HQ VAs, the need for functional area expertise, what VAs examine, pre-deployment VAs, and where to obtain information regarding pre-deployment VAs from a geographic Combatant Commander.

C18.2.3.2.1.5. Executing the AT program using the terrorism threat assessment, developing FPCONs with site specific measures, and mitigating vulnerabilities through procedural and/or resource means.

C18.2.3.2.1.6. AT plan development, execution, review, and improvement. Instruction should inform ATOs on how to develop a plan, available tools to assist in plan development, WMD considerations, and development and use of a Random Antiterrorism Measures (RAM) program.

C18.2.3.2.1.7. ATO's should be familiar with current policy on resource management and the requirements generation process in support of the PPBE and the CbT RIF.

C18.2.3.2.1.8. As part of the overall AT program, training and exercises are management responsibilities of the ATO. Specifically, ATOs should know how to obtain AOR-specific information for deployment and travel areas. They should also understand that generally they are responsible for providing and tracking (or assisting the responsible organization with tracking) Level I training accomplishment of unit personnel. Additionally, awareness of the requirement to conduct annual AT exercises and associated responsibilities noted in current directives is appropriate.

C18.2.3.2.2. The minimum training standards require a review of several AT publications. A comprehensive review of reference (e) can serve as an advisory of all responsibilities and requirements. For example, effective program management should include awareness of AT roles in the logistics contracting process, facility and site evaluation criteria, selection and security of off-installation housing, high risk personnel training, and pre-deployment vulnerability assessments. This does not necessarily require the ATO to perform these functions, but advises him/her that the requirements exist and to ensure they are included in the overall AT program and planning process.

C18.2.3.2.3. Component directed modules serve to round out the minimum required training. Examples include introductions to AT, physical security and security design requirements, technology updates, first responder and emergency responder roles, consequence management, interagency roles, hostile intent decision making, issues relating to specific functional areas i.e. (e.g., legal, PAO), case studies, and component areas of interest.

C18.2.4. Level III Pre-command AT Training. Level III training for commanders shall be conducted at the O-5 and O-6 level by the Services in conjunction with pre-command training. The focus of this training shall be on the responsibilities discussed in the pertinent DoD 2000 series publications, Service publications, and associated joint doctrine.

C18.2.5. Chair Joint Chiefs of Staff Level IV Antiterrorism Executive Seminar. Executive level seminars conducted by the Joint Staff and tailored for an O-6 to O-8 audience. The focus of this training is to provide current updates, briefings, and discussion topics pertinent to an AT program. The training shall include, but not be limited to, AT simulations and war games. Level IV Seminars are held three times a year. The Combatant Commanders, Services, and DoD Agencies are responsible for nominating attendees. Individuals wanting to attend can make their desires known by forwarding a request through their respective Combatant Commander/Service/Agency channel.

C18.2.6. The Commanders should identify and assess the antiterrorism education and training status of the following categories of personnel to ensure that individuals are adequately trained to be reasonably protected against terrorist acts and to perform their assigned tasks:

C18.2.6.1. High-risk personnel or personnel assigned to high-risk billets.

C18.2.6.2. Personnel who provide expertise in AT activities, including installation, base, unit or ship Antiterrorism Officers; and

C18.2.6.3. Personnel responsible for specialized AT functions (e.g., planning, intelligence, special reaction teams, hostage negotiation, evasive driving, security engineering and other specialized schools).

C18.3. APPOINTMENT OF AT OFFICERS (ATOs)

ATOs shall be assigned in writing at each installation or base, as well as deploying organization (e.g., battalion, squadron, ship). The ATO shall be responsible for ensuring that each person within the unit is trained and fully aware of terrorist attack potential and methods to reduce the risk and mitigate effects should an attack occur.

C18.4. AOR-SPECIFIC AT TRAINING

C18.4.1. Geographic Combatant Commanders are responsible for protecting all personnel within their AOR except those for whom the COM has security responsibility. All DoD personnel and/or personnel under DoD sponsorship shall complete the prescribed AT awareness training within one year and specific AOR training within three months (refer to paragraph C18.2.2) prior to OCONUS travel. The Geographic Combatant Commanders shall make AOR-specific antiterrorism protection information available to military departments, supporting Combatant Commanders, and DoD components for this training. This can be accomplished through any means available to include messages, electronic bulletin board systems, Wide-World-Web pages, file transfers, or other appropriate communications.

C18.4.1.1. ATOs shall work with commanders and representatives from geographic Combatant Commands to develop training materials that address AOR-specific issues. Among topics to be addressed are the following:

C18.4.1.1.1. Specific terrorist groups, their history, tactics and techniques, and methods of operation.

C18.4.1.1.2. Self-protection measures for individuals while on a DoD or U.S. Government facility or installation.

C18.4.1.1.3. Self-protection measures for individuals while away from a DoD or U.S. Government installation.

C18.4.1.1.4. Self-protection measures for individuals while in transit from domicile to duty stations (for those living off an installation) or from one locale to another while on official business.

C18.4.1.1.5. Improvised Explosive Device (IED) recognition.

C18.4.1.1.6. Physical security measures for residents of single or multiple family housing units located off a DoD installation.

C18.4.1.1.7. Security measures for executives and their immediate staffs.

C18.4.1.1.8. Family security measures; and

C18.4.1.1.9. Other topics as specifically mandated by the Combatant Commanders.

C18.4.1.2. Commanders receiving individuals and units not properly trained shall report the deficiency through the chain of command or line of authority.

C18.5. HIGH RISK POSITIONS AND HIGH RISK BILLET DESIGNATIONS

C18.5.1. The Combatant Commanders have substantial AT responsibility for DoD personnel in their AORs assigned to high-risk billets (HRB) or high-risk positions. High Risk Personnel (HRP) assigned to high-risk positions become eligible for advanced AT training. In some instances, the training may be extended to include family members.

C18.5.2. The designation of personnel or billets as “high-risk” imposes a requirement on both the incumbents and the government to take special precautions to ensure the safety and security of these individuals and their family members. These individuals shall attend some of the resident AT training programs.

C18.5.3. Training for High Risk Billets and High Risk Personnel

C18.5.3.1. The Combatant Commanders annually identify a list of High-Risk Billets in their AORs. These lists are then forwarded through the appropriate Service personnel channels in order for each Service to identify, plan, and resource executive training requirements by June 30th each year.

C18.5.3.2. All executives, and their adult family members, en route to High Risk Billets shall attend the Individual Terrorism Awareness Course (INTAC) or the Dynamics of International Terrorism course. During this one-week course, executives shall receive instruction in defensive driving techniques and survival shooting, as well as individual protective measures and hostage survival.

C18.5.3.3. Executives should also attend the appropriate Regional Orientation Course (Middle East, Asia/Pacific, Latin America, or Africa) offered at the U.S. Air Force Special Operations School, Hurlburt Field, Florida.

C18.5.3.4. Executives whose duties shall require frequent vehicle operation should attend an appropriate evasive driving course. Information on current course offerings may be obtained by contacting the Service representative to the DoD Antiterrorism Coordinating Committee or the Combating Terrorism Branch in the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (OASD (SO/LIC)).

C18.5.4. Travelers to High/Potential Physical Threat Risk Areas

C18.5.4.1. Executives en route to potential physical threat risk shall attend one of the following courses:

C18.5.4.1.1. The Dynamics of International Terrorism Course conducted at the U.S. Air Force Special Operations School at Hurlburt Field, Florida. During this one week course executives shall receive lectures on threats by region (Europe, Middle East, Latin America, Asia/Pacific, and Africa), the history, and psychology of terrorism, personnel combating terrorism measures (vehicle, personal, airline, and physical security), and hostage survival.

C18.5.4.1.2. A Regional Orientation Course (Middle East, Latin America, Africa, Asia/Pacific) at the U.S. Air Force Special Operations School at Hurlburt Field, Florida. These one-week courses offer executives instruction in cultural, political/military, and individual security factors associated with the region.

C18.5.4.1.3. Training may also be administered by AT Level II qualified personnel.

# C19. CHAPTER 19
# PUBLIC AFFAIRS

## C19.1. INTRODUCTION

C19.1.1. A major goal of terrorist groups is to capture the attention of the news media. During and immediately following a terrorist incident involving DoD personnel or occurring on a Defense Department facility, the PAO becomes the conduit between DoD and the media. This chapter discusses the PAO's responsibilities and how they support the Commander's AT Program. The PAO role becomes highly valuable to a Commander after a terrorist attack. Following list of PAO activities highlight his value during a critical time.

C19.1.1.1. Maintain the flow of authoritative information between the authorities and the media.

C19.1.1.2. Keep the general public informed.

C19.1.1.3. Protect the interests of hostages or DoD personnel participating in incident resolution.

C19.1.2. The PAO has specific functions to perform, including screening information provided to the media to ensure operational security, preserving the privacy of hostages, victims, and their families, and advising the Department of Defense and other U.S. Government or foreign government officials managing the crisis on public affairs matters. DoD Directive 5200.1, DoD Directive 5230.16, DoD Directive 5410.1, and DoD Directive 5410.14 (references (al) through (ao)) provide guidance when coordinating with PAO.

## C19.2. BACKGROUND

C19.2.1. Risks. Many aspects of CbT operations are inherently sensitive and may involve various risks to DoD personnel or their dependents that may be heightened by the release of information to the public. These risks include, but are not limited to:

C19.2.1.1. Personal safety of law enforcement and intelligence personnel involved in terrorism investigations, analyses, or other related activities.

C19.2.1.2. Jeopardizing follow-on activities related to a terrorist incident.

C19.2.1.3. Jeopardizing the prosecution of people arrested for terrorist acts that inherently involve criminal acts.

C19.2.1.4. Operational security (OPSEC) of ongoing operations.

C19.2.1.5. Intelligence systems and sources.

C19.2.1.6. Relations with other Governments whose citizens, vessels, territory, etc., may be involved in terrorist activities, either by providing support or direction, or by being targets for future terrorist assault. These risks can be minimized only through a comprehensive coordination process before any information is released to the public.

C19.2.2. Teamwork. Most terrorist incidents shall trigger cooperative efforts among military and civil authorities, including the FBI, the DoS, other Federal agencies and departments, state and municipal law enforcement agencies, and host government activities if the event should occur overseas. Rarely shall a single agency and/or organization be able to take full credit for the termination of an event and the successful restoration of public order. By their nature, DoD combating terrorism and counter-terrorism efforts triggered by a terrorist incident shall rarely be unilateral. They almost always shall be in support of U.S. law enforcement agencies or cooperating host national military, police or security forces.

C19.3. RELEASE OF INFORMATION

C19.3.1. Policy Statements. The DoD Components shall not attempt to publicly discuss or interpret overall DoD policy regarding use of armed forces in law enforcement matters. Components may provide copies of speeches and other printed material originated within the Office of the Secretary of Defense (OSD), but shall refer to the OASD (PA) any news media questions on matters beyond their purview.

C19.3.2. Mission Statements. Previously approved statements and associated "Questions and Answers" pertaining to Combatant Command missions in the DoD effort may be used by the Commands concerned in the military departments for public affairs purposes as they deem appropriate.

C19.3.3. Announcements of Investigations and Arrests. The announcement regarding a terrorism-related investigation or arrest normally shall be made by the agency/organization that conducted the investigation or actually made the arrest. Such announcements shall indicate that the operation was a "coordinated federal effort" and shall list participating agencies and/or organizations following coordination with each. Although the DoD Components shall not make announcements of investigations and arrests, it may be of interest to note the general ground rules that the law enforcement agencies observe in making such announcements.

C19.4. INTERVIEWS AND PRESS CONFERENCES

C19.4.1. Interviews. Numerous interview requests concerning the DoD CbT Program may be received at the installation, base or unit levels. The OASD (PA) has no objection to such interviews if the following criteria are met:

C19.4.1.1. All interviews shall be on the record, unless a different category of attribution has been agreed upon by the lead PAO and the interviewer when the ground rules are established.

C19.4.1.2. Interviewed personnel shall discuss only information within their personal purview and expertise. No classified information shall be discussed.

C19.4.1.3. Do not discuss or interpret overall DoD policy regarding armed forces support of the U.S. Government's counterterrorism efforts.

C19.4.1.4. Responses given during the interview shall meet operational security requirements. Interviewees wishing to protect their identity in published media must establish appropriate media ground rules prior to interview. Appropriate public affairs offices must be included in planning and conducting all interviews.

C19.4.1.5. Interviewees shall not answer questions regarding hypothetical situations. Furthermore, interviewees shall not comment on matters pertaining to other U.S. Federal/State/local organizations/agencies and/or the military, police or security forces of other nations.

C19.4.1.6. A summary of controversial interview discussions and/or notification of interview results that might require OASD (PA) response shall be provided through appropriate command channels to OASD (PA): DPO.

C19.4.2. Joint Press Conferences. DoD spokespersons may be invited to participate in joint press conferences organized by Federal/State/local law enforcement agencies following the conclusion of a terrorist episode involving DoD personnel, facilities, or materiel or where DoD support contributed to the success of the combating terrorism operation. It is generally the case that Department personnel shall be in supporting roles in such operations and the presence at joint press conferences should reflect the supporting, as opposed to leading, nature of DoD participation. OASD (PA) has no objection to such participation if the following criteria are met:

C19.4.2.1. Appropriate public affairs offices in the chain of command must be included in the planning for such press conferences.

C19.4.2.2. Spokespersons shall discuss only information within their personal purview and expertise. No classified information shall be discussed.

C19.4.2.3. Spokespersons shall not discuss or interpret overall DoD policy regarding armed forces support of the U.S. Government's Counter-terrorism policy (use of force against terrorist groups, their state supporters, or those states that direct attacks by terrorist groups against U.S. interests).

C19.4.2.4. Responses given during the press conference shall meet operational security requirements.

C19.4.2.5. Spokespersons shall not answer questions on hypothetical situations. They shall not comment on matters pertaining to other U.S. Federal organizations and/or agencies and/or the military, policy or security forces of other nations.

C19.4.2.6. After-action reports and/or transcripts of press conferences shall be provided through appropriate command channels to OASD (PA) DPO, if appropriate.

C19.4.2.7. The following may not be released:

C19.4.2.7.1. Statements by the accused or the fact the accused made or refused to make a statement.

C19.4.2.7.2. Indications of the prospective witnesses in the case.

C19.4.2.7.3. Comments on the credibility or testimony of anyone involved in the case.

C19.4.2.7.4. Information involving the possibility of a guilty plea, the accused guilt or innocence or the merits of the charges or defense in the case.

C19.4.2.7.5. Whether intelligence led to the seizure (the only exception is if the agency that provided the intelligence decided the information may be released).

C19.3.4.7.6. Names of DoD casualties, subject to release upon notification of next of kin and PA authorization.

C19.4.3. Training Versus Operations. OASD (PA) understands that media may be interested in covering training involving the DoD of Defense and other agencies to get an idea of the type of support the DoD is providing. OASD (PA) has no objection to this type of coverage as long as thorough coordination has been completed with other agencies and foreign governments where foreign personnel are involved, and operational security considerations have been addressed.

C19.5. SENSITIVE ISSUES

Speaking With One Voice. Speaking with one voice has become even more critical for the DoD. DoD spokespersons talking or writing about terrorism must not only be consistent within the DoD, but also must be consistent with the stated goals and objectives of other agencies supporting the nation's combating terrorism effort. If various agencies appear to be at odds or making conflicting statements, the public perception shall be one of confusion and misunderstanding that shall subject all participants to criticism of what is supposed to be a "coordinated federal effort." Terrorist acts are by definition criminal acts. Drug-related activities such as money laundering, smuggling, gunrunning, assassination, kidnapping, and extortion, often associated with terrorist incidents, are also criminal acts. The Department of Defense plays a strong role in supporting the application of Federal jurisdiction in criminal courts around the world to bring perpetrators of unlawful acts against American citizens to justice, but it does not act alone.

C19.6. INTERNAL INFORMATION

DoD efforts in combating terrorism operations shall be of great interest to our internal audiences as well as the general public. The internal use of descriptions, photographs and videotape of these operations has the potential of gaining public attention. This material must be subjected to the same guidance with respect to review and release as other material intended for release outside the Department of Defense. Other information collected during and immediately after a terrorist incident for internal DoD use (including witness interviews, crime scene photographs recordings of communications or other electronic signals) should also be reviewed by representatives of the U.S. Attorney having jurisdiction over the incident to ensure that no information which might be deemed evidence in a court become tainted or is released within the Department of Defense or to others.

## C19.7. TERRORIST ACTS AND PUBLIC AFFAIRS RESPONSIBILITIES

### C19.7.1. General Public Affairs Antiterrorism Responsibilities

C19.7.1.1. Public affairs responsibilities for dissemination of information following terrorist incidents mirror jurisdiction and authority. In the United States, its territories, and possessions, public affairs responsibilities belong principally to the DoD activity where the terrorist incident has occurred, with guidance and support coming from OASD (PA) through the chain of command. The DoJ and the FBI have primary responsibility for public affairs matters when the U.S. Attorney exercises Federal jurisdiction and the FBI when they are investigating and prosecuting alleged perpetrators of criminal acts. If State or local jurisdiction is exercised; those authorities would execute principal public affairs responsibilities.

C19.7.1.2. When terrorist incidents occur outside the United States, its territories, and its possessions; the host nation, DOS, and the Department of Defense (OSD and the Combatant Command) all have public affairs responsibilities.

C19.7.1.3. Terrorist incidents require practiced public affairs skill. The right of the public to know the scope and magnitude of terrorist attacks involving DoD personnel, facilities, or materiel must be balanced by the need to safeguard information of military or security significance. The ability of U.S. and host government authorities to resolve a terrorist incident should not be compromised, nor should the rights to privacy of terrorist incident victims be unilaterally overridden by public affairs activities.

C19.7.1.4. All DoD activities strive to fulfill the Department of Defense's goal of providing as much information to the public about DoD activities as possible, consistent with the requirements of OPSEC, technology security, and information security. The Department of Defense's approach to the provision of information on its AT efforts is no different.

C19.7.1.5. DoD PAOs have a special, prominent role to play in the DoD AT program. All DoD installations, facilities, organizations, and commands should have an ongoing program intended to reduce its risk and vulnerability to terrorist attack. A PA annex should be developed in support of an installation AT plan.

### C19.7.2. Understanding the PAO's Role in DoD AT Programs

C19.7.2.1. PAOs play a major role in the DoD AT program. They are educators, making audiences within and outside DoD aware of the threat of terrorism. They are communicators, explaining to DoD personnel, their family members, and the communities in which the DoD

Components are present the measures taken to reduce their risk and vulnerability to terrorist attack. They are "pollsters," pulsing and reporting back to the DoD Components, the concerns and fears of the community generated by DoD presence or DoD activities in their communities and the risks of terrorist attack that may ensue.

C19.7.2.2. The challenge facing PAOs from the terrorist threat is great. To succeed in their mission, PAOs exercise constant vigilance and sensitivity to the needs of their audiences. They also remember that the terrorists themselves are a part of that audience. In making information available to the news media, PAOs delicately balance the legitimate information requirements of their DoD and civilian audiences against the intelligence requirements of the terrorists. PAOs constantly coordinate with other members of the installation, activity, organization, or command staff.

C19.7.2.3. Membership in the Force Protection Working Group. The PAO is an important, although often overlooked, member of the unit/installation antiterrorism program. During a terrorist incident, the PAO serves an important function in providing information to local authorities as well as the media, thereby allowing the Commander and ATO to focus on the incident at hand. Therefore, it is important that the Commander ensure his PAO be knowledgeable about the AT Program and AT Plan, and to participate in AT Program development and implementation.

C19.7.2.4. Establishment of an Incident Information Center. In the event of a terrorist incident, the PAO should establish an Incident Information Center. The purpose of the Incident Information Center is to provide a single location where news media can meet with the PAO to attain information about the incident. The Incident Information Center should be located where media access can be controlled, for example, in close proximity to an access control point. The Incident Information Center should not be collocated with the EOC.

C19.7.2.5. Terrorism Awareness. Individual terrorism awareness is an important element in overall antiterrorism readiness. DoD personnel and family members should have a general knowledge of the terrorist threat, know how to reduce their vulnerability to terrorists, and be knowledgeable of FPCONs. An AT involved PAO can significantly enhance the installation AT awareness training program by using the various mass notification means available to educate personnel, including newspapers, newsletters and flyers, closed circuit television, and billboards. Also, as individuals are "inconvenienced" by the effects of increased security measures such as base access restrictions, vehicle searches, and commissary and/or exchange closures, the PAO can reduce personnel frustration and tension by keeping them informed of AT measures and

rationale. The PAO's terrorism awareness efforts can also have considerable terrorist deterrence value. Terrorists shall be able to gain access to the various unclassified notification means intended for DoD personnel. If this information convinces the terrorist that the installation is a "hard target" he might look elsewhere.

C19.7.2.6. Training and Exercise Participation. A comprehensive AT training and exercise program is essential to AT readiness. The PAO's responsibilities in a catastrophic incident shall be significant and require the ability to effectively communicate with the Commander, the Operations Center personnel, the media, and the local authorities. Planned, command approved media questions and answers can significantly enhance the PAO's ability to train for and respond to terrorist incidents. The PAO shall also be responsible for maintaining control over medial personnel at the Incident Information Center. Therefore, the facility Commander should include the PAO participation in the development of terrorism scenarios and participate in all phases of this program.

# C20. CHAPTER 20
# SPECIAL CONSIDERATIONS

## C20.1. OVERVIEW

C20.1.1. Discussion of efforts by the Department of Defense to combat terrorism would be incomplete without reviewing AT DoD contractor issues and website vulnerabilities.

C20.1.2. DoD contractors provide many critical and essential services to U.S. forces. As noncombatants, DoD contractors are entitled to certain protections under international law. Further, commanders may be required to provide AT training and resources as specified in terms of their contract.

C20.1.3. Website vulnerabilities are an increasing concern for DoD personnel. With the global reach of the World Wide Web, or Internet, it is imperative that safeguards be implemented to protect information posted on U.S. Government websites.

## C20.2. DoD CONTRACTORS

C20.2.1. Contractor support continues to increase in significance as a major contributor in military operations. Properly applied, contractor support is a force multiplier and enhances operational capabilities. However, contractors are not combatants and must not be allowed to act or appear to act as combatants. The Commanders should take care to ensure contractor personnel are not used in any manner that would jeopardize their status under international law, references (ap) and (aq) provide guidance. The Combatant Commanders do not have the same legal responsibility to provide security for contractors as we do for our military forces or direct hire employees. However, in many cases from a practical standpoint, protecting contractor activities might be necessary to ensure mission accomplishment. Contractors remain private American citizens. The Department of Defense shall assist the Department of State, where militarily feasible, in supporting their efforts to protect Americans abroad. Contractors are required to contact the combatant command in order to obtain and comply with the specific antiterrorism guidance for the particular area they shall work in. Contractors must ensure their personnel receive antiterrorism/force protection awareness (Level I) training prior to travel. They must also ensure their personnel register with the U.S. Embassy and affiliate with the Overseas Security Advisory Council. The Combatant Commanders maybe required to offer training to contractors under the terms specified in the contracts. Contractors working within a

U.S. facility overseas or in close proximity of our forces shall receive incidentally the benefits of measures undertaken to protect our own forces.

C20.2.2. All U.S. contractors are expected to comply with all applicable laws, including international law, affecting the contractor and/or contract. Unless addressed otherwise by international agreement, contractor personnel are subject to the law of the nation in which they are located to include all local taxes, immigration requirements, customs formalities and duties, environmental rules, bond or insurance requirements, work permits, and transportation or safety codes. In addition, contractors who violate U.S. Federal law while accompanying the Armed Forces overseas can be removed to the U.S. for Federal prosecution under the Military Extraterritorial Jurisdiction Act (Public Law 106-523, November 22, 2000 (reference (ar)). During a period of declared war, contractor personnel accompanying the armed forces are subject to the criminal jurisdiction of the military and the Uniform Code of Military Justice.

C20.2.3. When contractor personnel are employed in support of the Department of Defense, the Department of Defense shall provide or make available, under the terms and conditions as specified in the contract, AT training commensurate with that provided to DoD civilian personnel to the extent authorized by U.S. and host nation law.

C20.2.4. As a general rule, the Commanders should not issue firearms to contractor personnel, nor should they be allowed to carry personally owned weapons. After consultation with host nation authorities, the Combatant Commanders may deviate from this rule in the most unusual circumstances (e.g., protection from criminals or animals if no military personnel are present to provide protection).

C20.2.5. The Commanders should not issue contracted personnel military garments unless there is a compelling reason to do so. Care should be taken to ensure contracted personnel are clearly distinguishable at a distance from military personnel through the use of distinctly colored patches, armbands, or headgear.

C20.2.6. When developing logistics contracts to support operational forces, commanders shall incorporate AT considerations during the entire contracting process. During the evaluation process, future contract awards shall consider whether a potential contractors prior compliance with AT measures was satisfactory.

C20.2.7. Contractor employees, being an integral part of a unit's mission to include higher headquarters, shall be offered Level I AT Awareness training under terms and conditions as specified in the contract.

C20.3. WEBSITE VULNERABILITY

C20.3.1. The potential for inadvertent or unauthorized disclosure of sensitive information continues to grow. The World Wide Web provides the Commander a powerful tool to convey information quickly and efficiently on a broad range of topics. The global reach of the Internet provides our adversaries with a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregated information on defense personnel and activities. When combining the infrastructure components, networks, and domains, the OPSEC-oriented user shall quickly recognize the vast resources of information available to our public and adversary.

C20.3.2. The worldwide connection of computer local-area and wide-area networks, such as the Non-Secure Internet Protocol Router Network (NIPRNET), offers easy access to defense information from anywhere in the world. Separation between the NIPRNET and the World-Wide-Web is ambiguous, and occasionally these networks may be indistinguishable to web page administrators. Web pages intended for internal DoD use should not be made available on the NIPRNET without appropriate access control, as this information is likely to be accessible to non-DoD or unauthorized users.

C20.3.3. Webmasters, page maintainers, network administrators, subject matter experts, PAOs and OPSEC personnel must develop a disciplined review of all information posted to their locally generated websites. This must be done to protect sensitive unclassified and classified information while recognizing the importance of making available timely and accurate information to the intended DoD audience.

C20.3.4. Evaluations of activity information provided on the NIPRNET and DoD websites that are publicly accessible, should follow current OPSEC procedures:

C20.3.4.1. Identify information access points (such as NIPRNET or the Internet) and evaluate their importance to activity operations.

C20.3.4.2. Determine the critical information for the activity's operations and plans. Information that would not be of interest or use to the general public should not be on a public-access page.

C20.3.4.3. Determine the threat, and assume that any potential adversary has access and knows how to search the net.

C20.3.4.4. Determine the vulnerabilities and evaluate how protected are the web pages. Remember that the hacker is generally the information security threat; the search engine and browser are generally the OPSEC threat.

C20.3.4.5. Assess the risk and determine what protection should be applied to minimize potential loss of critical information and what is the impact on operations and operations support.

C20.3.4.6. Apply protection, which combines information security and OPSEC tools to minimize information loss and vulnerability.

C20.3.5. When applying the OPSEC process to information posted to web sites, the activity shall also need to evaluate subject data with regard to the time factor. Information gathering in the past was a manpower and resource intensive process, dependent on various types of overt and clandestine means. Collection, compilation, analysis and dissemination of information could take days, weeks, or months. Today, a single user can connect to the Internet and, using various search engines, browsers, and certain aggregation methods, develop a composite of information that surpasses traditional knowledge levels. In essence, geography is no longer a factor in information retrieval; time becomes the dominant factor.

C20.3.6. The user must determine the value of information with regard to time. Certain data, such as unit history, emblems, and command affiliation, shall have less time criticality than deployment orders for exercises or real-world operations. The value of information may also flex over time. For example, the specifics of post-deployment preparation should not be posted to a publicly accessible web site prior to the deployment. But once in theater, unit types, number of personnel, and equipment shall be public knowledge over time, decreasing the sensitivity as redeployment dates and unit withdrawal specifics are planned. This shall require units to actively scrutinize their web pages for time-sensitive data.

C20.4. INFORMATION REQUIREMENTS

C20.4.1. All RAs and antiterrorism plans referred to in this publication are exempt from licensing in accordance with reference (as).

C20.4.2. All DD Forms and all checklists referred to in this publication are exempt from licensing in accordance with reference (as).

# C21. CHAPTER 21
# INDIVIDUAL PROTECTIVE MEASURES

## C21.1. INTRODUCTION

Security against terrorism is the responsibility of every DoD civilian and uniformed member. There are some basic measures high-risk personnel and/or any DoD civilian and uniformed member can take to make them less vulnerable, commonly referred to as a "hard target," and reduce the probability of becoming a victim of a terrorist incident. This Chapter shall outline general individual protective concepts and conclude with a discussion on Protective Service Operations. For more comprehensive and specific guidance, consult applicable Service, Combatant Commander, or Agencies.

## C21.2. GENERAL APPROACH TO INDIVIDUAL PROTECTIVE MEASURES

C21.2.1. Personnel associated with the U.S. Government are often targets for terrorist activity. The Heads of the DoD Components have two major AT responsibilities:

C21.2.1.1. Provide as much security for personnel under their authority and control (to include family members) as is consistent with threat, risk, vulnerability, and criticality assigned roles, missions, and resources.

C21.2.1.2. Provide awareness information and educational materials to assist service members, DoD civilians, contractor personnel and their family members in reducing their individual risk and vulnerability to terrorist attack.

C21.2.2. ATOs or commanders or others designated by the Heads of Defense Agencies, the Military Services, the Combatant Commands, the Commanders of military installations, and the Commanders at all echelons, should ensure AT personnel protection is part of their AT Plan.

## C21.3. PERSONAL PROTECTION MEASURES FOR DOD PERSONNEL

C21.3.1. One of the most important individual protective measures DoD-affiliated persons can take is to develop personal habits and practices that frustrate terrorist attempts to determine their nationality, their professions, their individual job responsibilities, their association with the Department of Defense and their overall importance to the Department of Defense. Three basics rules frame personnel protective measures for DoD personnel, DoD contractors, and family members:

C21.3.1.1. Maintain a Low Profile. DoD personnel, DoD contractors, and their family members should dress and behave in public in a manner consistent with local customs. Items that are distinctively American should not be worn or displayed outside American compounds unless necessary to accomplish official business.

C21.3.1.2. Be Unpredictable. Most persons and organizations fall into habits or routine behaviors. Work begins and ends at the same time every day; meals are eaten in the same cafeteria; exercise takes place at the same time and at the same location every day; and individuals follow the same route to and from the office every day. Terrorists normally plan their actions carefully. They shall observe the potential target's routines in order to decrease their risks and increase the probability of success. The ability to be unpredictable increases the risks to terrorists and severely decreases the chances of their success. Reduced probability of success in kidnapping or killing a target makes that target far less desirable.

C21.3.1.3. Even though DoD personnel, DoD contractors, and their family members may do everything recommended above and elsewhere in this Handbook, they may still be threatened by or become victimized by a terrorist act. Be alert for anything suspicious, abnormal, or out of place.

C21.3.2. General Considerations. The following are general practices that shall aid in reducing the likelihood of being a victim of a terrorist attack.

C21.3.2.1. Office Security.

C21.3.2.1.1. Establish and support an effective security program for the office.

C21.3.2.1.2. Discourage use of office facilities to store objects of significant intrinsic value unless essential for the mission or function of the activity (such items include petty cash boxes, firearms, personal stereos, binoculars, negotiable securities, original artwork of potential commercial interest, etc.).

C21.3.2.1.3. Ensure that all persons working in an office are trained to be alert for suspicious activities, persons or objects.

C21.3.2.1.4. Arrange office interiors so that strange or foreign objects left in the room shall be immediately recognized. As an example, remove obvious obstructions behind which or within which IEDs could be concealed such as draperies, closed waste baskets, unsecured desks and filing cabinets, and planters.

C21.3.2.1.5. Provide for security systems on exterior doors and windows.

C21.3.2.1.6. Ensure installation and facility access control procedures are rigorously observed.

C21.3.2.1.7. Use an identification badge system containing a photograph. Photo badge systems facilitate security by making it easy to identify employees, visitors, maintenance personnel, and facilities management/security personnel. Badges should be renewed periodically; the badge systems should be modified every 2 or 3 years to preclude use of altered, expired or stolen badges.

C21.3.2.1.8. Locate desks in a way that persons entering the office or suite can be observed.

C21.3.2.1.9. Identify offices by room number, color, or object name, and not by rank, title, or name of incumbent. In other words, identify rooms by room 545, the gold room, the Berlin room, the maple room, and not by titles such as the General's office, the Assistant Attaché's office, or the S-2's office.

C21.3.2.1.10. Do not use nameplates on offices and parking places.

C21.3.2.1.11. Telephone and Mail Procedures.

C21.3.2.1.11.1. Consider not using rank or title should not be used when answering telephones.

C21.3.2.1.11.2. When taking telephone messages, do not reveal the whereabouts or activities of the person being sought unless the individual taking the message knows the caller personally.

C21.3.2.1.11.3. Collect telephone messages in unmarked folders; do not expose them for observers to identify caller names and phone numbers, persons called, and messages left.

C21.3.2.1.11.4. Observe caution when opening mail. In particular, be on the look out for letters or packages that might contain IEDs.

C21.3.2.1.12. Visitor Control Procedures.

C21.3.2.1.12.1. Access to the executive office area should be strictly limited; during periods of increased threat, access to additional office, shop, laboratory, and other areas within the installation should also be controlled.

C21.3.2.1.12.2. Doors from the visitor access area to executive offices or other restricted areas of a facility should be locked from within; there should be only one visitor entrance and exit to a restricted access or exclusion area.

C21.3.2.1.12.3. Have a receptionist clear all visitors before they enter inner offices.

C21.3.2.1.12.4. Permit workmen or visitors access to restricted areas or exclusion areas only with escort and only with proper identification; confirm work to be accomplished prior to admitting workmen to restricted areas of the facility.

C21.3.2.1.12.5. When possible, limit publicity in public waiting areas to information that does not identify personnel by name, position, or office location.

C21.3.2.1.12.6. Do not post unit rosters, manning boards, or photo boards where they can be viewed by visitors or local contractors providing cleaning services, food and beverage services, delivery of office supplies, removal of trash or waste, care of plants, etc.

C21.3.2.1.12.7. Restrict use of message boards, sign in-out boards, and other visual communications to general statements of availability; do not publicly list local travel itineraries or phone numbers where visitors have easy, unrestricted access to such information. When using sign-out logs, be sure to keep the log in a secure location known only to those using it, thereby restricting public access.

C21.3.2.1.13. General Working Procedures.

C21.3.2.1.13.1. Avoid carrying attaché cases, brief cases, or other courier bags unless absolutely necessary. Brief cases and attaché cases have become symbols of power and prominence in many cultures. When possible, use satchel bags or other locally obtained book bags instead.

C21.3.2.1.13.2. Do not carry items that bear markings that identify the owner by rank or title, even within the office environment. Coffee mugs labeled "General, Attaché, Boss" may be seen in use by a visitor to gather targeting intelligence.

C21.3.2.1.13.3. Avoid working alone late at night and on days when the remainder of the staff is absent. Work in conference rooms or internal offices where observation from the outside of the building is not possible if late night work is necessary. Persons working at night should turn lights on and off in several offices before going to their own offices to disguise the purpose of their activities to outside observers.

C21.3.2.1.13.4. Office doors should be locked when vacant for any lengthy period, at night and on weekends. The security office and the incumbent should retain keys to the office.

C21.3.2.1.13.5. Papers, correspondence, communications materials, and other documents should not be left unattended overnight. A clean desk policy facilitates improved security as it makes it difficult to hide intelligence collection devices or improvised explosive devices in occupied offices at the close of a working day.

C21.3.2.1.13.6. Monitor maintenance activity and janitorial services in key offices. Consider shredding unclassified documents, particularly in high threat areas. Sifting through garbage cans and recycling bins that may prove helpful to terrorists in operational planning can gather a wealth of information.

C21.3.2.1.13.7. Removal of property, materiel, or information stored on any media from the facility should be prohibited without proper written authorization.

C21.3.2.1.13.8. Prohibiting the importation of property, materiel, or information stored on any media into the facility unless such items have been properly inspected should be considered. Inspection of electronic media should focus on computer viruses or other programs that might be used to modify operating systems or applications programs permitting unauthorized access to information stored on or accessed through the facility's computers.

C21.3.2.1.13.9. Offices not in use should be locked to prohibit unauthorized access or the storage of material that could be used to hide IEDs or intelligence collection devices.

C21.3.2.1.13.10. All personnel should have access to some sort of duress alarm to annunciate and warn of a terrorist attack.

C21.3.2.1.13.11. Consider equipping secretaries and guard posts with covert duress alarms. For high-risk personnel and their secretaries, consider connecting covert duress alarm to system that annunciates at the local security forces, law enforcement control center, and/or U.S. consulate security control center, as appropriate.

C21.3.2.1.13.12. Move office furnishings away from exterior windows.

C21.3.2.1.14. Special Procedures for Executive Assistants. The following suggestions are intended to be a guide for secretaries and executive assistants who may find themselves performing personnel security duties as collateral duty.

C21.3.2.1.14.1. Consider installation of physical barriers such as electro-magnetically operated doors to separate offices of senior executives from other offices.

C21.3.2.1.14.2. Consider installation of a silent trouble alarm button, with a signal terminating in the Security Department.

C21.3.2.1.14.3. Do not admit visitors into the executive area unless they have been positively screened in advance or are known from previous visits.

C21.3.2.1.14.4. Unknown callers should not be given information.

C21.3.2.1.14.5. Consider storing a fire extinguisher, and first-aid kit in the office area.

C21.3.2.1.14.6. Post procedures for handling threatening calls by the phone.

C21.3.2.1.14.7. Do not accept packages from strangers until satisfied with the individual's identity and the nature of the parcel.

C21.3.2.1.14.8. Limit distribution and visibility of travel itineraries and schedules of senior officials.

C21.3.2.1.15. Safe-haven. A safe-haven is any location one can go to seek safety or emergency assistance. Consider safe-havens when planning travel routes. As discussed earlier, a safe-haven can be constructed in a residence or at work.

C21.3.2.1.16. At Home. See section C21.4.

C21.3.2.1.17. At Social and Recreational Activities

C21.3.2.1.17.1. DoD personnel are encouraged to participate in many social and recreational activities. Participation in such activities does not in and of itself add to the risk or vulnerability of DoD personnel or their family members to terrorist attack. However, some precautions are noteworthy.

C21.3.2.1.17.2. Respond to formal social invitations by personal visit where possible or direct telephone contact with the principal; avoid widespread uncontrolled dissemination of social or recreational plans.

C21.3.2.1.17.3. Be attentive to the security environment of social gatherings; do not remain at a function if it does not appear to be adequately protected.

C21.3.2.1.17.4. Avoid the development of patterns regarding time of arrival or departure at social events; don't always arrive promptly on time or be consistently 15 minutes late; don't always leave early or be the last person to leave the function.

C21.3.2.1.17.5. Try to avoid prolonged presence at social functions where there is a high concentration of persons thought to be terrorist targets.

C21.3.2.1.17.6. Refrain from excessive use of alcohol at social functions; remain clear headed and unimpaired; be ready for the unexpected.

C21.3.2.1.17.7. Vary routes to and from social events held at a central facility; use different entrances and exits.

C21.3.2.1.17.8. Minimize appearances in uniform or formal attire.

C21.3.2.1.17.9. Decline invitations to appear in publicity photos; if photos are taken, discourage publication of names associated with persons appearing in the photo.

C21.3.2.1.17.10. Participate in recreational activities within the American compound or at a DoD installation whenever possible; try to select playing fields or recreational areas in secured installations or within easy reach of such installations if it is thought that terrorist activity is particularly likely.

C21.4. FAMILY MEMBERS OF DOD AFFILIATED PERSONS.

C21.4.1. All DoD affiliated family members should be knowledgeable about basic AT personal security measures. DoD personnel should cultivate an interest in and attract participation from all family members in the security effort. This should include a predetermined plan for responding to potential criminal or terrorist acts. The following general guidance shall assist personnel in reducing the AT threat. The three basic rules apply; keep a low profile, be unpredictable, and be alert. In addition, avoid unnecessary publicity and photographs that identify individual family members or which associate family members and DoD personnel. Appendices 10 and 11 offer additional suggestions for family and household security.

C21.4.2. General Guidance. Develop a family oriented antiterrorism awareness, education, and training plan as part of preparing for each new assignment. Preparation should begin prior to departure for a new assignment. All family members should try to learn about the customs,

culture, history, and geography of the area that the DoD member has been assigned. Family members on travel orders accompanying a service member overseas shall receive Level I AT Awareness Training as part of their pre-departure requirements. Furthermore, DoD personnel and their family members are encouraged to receive Level I AT Awareness Training prior to any unofficial OCONUS travel, such as going on leave or vacation. The standard DoD Level 1 brief is probably not appropriate for children under 8-10 year old and an alternative method of training could be the online program offered by the National Crime Prevention Council at www.mcgruff.org.

C21.4.2.1. Do not use nameplates or uniquely American symbols on the exterior of residences occupied by DoD personnel overseas.

C21.4.2.2. Do not use name plates on parking places; avoid parking private or government vehicles in the same location day after day.

C21.4.2.3. All mail delivered to the residence should be carefully examined; any mail or packages from senders who cannot be immediately identified should be set aside for further evaluation by the DoD member.

C21.4.2.4. Never leave house or trunk keys with your ignition key while your car is being serviced.

C21.4.2.5. Do not "hide" keys or give them to very young children.

C21.4.2.6. Never leave young children at home alone.

C21.4.2.7. Never admit strangers into your home without proper identification.

C21.4.2.8. Teach children how to call the police and ensure they know what to tell the police (name, address, etc.).

C21.4.2.9. Carefully screen all potential domestic help.

C21.4.2.10. Use off street parking at your residence, if at all possible.

C21.4.2.11. Avoid frequent exposure on balconies and in windows.

C21.4.2.12. Do not tack notes on the door for family and friends.

C21.4.2.13. Keep tools, particularly ladders, under lock.

C21.4.3. Overcome Routines. Vary routes, arrival, and departure times to and from school, after school activities, day care, religious school, music lessons, and other regularly occurring family member activities.

C21.4.4. Maintain a Low Profile. DoD personnel should explain the risks and benefits of high profile, high visibility lifestyles to their family members. It is sometimes very difficult for many families to go from being highly visible members of a community to being nearly invisible. Visibility is often especially important to adolescents and non-working spouses of DoD personnel. The differences and distinctions among participation in community events such as school plays, sports, and social clubs as opposed to high profile participation should be discussed. DoD personnel should explain to their family members the benefits and risks associated with high profile, highly visible lifestyles in certain environments.

C21.4.5. Family "Operations Security" Procedures. The purpose of operations security is to frustrate adversary collection of information about one's activities. Family "operations security" measures seek to frustrate efforts by terrorists to identify the nationality, the specific name, the functions, and the patterns of behavior of DoD-affiliated persons and their family members. The following measures are only a small number of examples of steps that should be implemented to make it harder for terrorists to learn the nationality, specific identity, position, and responsibilities of DoD personnel, as well as the day-to-day activities of DoD families.

C21.4.5.1. Do not place your name on exterior walls of residences.

C21.4.5.2. Do not answer your telephone with your name and rank; children and domestic employees should be instructed not to identify the name, title, or affiliation of the occupants, when answering the telephone. All family members should answer the telephone politely but should provide no information as to the name of the occupants until the identity of the caller has been established. Further, family members should treat all telephone conversations as though a third party was monitoring them. Children should be taught not to tell strangers over the phone if their parents or other adults are in the house. A simple “they can’t come to the phone right now” should be adequate for any possible inquires.

C21.4.5.3. Do not list your telephone number and address in local directories.

C21.4.5.4. Create the appearance that the house is occupied by using timers to control lights and radios while you are away.

C21.4.5.5. Personally destroy all envelopes and other items that reflect personal information.

C21.4.5.6. Close draperies during periods of darkness. Draperies should be opaque and made of heavy material.

C21.4.5.7. Don't let your trash become a source of information.

C21.4.6. Be Alert to Changes. All DoD personnel and their family members should be attentive to their security environment and changes that may occur in it. Family members should be instructed to be alert for surveillance attempts, suspicious persons or activities, and report them to the proper authorities.

C21.4.6.1. Watch for unexplained absences of local citizens as an early warning of possible terrorist actions.

C21.4.6.2. Avoid public disputes or confrontations. Report any trouble to the proper authorities.

C21.4.6.3. Do not unnecessarily divulge your home address, phone number, or family information.

C21.4.7. Potential Threats. The following steps should be implemented when appropriate:

C21.4.7.1. Any unusual occurrence such as anonymous phone calls or threats should be reported immediately.

C21.4.7.2. Children should be on guard against any approach or interrogation by strangers; efforts by strangers to pick up children, engage them in long conversations about their home life or find out what their parents do for a living should be reported to law enforcement and intelligence activities immediately.

C21.4.7.3. Never accept unexpected package deliveries.

C21.4.7.4. Examine all mail carefully and look for signs that an improvised explosive or incendiary device has been received.

C21.4.7.5. Report frequent wrong numbers or nuisance telephone calls to the Telephone Company and the police. Someone may be attempting to determine the presence of family members.

C21.4.7.6. Report any interruption in telephone or electrical service, strange noises on telephone lines or any unusual interference with radio, television, or home computer operations to the nearest intelligence or law enforcement activities.

C21.4.7.7. Do not automatically open your door to strangers; use the peephole and always check credentials.

C21.4.7.8. Be wary of talking to or admitting polltakers and salespersons to your home. Terrorists are known to have gathered substantial information relative to their victims using these ruses.

C21.4.7.9. Be alert to peddlers and all strangers.

C21.4.7.10. Be alert to public utility crews or other workmen who request access to your residence. Check identities. If there is any doubt, refuse them admittance.

C21.4.7.11. Report the presence of strangers in the neighborhood to military law enforcement or military intelligence activities as soon as their presence is detected.

C21.4.7.12. Watch for strange cars cruising or parked frequently in the area, particularly if one or more occupants remain in the car for extended periods. Make a note of occupants, license numbers and province designators of suspicious vehicles.

C21.4.7.13. If you come home and suspect that an unauthorized person is inside, do not go in to investigate and do not call out to the possible intruder. Contact the police or your security patrol.

C21.4.7.14. Do not accept unsolicited packages. All mail should be routed through normal office channels.

C21.4.8. Be Prepared for Unexpected Events. Instruct family members of the Department of Defense on steps they should take to deal with unexpected events. It is good practice to get into the habit of "checking in" to let your friends and family know were you are or when to expect your return.

C21.4.8.1. Telephone systems overseas can be quite different from those in CONUS therefore family members should know and understand how to use the local phone system. Always carry enough currency to make a telephone call.

C21.4.8.2. Family members should know the locations of civilian police, military police, hospitals, Government Agencies, the U.S. Embassy, and other safe locations where refuge or assistance can be acquired. Always carry identification showing your blood type and any special medical conditions.

C21.4.8.3. Learn key phrases in the native language such as "I need a policeman," "Take me to a doctor," "Where is the hospital?" and "Where is the police station?"

C21.4.8.4. Develop a family duress code so family members can warn each other when they are in danger.

C21.4.8.5. Develop emergency procedures and practice them.

C21.4.8.6. Maintain emergency telephone numbers for all family members.

C21.4.9. Kidnapping and Hostage Issues. DoD-affiliated persons and their families should discuss steps to be taken if a member is kidnapped or otherwise becomes the victim of a terrorist attack. Families should understand the U.S. Government makes every effort to affect the rapid, safe release of any U.S. citizen held hostage. The importance of family cooperation in such a situation should be stressed.

C21.4.10. Special Guidance for Children. Parents have special responsibilities when providing personal security instruction for children. There are several children oriented or children specific measures that can be taken to reduce the risk of terrorist attack against them:

C21.4.10.1. Never leave young children alone or unattended. Be certain when they are left, they are in the care of a trustworthy person.

C21.4.10.2. Instruct children to keep doors and windows locked, and never to admit strangers.

C21.4.10.3. Try to locate children's room(s) in a part of the residence that is not easily accessible from the outside.

C21.4.10.4. Make sure that outside doors and windows leading to children's rooms are kept locked, especially in the evening.

C21.4.10.5. Keep the doors to your children's rooms open so that unusual noises can be heard.

C21.4.10.6. Teach children how to contact the police or a neighbor in an emergency; also teach them how to contact DoD security or intelligence activities nearby; teach them how to contact the U.S. Embassy if overseas.

C21.4.10.7. Know where your children are all the time.

C21.4.10.8. Advise school officials that children are not to be released to strangers under any circumstances.

C21.4.11. Special Guidance for Pre-Adolescents and Teenagers. Pre-adolescents and teenagers should be taught and encouraged to take the following personal security steps.

C21.4.11.1. Never leave home without advising their parents where they shall be and who shall accompany them.

C21.4.11.2. Travel in pairs or groups.

C21.4.11.3. Walk along busy streets and avoid isolated areas.

C21.4.11.4. Use locally approved play areas where responsible adults supervise recreational activities and police protection is readily available.

C21.4.11.5. Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot, even if the told by strangers that mom or dad sent them or said it was okay.

C21.4.11.6. Report immediately to the nearest person of authority (teacher, police) if anyone tries to pick you up or insists that you go for a ride with them.

C21.4.11.7. Ask schools to help provide security. Schools should be asked to do the following.

C21.4.11.7.1. Refrain from disseminating any information about students.

C21.4.11.7.2. Avoid any kind of publicity in which students are named or their pictures are shown.

C21.4.11.7.3. Consider procedures for releasing a student to someone other than his/her parents or custodian.

C21.4.11.7.4. Report to the police if any strangers are seen loitering around the school or talking to students. If such strangers are in a car, the teacher should note its make, color, model, and tag number and pass this information on to the police.

C21.4.11.7.5. Have teachers closely supervise outside play periods.

C21.5. TRAVEL SECURITY

C21.5.1. Appendix 6 provides in transit forces AT guidelines that when applied to official travel can decrease the likelihood of a terrorist attack on DoD personnel and their family members in transit. Additional AT measures provided in appendixes 12 through 14 are intended to reinforce the general philosophy underlying personal protective measures during both official and recreational travel.

C21.5.1.1. Keep a low profile.

C21.5.1.2. Be unpredictable.

C21.5.1.3. Be alert.

C21.5.2. The number of specific measures individuals and groups can take to implement this general approach to personal security while traveling is limited only by the imagination and creativity of the travelers.

C21.5.3. Readers are encouraged to expand the list of measures listed below, as well as to consider the specific circumstances under which a proposed measure might diminish, not increase the security of DoD personnel and their family members in travel status.

C21.5.4. General Travel Security Suggestions.

C21.5.4.1. The global distribution of DoD personnel, facilities, and contractors ordains much international and long haul domestic travel for DoD personnel. Even local travel may pose security risks. The following are some general comments that apply to all official travel. Additional travel security tips can be found in Appendices 12 through 14.

C21.5.4.2. Do not assume that acts of terrorism "can't happen to me." A common thread among accounts of individuals held hostage by Hizballah terrorists in Lebanon after their release was their own cavalier attitude towards warnings issued by the U.S. State Department and other governments' foreign ministries regarding travel to Lebanon.

C21.5.4.3. Realize the impact of security on your travel itinerary. Consider the security implications of destination, routing, and timing of travel and allow extra time for investigating, planning, and using alternative, more secure itineraries. Allow extra time between connections, if any, to allow for security inspections at airports, ports of entry, and other inspection points.

C21.5.4.4. Avoid routine schedules. Avoid following travel routines used by others when planning a trip or executing a plan assembled by others. Select unusual departure and arrival sites; schedule personal time and business activities at odd hours, during evenings, or on weekends. Be particularly sensitive to the possibility of surveillance. Arrival and departure times, as well routes taken to and from work/home, should be varied as often as possible. Different vehicles should be used to make targeting more difficult. For official business, consideration should be given to using unmarked Government vehicles where available.

C21.5.4.5. Travel in groups when possible where appropriate. Isolated travelers make easy targets; small groups provide a sufficient number of eyes and ears to be alert to local security matters.

C21.5.4.6. Avoid wearing military clothing. Wearing military uniforms during periods of travel and recreation could attract unwanted attention. Even wearing "military style" clothing may arouse more attention than desired.

C21.5.4.7. Carry identification. When asked for identification give only the information requested. Never surrender your entire wallet or purse or leave your wallet and/or purse unattended. Carry identification that gives your blood type, as well as any special medical condition or medication requirement.

C21.5.4.8. Carry extra medication, eyeglasses, and other medical necessities. If you take any medication regularly, take at least one week's extra supply with you. If you wear glasses, take an extra pair along. Keep all medication in its original container for customs inspections. If your medication is a narcotic, make sure you have a letter from your doctor in your possession. Carry all necessary medication with you in your purse or briefcase; do not put it in checked luggage.

C21.5.5. Travel Arrangements. The process of making travel arrangements can provide terrorists copious quantities of information about travelers, their authorities and responsibilities, their importance to the Department of Defense and the U.S. Government, and their personal tastes in matters of lifestyle. Such information is of incalculable value for purposes of targeting. The steps outlined below are intended to deny access to such information by terrorists. Other measures may be equally helpful in preserving the anonymity of DoD travelers, thereby complicating detection, identification, and targeting of such personnel for terrorist acts.

C21.5.5.1. If available, consider using U.S. Transportation Command/Air Mobility Command flights or military contract carriers.

C21.5.5.2. Try to arrange international travel through American military air terminals if possible.

C21.5.5.3. Avoid travel through high threat areas, if possible.

C21.5.5.4. Travel under a properly coordinated and authorized assumed name.

C21.5.5.5. Consistent with financial regulations, adjust travel reservations to foil terrorist targeting based on data stored in travel reservation computers.

C21.5.5.6. Do not discuss military affiliations with strangers.

C21.5.5.7. Consider using a tourist passport.

C21.5.5.8. Consider using a new tourist passport if your old passport contains entry/exit stamps or visas indicating travel to countries known to be targets of terrorist activity, e.g., Israel, South Africa, United Kingdom, etc.

C21.5.5.9. Carry only limited official documentation, such as military ID, official passports and leave papers on one's person (keep discrete). Remaining documents, such as travel orders, club cards, and billeting receipts should be stored in checked luggage. Maintain an unofficial form of identification, such as a driver's license, readily available for use.

C21.5.5.10. Do not use luggage that clearly labels its owner as a DoD civilian employee or military member. Examples include B-4 bags, duffel bags, and sea bags.

C21.5.5.11. Remove destination and baggage claim tags from luggage, as well as decals, stickers, and other markings that unambiguously identify the luggage as having been through the United States (i.e., U.S. Custom's stickers).

C21.5.5.12. Use baggage identification tags that require some manipulation before the name of the bag owner are visible. Try to use baggage tags that allow airline officials and customs inspectors to identify the owner of the bag by name, but otherwise do not provide information on the owner's address or country of origin.

C21.5.5.13. Do not include controversial or inflammatory reading material in carry-on bags or checked luggage on international travel.

C21.5.6. Additional Information Sources for Air Travel security.

C21.5.6.1. TSA Security Bulletins. The Department of Defense complies fully with the U.S. Government policy of "no double standard" with respect to warnings of terrorist attack. The Department of Defense shall disseminate all TSA security information in a manner that is consistent with this policy. If TSA security information deals with threats to DoD personnel only, then such information shall be disseminated in accordance with the DoD Component procedures. If TSA security information includes the general traveling public as well as U.S. Government or DoD passengers on international air carriers, then the Department of Defense shall release only that information cleared by the DoS for international terrorism information and the FBI for domestic terrorism information.

C21.5.6.2. DoS. The DoS monitors security conditions in countries with U.S. Embassies and Consulates. It provides a wide variety of security-related information and advice upon request. It is the releasing authority for all unclassified and unlimited distribution information on international terrorism. DoD-affiliated personnel seeking the most current public information on international terrorist threat concerns may call the Department of State in Washington, DC, Commercial, (202) 647-5226 or at http://www.travel.state.gov/ to obtain the most recent unclassified unlimited information regarding the international terrorist threat and international travel.

C21.5.7. Vehicle Travel Tips. DoD personnel make millions of trips each year by automobile. Most occur without any incident. Automobile trips have become so integrated with official business it is easy to dismiss use of vehicles as much more dangerous than a walk down a corridor from one office to another.

C21.5.7.1. Indiscriminate use of automobiles for the conduct of official business can be a major weakness in personal security efforts. As in the foregoing discussion of travel arrangements, consider steps to be taken to reinforce efforts of DoD personnel and their family members to make identification of DoD personnel difficult. It is essential to make determination of the prominence or importance of individuals by direct observation difficult, and to reduce the vulnerability of DoD personnel to successful attack while they are traveling between a security facility and their homes or a secure transfer point for a change in travel mode.

C21.5.7.2. Appendixes 12 and 13 contain several tips on reducing terrorist risk while operating a motor vehicle.

C21.5.8. Rail Travel. Rail schedules and routes are highly regular and predictable; they afford terrorists multiple opportunities to board and leave the train without arousing suspicion. Rail travel is strongly discouraged in high-risk areas. If rail travel is necessary, the general precautions outlined above for air travel are equally appropriate. In addition, the following measures should be implemented.

C21.5.8.1. Avoid travel through high-risk areas; leave the train and switch to foreign flag airlines if necessary to avoid such areas.

C21.5.8.2. Select a window seat in the middle section of open coach (U.S. style) rail cars; select a compartment towards the middle of a rail car in multi-compartment European rail cars; avoid taking seats near passageways between two rail cars if at all possible.

C21.5.9. Travel at Sea. Although DoD personnel and their family members do not frequently use ferries, transoceanic passenger liners, or cruise ships for official travel, there are many international waterways for which these modes of travel are appropriate for recreational travel. Unfortunately, there have been several instances of terrorist attacks on international passenger travel. The purpose of personal security precautions at sea remains unchanged. In addition to the travel precautions appropriate for flying outlined above, some additional precautions should be considered.

C21.5.9.1. Select ferry lines, cruise lines, or transoceanic passenger lines noted for good safety and public health records.

C21.5.9.2. Avoid travel through high-risk areas; avoid sailing on vessels that make port calls in high-risk areas.

C21.5.10. Hotel Procedures. It becomes readily apparent that AT security precautions taken by DoD personnel and their family members at home have direct counterparts when staying in hotels, motels, or guest quarters on U.S. military installations. The approach taken, from site selection, to installation of additional AT security precautions, to family "operations security" measures are quite similar. The list of measures that follows is long, but by no means exhaustive. DoD travelers should use their own imagination and develop additional measures that address the goals of antiterrorism measures spelled out above.

C21.5.10.1. Stay at DoD facilities while on TDY/TAD whenever possible.

C21.5.10.2. Consider staying in trusted hotels that don't have distinctively American names or predominantly American guests.

C21.5.10.3. Consistent with financial regulations, adjust hotel reservations and use an assumed or modified name to confuse terrorist targeting.

C21.5.10.4. Avoid taking street-level rooms, terrace level rooms with direct access to hotel grounds, or stairwells. If possible, stay in a room located between the fourth and tenth floors. When checking into guest quarters and hotels, avoid taking a street-level room if at all possible. Similarly, seek out alternatives to terrace, veranda, or other rooms which open directly on to areas which can be easily accessed from other rooms, common areas of the hotel, the street, or walkways along seawalls, beaches, lakes, etc. Use elevators in buildings rather than risk attack in stairwells, but know stairwell locations to use as alternative exits and/or entrances and in the case of fire or power outage. When in elevator, stand near the control panel; if threatened, push the alarm button.

C21.5.10.5. Retain control over all luggage upon arrival in a hotel lobby. After arriving at a hotel, the family should promptly move all luggage inside. However, it is again recommended that the family never let the luggage out of their sight. This shall ensure that no explosive device has been added to a bag and timed to detonate later in the family's room.

C21.5.10.6. When in a hotel, note all escape routes. Shortly after arriving in a strange hotel or other public place, try to find out the locations of fire escapes, emergency exits, fire alarms and fire extinguishers that you may need in an emergency.

C21.5.10.7. Vary your pattern of entering and leaving your hotel. Alternate entrances and exists to the building should be used if they are available to avoid setting an identifiable pattern of coming and going.

C21.5.10.8. Do not discuss travel plans over hotel phones.

C21.5.10.9. Use extra caution in hotel lobbies and other public places where bombs may be placed. Public lavatories have been favorite sites for terrorists to hide bombs in the past. Use of public rest rooms should be avoided to the maximum extent possible. Discovery of objects such as shopping bags, briefcases, boxes and items wrapped in newspaper which have been left unattended or which look out of place, should be reported to someone in authority. Exposed wires or noise, such as a hum or ticking should also cause an object to be considered suspect. DO NOT TOUCH SUSPECT OBJECTS. Notify authorities.

C21.5.10.10. Bellboys and other strangers in hotel lobbies should not be asked directions for specific places you intend to go. Preserve anonymity and camouflage the nature of your business travel. Ask directions from local police or from U.S. military personnel, if possible, not hotel staff or other guests.

C21.5.10.11. Do not conduct official business or meet casual acquaintances in your temporary living quarters; do not divulge the location of your quarters.

C21.5.10.12. Discourage efforts to enter your room while you are gone by preserving a "lived in" look in your room. Leave a light and radio or television on in your room when you go out. This shall give the appearance that the room is occupied. A light shall also make it easier for you to see what or who is in the room when you return. Keep your hotel room key with you at all times as well. This, too, shall make it more difficult to determine when the room is occupied and when the room is vacant. Never use the “Clean Room” sign, as it also announces you are probably not in the room.

C21.5.10.13. Keep your room neat. Neatness shall make it hard for things to be placed in your room without your knowledge. Luggage, briefcases and packages that appear to have been moved or otherwise disturbed should be treated with caution. A light dusting of talcum powder can be spread on the surface of suitcases, a dresser, or a desk just before you leave the room. A package that appears to have been opened and resealed should not be touched. Report such things promptly to military or civilian police.

C21.5.10.14. Hallways should be checked before exiting from an elevator or your room, for out of place objects or for persons who seem to be loitering. The management should be asked to remove any boxes, trash cans or other receptacles near your room which may be used to hide a bomb, or which might get in your way in case of a fire or other emergency evacuation.

C21.5.10.15. Packages should not be delivered to your room. Purchases should be picked up in person and wrapped in your presence. Suspicious deliveries to your room should be refused and the article removed from the building until it can be checked out. Doors should not be opened for strangers or to accept an unexpected delivery.

C21.5.10.16. Unexpected mail left for you at the desk or slipped under the door of your room should be viewed with suspicion. Mail, packages, or other articles with any of the characteristics listed in Table C21.T1. should be treated as potential improvised explosive devices.

C21.5.10.17. Suspect letters or packages should be isolated. They should not be put in water, because this could weaken wrappings allowing mechanical devices to operate (or otherwise cause detonation) if the letter or package is in fact a bomb. DO NOT OPEN OR TAMPER WITH THE SUSPECT ITEM IN ANY WAY. Notify military or civilian authorities and follow their advice.

**Table C21.T1. Possible Indications of Package or Letter Bomb**

| | |
|---|---|
| Excessive postage or no postage.<br>No return address.<br>Incorrect title or titles without name.<br>Hand printed or poorly typed address.<br>Postage cancellation stamp does not match location of return address.<br>Rigid envelope.<br>Excessive securing materials, such as tape or string. | Lopsided or uneven envelope.<br>Oily stains or discoloration.<br>Protruding wires or tinfoil.<br>Misspelled words.<br>Presence of peculiar odor of shoe polish, almonds or marzipan.<br>Restricting markings, such as "Personal," "Confidential," and so forth. |

C21.6. HIGH RISK PERSONNEL PROTECTION

C21.6.1. Reference (a) addresses the need to provide protection to those military officers, DoD civilians and their family members who are assigned to high risk billets and/or by virtue of their rank or grade, assignment or symbolic value, or relative isolation, are more likely to be attractive targets to terrorists.

C21.6.2. Reference (e) establishes two standards directly pertaining to “Training for High Risk Personnel and High Risk Billets” and “Executive Protection and High Risk Personnel Security.”

C21.6.3. Protective Service Operations entail the protection of dignitaries and other high-risk personnel in the Combatant Commander’s area of responsibility where significant threat exists. Those threats include assaults, kidnappings, assassinations, and attempts to embarrass the U.S. Government. This chapter is intended to supplement and consolidate information provided in other sections of this Handbook, with a focus on the mission of executive protection. Other sections of this Handbook should serve as the primary reference for many of the concepts discussed here. For purposes of this chapter, the term "executive" applies to all persons requiring additional security protection because they are assigned to High Risk Billets or have been designated as High Risk Personnel.

C21.6.4. The specific supplemental security measures that may be furnished to executives are subject to a wide range of legal and policy constraints. U.S. law establishes stringent requirements that must be met before certain security measures may be implemented. DoD

Component regulations, instructions, and legal opinions may further constrain implementation of the executive protective measures described in this Handbook. SOFAs and MOU between the U.S. Government and a foreign government shall also limit use of supplemental security measures. The U.S. Government contracted use of land or buildings for use by the Department of Defense may also limit application of certain security techniques. All of these constraints should be carefully considered when conducting security surveys, developing plans, and implementing additional security measures to protect executives.

C21.7. EXECUTIVE PROTECTION GOALS

C21.7.1. In the discussion that follows, several measures are outlined which can afford DoD executives additional protection against terrorist acts. The primary purpose underlying these measures is to:

C21.7.1.1. Delay at a Distance. Increase the time that elapses between the detection of an imminent terrorist attack and the actual onset of an attack to permit the arrival of response forces or the successful evacuation of executives.

C21.7.1.2. Delay to Permit Flight. Increase the amount of time that elapses between the onset of an attack and terrorist access to executives to permit the arrival of response forces or the successful evacuation of executives under attack.

C21.7.1.3. Delay, Hold, and Counterattack. Increase the duration of an attack by allowing executives, their staffs, and their families to remain secure in a safe haven until a response force can arrive to repulse the attack, apprehend the terrorists, and relieve the executives and those with them in the safe haven.

C21.7.2. Each supplemental security measure should be applied judiciously. There is a clear trade-off between increasing the level of executive office and residence AT measures and the need to preserve the anonymity of executives to avoid activity that may point to the executive's prominence or criticality.

C21.7.3. Supplemental AT measures can be expensive. The expense should be measured not just in terms of dollars, but also in terms of changes to organizational routine. Therefore, two primary questions must be addressed prior to the implementation of potentially bold, disruptive, and expensive supplemental security enhancements.

C21.7.3.1. What are the most cost-effective means of enhancing the security of executives at risk? How many changes in organizational routines and personal behavior shall

have to be made in order for security measures to be effective in reducing the vulnerability of executives and the risk of terrorist attacks?

C21.7.3.2. What are the anticipated costs of additional security measures in terms of dollars, organizational functionality, and mission capability?

C21.7.4. The security enhancements described in this Handbook shall be even more effective if the executives and their families take full advantage of the enhancements and reinforce the security measures. If executives do not change their behavior to accommodate additional security and protective measures, then their behavior can effectively defeat the purpose of the additional protection.

C21.7.5. Security measures can be enhanced to deter almost any terrorist threat. However, there may be a point where it is no longer economical to add layer upon layer of protective measures to deter a threat that is capable of overwhelming available protective measures. When facing a well-armed and capable terrorist threat, additional security measures coupled with an alternative security posture may provide the greatest deterrence to a terrorist attack.

C21.8. SUPPLEMENTAL SECURITY MEASURES FOR EXECUTIVES.

C21.8.1. General AT Principles. Sound AT principles apply to both executive offices and residences. The following principles should be reviewed prior to implementing supplemental AT measures.

C21.8.1.1. A thorough physical security survey serves as the foundation for a strong executive protection program. Physical security surveys of the offices and residences of DoD elements and personnel attached to U.S. Embassies should be performed by the DoS. Cognizant physical security and facilities engineering staffs should perform surveys of other DoD facilities.

C21.8.1.2. The optimal approach to a physical security site survey is from the viewpoint of a potential terrorist. The survey should examine avenues of approach to the installation, facility, or residence; points of access to the executive offices or residences; and how attacks on offices, residences, or other frequently used facilities could be mounted.

C21.8.1.3. A Technical TA is the next step in evaluating the need for supplemental executive AT measures.

C21.8.1.3.1. A Technical TA provides a thorough and detailed assessment of the weapons and tactics terrorists might use to attack the structure where DoD executives work and

reside. In order to enhance executive AT measures, security engineers and architects need technical threat data or assessments containing the following information.

C21.8.1.3.1.1. Potential terrorist modes of attack.

C21.8.1.3.1.1.1. Standoff weapons (mortar, rocket grenade, man-portable anti-tank/antiaircraft weapon, and sniper rifle).

C21.8.1.3.1.1.2. Close combat (sub-machine gun, pistol, and knife).

C21.8.1.3.1.1.3. Contact weapons (bombs, incendiary devices).

C21.8.1.3.1.2. Use of perimeter penetration aids such as power tools, hand tools, or explosives.

C21.8.1.3.1.3. Time of attack.

C21.8.1.3.1.4. Attacking force size.

C21.8.1.3.1.5. Anticipated degree of outside support or autonomy.

C21.8.1.3.2. Technical Threat Assessments also provides the basis for the development engineering design requirements. The data contained in the assessment permits the engineers to:

C21.8.1.3.2.1. Calculate forces to be withstood by load bearing structures in buildings.

C21.8.1.3.2.2. Identify appropriate security window glazing materials and calculate the thickness necessary to achieve desired penetration resistance for anticipated threats.

C21.8.1.3.2.3. Calculate the total amount of delay time that must be achieved through use of camouflage, deception, barriers, and semi-active security devices. This delay time shall permit security forces to respond to the scene of a terrorist attack in time to thwart the attack, capture or eliminate the terrorists, and rescue executives and their staffs or family members.

C21.8.1.3.3. A Technical Assessment of Responses provides engineers information on the anticipated performance of the security forces responding to a terrorist threat and the expected or desired behavior of the protected executives. The following paragraphs identifies a few of data elements required by security engineers:

C21.8.1.3.3.1. Response force size, capability, supporting weapons, response time and estimated effectiveness against range of attacks.

C21.8.1.3.3.2. Desired options for executive protection (evacuate on warning, evacuate on detection, evacuate only if attacked, evacuate only if forced to capitulate, or do not evacuate).

C21.8.1.3.4. Security planners require information on the expected duration of a terrorist attack on the structure housing executives prior to security force response. A comparison of terrorist threat capabilities and the security response force capabilities provides significant AT system performance parameters. These parameters can be quantified and used to develop detailed plans, drawings, and AT equipment acquisition plans.

C21.8.1.3.5. While AT enhancement measures are intended to provide additional protection for executives, the primary purpose of these measures is to increase time required by terrorists to penetrate the executive's office or residence.

C21.8.2. Office. The office environment should normally provide executives the greatest degree of AT protection. AT measures, guards, security checkpoints, office workers, aides, and/or secretaries all serve to insulate the executives from potential threats. Unfortunately, the considerable media attention provided to attacks on executives in government facilities may further entice terrorists. Hence, there may be a need to enhance security measures to offset the escalating capability of attack on more secure office areas by terrorist groups.

C21.8.2.1. The following measures can be selectively implemented to enhance executive office AT security:

C21.8.2.1.1. Increase Threat Detection Time by installing sensors on perimeters and barriers.

C21.8.2.1.1.1. Install surveillance systems, including seismic, acoustic, and infrared sensors at or beyond the outer perimeter; supplement these systems with closed circuit TV and/or imaging infrared systems tied into the alert security response force staging area.

C21.8.2.1.1.2. Extend restricted areas or exclusion zones and relocate access control points from the executive's office or residence to a point closer to the boundary of the installation.

C21.8.2.1.1.3. Increase and extend IDS from the within the installation or facility perimeter to the installation perimeter, allowing IDS to collection additional data in order to classify and identify an intrusion before response force arrives at scene or track of the intruder.

C21.8.2.1.1.4. Increase the number of surveillance and duress detection systems within the executive office area as well as approaches to the office area.

C21.8.2.1.2. Increase Threat Delay Time between perimeter and executive office building.

C21.8.2.1.2.1. Install vehicle barriers and realign roadways to eliminate straight, level stretches of road in excess of 50 meters in length.

C21.8.2.1.2.2. Increase concentric rings of fences, Jersey barricades, planters, bollards, and vehicle and/or personnel barriers.

C21.8.2.1.2.3. Install access control areas, supplemented by fire doors and/or security doors kept in a closed condition, between the entrance to the building housing executive offices and the executive office area itself.

C21.8.2.1.2.4. Confuse, Camouflage, and Deceive Observers by Hiding Executives' Locations.

C21.8.2.1.2.5. Consider relocating executives to buildings not usually associated with office activities, e.g., barracks, motor pool, R&D facilities.

C21.8.2.1.2.6. Consider constructing office areas in barrack, motor pool, R&D facilities, etc.

C21.8.2.1.2.7. Add executive style, decorative lighting and window treatments to several different areas of office buildings to minimize differences in external appearances between executive and non-executive offices.

C21.8.2.1.3. Increase Delay Time between the entrance to the building housing executives and the executive office area.

C21.8.2.1.3.1. Consider the addition of fire doors, access control points, dead-end corridors, and mid-corridor physical barriers to complicate access to executive office areas.

C21.8.2.1.3.2. Consider the addition of security devices which when activated disrupt the ability of intruders to retain their thought processes. These types of security devices

include flashing strobe lights, fog generators, noise generators, sirens, and fire extinguishing systems.

C21.8.2.1.4. Increase Delay Time and make access more difficult within the executive office structure.

C21.8.2.1.4.1. Replace standard doors and doorframes in areas leading to executive offices with high security doors and doorframes.

C21.8.2.1.4.2. Install high security grating; wire mesh, or other materials to bar access to executive's office area through utility tunnels or conduits.

C21.8.2.1.4.3. Strengthen walls, floors, and ceilings against improvised explosive devices, small arms fire, incendiary devices, and powered hand tools by substituting steel plate, concrete filled, steel reinforced cinder blocks, or other ballistic resistant materials for plaster/lath or wallboard room dividers.

C21.8.2.1.4.4. Add steel plates or other ballistic materials in crawl spaces above dropped ceilings; extend walls separating executive office area from other portions of an office building to prevent unobserved and undetected access to space of dropped ceilings.

C21.8.2.1.5. Increase hold time to contain penetrators.

C21.8.2.1.5.1. Add positive action controls to facility and doors and gates to ensure the gates and doors default to a closed and locked condition unless manually released.

C21.8.2.1.5.2. Add positive action controls to access control areas such that persons inside an access control area can neither advance nor withdraw without affirmative action by a security officer posted outside the access control area.

C21.8.2.1.6. Increase protection for building occupants against ballistic threats to windows and exterior walls.

C21.8.2.1.6.1. Substitute polycarbonate panels for glass windows; add a ballistic absorbing plastic film to the interior side of glass windows.

C21.8.2.1.6.2. Add exterior screens/plates to cover window areas and protect against gunfire and grenade/bomb fragments.

C21.8.2.1.6.3. Install blast curtains, metal blinds, metal shutters or other window treatments in executives' offices to protect interior space from glass shards and other small projectiles.

C21.8.2.1.7. Install emergency executive support facilities including a safe haven with duress system and telephone, and an emergency evacuation capability.

C21.8.2.1.7.1. Consider installation of helicopter landing aids on the roof of a structure or on an adjacent field far removed from parking areas.

C21.8.2.1.7.2. Consider installing a safe haven or other reinforced security structure adjacent to a helicopter landing facility to provide a secure waiting place for executives until a rescue helicopter with additional supporting air and ground units can extract the executives.

C21.8.2.1.8. Office Security Practices and Procedures.

C21.8.2.1.8.1. Executives should discourage their staff from disclosing the executive's whereabouts or activities when taking telephone messages.

C21.8.2.1.8.2. An executive's staff should use caution when opening executive mail. In particular, the staff should look for letters or packages that might contain improvised explosive devices.

C21.8.2.1.8.3. Strictly limit access to the executive office area.

C21.8.2.1.8.4. Limit publicity about the executive to a bare minimum; keep official biographies short; provide minimal information concerning the executive's personal interests and hobbies, and consider using outdated photographs if a publicity photograph is absolutely essential.

C21.8.2.1.8.5. The executive should avoid working alone late at night and on days when the remainder of the staff is absent.

C21.8.2.1.8.6. If late night work is necessary, the executive should work in conference rooms or internal offices where observation from the outside of the building is not possible. The executive should notify the security force that they shall be working late and ask that they look in periodically. Executives should enter and exit several offices, turning lights on and off before going to their own offices to disguise the purpose of their activities to outside observers.

C21.8.2.1.8.7. Executives should avoid placing office furnishings directly in front of exterior windows.

C21.8.2.1.9. Official business away from the office.

C21.8.2.1.9.1. Executives and their staff should discuss security requirements with the person planning the function.

C21.8.2.1.9.2. The executive should travel to and from the function with an escort.

C21.8.2.1.9.3. The executive's travel route should be chosen carefully to avoid potential hazard areas.

C21.8.2.1.9.4. The executive's planned attendance at official functions should not be publicized if at all possible.

C21.8.2.1.9.5. An attempt should be made for the executive to sit away from both public areas and windows.

C21.8.2.1.9.6. The sponsor(s) of the function should be encouraged to close the curtains to minimize the likelihood that anyone outside shall be able to see inside and determine who is attending the function and where they are located. This is extremely important for an evening function, when a well-lit interior can be easily viewed from a darkened exterior.

C21.8.2.1.9.7. The executive's staff should request that external floodlights be used to illuminate the area around the building where an evening function shall occur.

C21.8.2.1.10. Local official and unofficial travels.

C21.8.2.1.10.1. Executives should vary their daily pattern as much as possible, leaving and returning to their office or residence at different times.

C21.8.2.1.10.2. Executives should consider escorts to and from work, or travel with a neighbor.

C21.8.2.1.10.3. Executives should establish a simple duress procedure with their drivers. Any oral or visual signal shall suffice (i.e., something that the executive or driver says or does only if something is amiss).

C21.8.2.1.10.4. When using a taxi service, the executive should vary the Taxi Company. The executive should ensure that the identification photo on the taxi license matches the driver. If the executive is uneasy for any reason, the executive should simply take another taxi.

C21.8.2.1.10.5. When attending social functions, executives should attend the event with other guests if possible.

C21.8.2.1.10.6. Executive should examine their vehicle before entering to see if there has been any interference. A small mirror on a rod is a cheap and effective method to inspect underneath cars. Executive should not touch their vehicles until it has been thoroughly checked (look inside it, walk around it, and look under it).

C21.8.2.1.10.7. Executives should not leave personal items exposed in their vehicle, e.g., uniform items, service issued maps, official briefcases, etc.

C21.8.2.1.10.8. Executive should use the same precautions when driving their POV or a government owned vehicles (GOV).

C21.8.2.1.10.9. Executives should keep their car doors locked and not open windows more than a few inches.

C21.8.2.1.10.10. Executives should never overload a vehicle and ensure that all persons wear seat belts.

C21.8.2.1.10.11. Executives should always park vehicles in parking areas that are either locked or watched and never park overnight on the street. Before entering vehicles, executives should check for signs of tampering.

C21.8.2.1.10.12. Executives should keep the trunk of their vehicle locked.

C21.8.2.1.10.13. Where feasible, executives should drive in the inner lanes to keep from being forced to the curb.

C21.8.2.1.10.14. Executives should use defensive and evasive driving techniques. Executives should drill with their drivers by watching for suspicious cars and taking evasive action.

C21.8.2.1.10.15. Executives should avoid driving close behind other vehicles, especially service trucks, and be aware of activities and road conditions two to three blocks ahead.

C21.8.2.1.10.16. Executives should be aware of minor accidents that could block traffic in suspect areas. Crossroads are especially dangerous because they are preferred areas for terrorist or criminal activities since crossroads offer escape advantages to the attacker.

C21.8.2.1.10.17. Executives should take the following actions if they are attacked and a roadblock is encountered:

C21.8.2.1.10.17.1. Use the shoulder or curb (hit at a 30- to 45-degree angle) to go around the roadblock.

C21.8.2.1.10.17.2. If needed, ram the terrorist blocking vehicle in a non-engine area, at 45-degree angle, in low gear, and at a constant moderate speed. The main purpose of ramming the vehicle is to knock the blocking vehicle out of the way. In all cases, the executive's vehicle should not stop and the executive's vehicle should never be boxed in with a loss of maneuverability. Whenever an executive's vehicle veers away from a terrorist vehicle, the executive's vehicle is placed in an adverse position and it presents a better target to gunfire.

C21.8.2.1.11. Interurban, national, and international travel security practices and procedures.

C21.8.2.1.11.1. Executive airline seats should be booked at the last moment. If possible, the executive's seats should be booked using an alias.

C21.8.2.1.11.2. The use of an executive's rank or title should be restricted.

C21.8.2.1.11.3. Executives should not allow unknown visitors into their hotel room or suite.

C21.8.2.1.11.4. Executives should keep their staff and family members advised on their itinerary and subsequent changes to the itinerary. Executives should strictly restrict their itinerary information to only those individuals who require this information as a part of their official duties.

C21.8.3. Residential. The residential environment may provide executives a more limited degree of AT security. Executive residences are often located in more secluded areas of the installation or off the installation in the local economy and therefore may appear to present a "softer target" to terrorists. AT measures, guards, security checkpoints, household staff, aides, and/or secretaries can assist in insulating the executives from potential threats. An executive's entire lifestyle should be included in security surveys used to assess the need for supplemental AT security measures. The executive's residence and transportation between the residence and the office should also be examined for vulnerabilities.

C21.8.3.1. The same principles used to identify supplemental AT improvements in an office environment apply to executives' home environments as well. Recall that the purposes of AT enhancements are:

C21.8.3.1.1. Increase the amount of time terrorists need to initiate and complete an attack on executives while at home, thereby giving response forces more time to rescue executives and their family members.

C21.8.3.1.2. Reduce the potential threat to executives and their families as a consequence of a terrorist assault mounted against the residence.

C21.8.3.1.3. Increase the amount of time between detection of a threat and the onset of hostile actions.

C21.8.3.1.4. Delay the terrorists as long as possible; prevent their access to the executives and their family members on the one hand, and make the terrorists' departure from the scene to escape prosecution difficult; provided that in so doing, the lives of executives and their family members are not further jeopardized.

C21.8.3.1.5. Provide a safe haven that executives and their family members may flee for security pending the arrival of a security response force.

C21.8.3.2. Site Selection.

C21.8.3.2.1. Avoid selecting residences previously used by other senior U.S. Government or foreign government officials.

C21.8.3.2.2. Avoid selecting residences previously attacked by terrorist groups.

C21.8.3.2.3. While terrorist groups conduct surveillance to identify targets, mistakes have been made in the past. DoD personnel should avoid leasing residences previously used by representatives of Governments or organizations known to be targets of various terrorist groups. DoD personnel leasing residences formerly used by representatives of such Governments may be placing themselves unnecessarily at risk of being attacked as a result of mistaken identity.

C21.8.3.3. The following measures can be selectively implemented to enhance executive residential security:

C21.8.3.3.1. Increase time interval between detection of a threat and the onset of hostile terrorist acts.

C21.8.3.3.1.1. Ensure all door locks and window clasps are working.

C21.8.3.3.1.2. Ensure that all doors and windows are properly secured to their frames and the frames are properly anchored to the residential structure.

C21.8.3.3.1.3. Consider locking the driveway gates with a security lock to deter/delay entry.

C21.8.3.3.1.4. Consider installing a through-door viewing device or visitor intercom.

C21.8.3.3.1.5. Consider installing security lights to aid in viewing entrances.

C21.8.3.3.1.6. Increase the number of physical barriers between the outer perimeter of the residence and the interior of the residence.

C21.8.3.3.1.7. Add heavy, remotely operated gates to all fences, walls, and perimeter barriers, consistent with the penetration resistance of the barrier, between the residence, the street, and adjacent neighbors.

C21.8.3.3.1.8. Create a vestibule or "air lock" between living quarters and the exterior of a residence to ensure that no one can go from outside the residence directly into the residence.

C21.8.3.3.1.9. Add fire doors or security doors/gates between the bedroom areas and living areas of the residence.

C21.8.3.3.2. Increase the time required to penetrate exterior structural walls with explosives, hand-held power tools, and hand tools.

C21.8.3.3.2.1. Consider the addition of additional armor covered by aesthetically pleasing materials to exterior walls.

C21.8.3.3.2.2. Consider the addition of a separate reinforced masonry wall around the residence.

C21.8.3.3.3. Increase surveillance of residence and decrease response time.

C21.8.3.3.3.1. Consider installing closed circuit TV systems to permit remote viewing of all residential doors and windows accessible from the ground, nearby structures, trees, or easily acquired platforms (e.g., van parked next to a wall).

C21.8.3.3.3.2. Consider installing area intrusion detection systems between the residence perimeter and the residence itself. Increase the number and types of sensors. Add

backup communication channels between the intrusion detection system and a surveillance assessment and/or response dispatch center.

C21.8.3.3.4. Increase the durability and survivability of the residence to terrorist attack.

C21.8.3.3.4.1. Consider fitting windows with either Venetian blinds or thick curtains to reduce the visibility of activities within the residence and to reduce hazards of flying glass in the event of nearby explosions or gunfire.

C21.8.3.3.4.2. Install backup power systems for security devices, to include: surveillance systems, communication systems, and access control systems.

C21.8.3.3.4.3. Establish backup communications with the installation or embassy security department via secure landline or two-way radio.

C21.8.3.3.4.4. Consider placing a panic alarm bell to the outside of the house with switches on all floors of the residence. The panic alarm should also annunciate at the local police and the appropriate DoD or DOS security office.

C21.8.3.3.4.5. Install a safe haven in the home.

C21.8.3.3.5. Home Security Practices and Procedures.

C21.8.3.3.5.1. Executives should check persons entering their residences; e.g., electricians, plumbers, telephone maintenance personnel. If in doubt, the executive should call the person's office to verify the person's identity before allowing them into the residence.

C21.8.3.3.5.2. Executives should not open the door to a caller at night until the caller is identified by examination through a window or door viewer.

C21.8.3.3.5.3. The curtains in an executive's residence should be closed before turning on lights.

C21.8.3.3.5.4. Executives should consider placing the telephone where the executives shall not be seen from doors or windows when answering.

C21.8.3.3.5.5. Executives should investigate household staff (especially temporary staff).

C21.8.3.3.5.6. Executive should always be on the lookout for unusual activities and ensure their residence is locked and secure whenever the residence is unattended. Executives should be cautious upon returning to their residence.

C21.8.3.3.5.7. Executives should note and report suspicious persons.

C21.8.3.3.5.8. Executives should strictly control house keys.

C21.8.3.3.5.9. Executives should secure their vehicles in locked garages.

C21.8.3.3.5.10. Executives should be alert for the unusual, such as the movement of household furniture or the identification of unusual wires.

C21.8.3.3.5.11. The executive should consider the installation of a panic alarm bell on the exterior of the residence, with the placement of annunciator switches on every level of the residence.

C21.8.3.3.5.12. The area surrounding the executive's residence should be cleared of dense foliage or shrubbery.

C21.8.3.3.5.13. If the executive's residence is equipped with a duress alarm, the alarm should be routinely tested. Members of the executive's family should understand how the duress alarm works and the situations when the alarm should be activated.

C21.8.3.3.5.14. Executives should cooperate with law enforcement personnel and abide by their security recommendations concerning your home's security.

C21.8.3.3.6. Security at Social and Recreational Activities.

C21.8.3.3.6.1. Executives shall routinely be at risk to terrorist incidents, but they must continue with their professional as well as personal lives. The following measures are intended to permit executives to continue living as close to a normal life as possible while still remaining mindful of the risks to their security.

C21.8.3.3.6.2. Executives should ensure their hosts are aware of the executive's need for security and that the host establishes appropriate security measures.

C21.8.3.3.6.3. Executives should have their personal staff assist a civilian host if required.

C21.8.3.3.6.4. Executives should arrange for visitors to be subject to adequate security control.

C21.8.3.3.6.5. Executives or their staff should screen the invitation lists, if possible.

C21.8.3.3.6.6. Executives should vary the times of their athletic activities, such as golfing, jogging, etc.

C21.8.4. Transportation. Executives are most often at their peak accessibility to terrorists when they are in transit in official or privately owned vehicles. This section recommends steps to reduce the vulnerability of executives while in transit. Implementation of measures to enhance the transportation security of DoD executives must be in full compliance with U.S. laws and DoD directives.

C21.8.4.1. The domicile to duty transportation policy follows:

C21.8.4.1.1. As a general rule, Congress has strongly opposed provision of home to office (domicile to duty) transportation by the Federal Government to its officers and employees. Congress did, however, grant authority to the President and the heads of executive agencies and departments to provide domicile to duty transportation under certain circumstances. According to statute, "a passenger carrier may be used to transport between residence and place of employment. An officer or employee with regard to whom the head of a Federal agency can make a determination, [if] that highly unusual circumstances present a clear and present danger, that an emergency exists, or that compelling operational considerations make such transportation essential to the conduct of official business."

C21.8.4.1.2. The phrase, “highly unusual circumstances which present a clear and present danger”, is understood to mean that the perceived danger is:

C21.8.4.1.2.1. Real danger, not imagined.

C21.8.4.1.2.2. Immediate or imminent danger, not merely potential danger.

C21.8.4.1.2.3. A showing is made that the use of a government vehicle would provide protection against the danger that would otherwise not be available.

C21.8.4.1.3. The phrase, “emergency exists”, is understood to mean that there is an immediate, unforeseeable, temporary need to provide home-to-work transportation for an agency's essential employees.

C21.8.4.1.4. The phrase, “similarly compelling operational considerations,” is understood to mean that there is an element of gravity or importance to the need for government furnished transportation "comparable to the gravity or importance associated with a clear and present danger or an emergency situation." The Congress suggested further, "in such instances,

[it is expected] that home-to-work transportation would be provided only for those employees who are essential to the operation of the Government.

C21.8.4.2. Statutory Authorities and Limitations.

C21.8.4.2.1. The Secretary of Defense has statutory authority to allow a Combatant Commander to use Government owned or leased vehicles to provide transportation in an area outside the United States for members of the uniformed services and other DoD personnel under certain circumstances. Such circumstances include and are limited to a determination by the Combatant Commander that public or private transportation in the area is unsafe or is not available. Under such circumstances, the Department of Defense may provide transportation, usually in government buses or passenger vans to personnel and their family members if in so doing, it shall permit the Combatant Commander and his subordinate commanders maintain capability to perform or to undertake assigned missions. Such transportation is not intended to be used to convey persons from their residences to their places of work.

C21.8.4.3. DoD Non-tactical Armored Vehicle Policy.

C21.8.4.3.1. It is DoD policy to make non-tactical armored vehicles (NTAV) available where necessary to enhance the security of high-risk personnel, consistent with the requirements and limitations found in DoD Directive C-4500.51, "DoD Non-Tactical Armored Vehicle Policy (reference (at)). DoD issuances, Service regulations, and Combatant Commander guidance stipulate detailed procedures through which the Department of Defense manages NTAV programs.

C21.8.4.3.2. The Department of Defense categorizes non-tactical armored vehicles as heavy non-tactical armored vehicles (HAV) and light non-tactical armored vehicles (LAV) (these are normally armored sedans or sport utility vehicles).

C21.8.4.3.2.1. HAVs are fully armored vehicles intended to protect occupants from terrorist attacks using bombs, improvised explosive devices, grenades, and high velocity small arms projectiles. These vehicles are authorized on a case by case basis for designated high-risk personnel by ASD (SO/LIC). Factors to be considered are:

C21.8.4.3.2.1.1. Country Threat Level. HAVs are for use primarily overseas in countries with High Terrorist Threat Levels. Considerations include the threat capability and vulnerability of the target, and environment in which the threat operates.

C21.8.4.3.2.1.2. Protection Level. The threat must warrant the increased protection an HAV provides.

C21.8.4.3.2.1.3. Availability of Existing Assets. Diversion of existing HAVs is not possible.

C21.8.4.3.2.2. LAVs are less than fully armored vehicles (normally armored after purchase) intended to protect occupants from terrorist attacks using medium velocity small arms projectiles and at least some types of improvised explosive devices. LAVs are used to protect high-risk personnel who require protection but are not authorized the use of an HAV.

C21.8.4.3.3. Each of the Departments and some Defense Agencies (DIA, NSA, and PFPA) manage a portion of the DoD Non-Tactical Heavy Armored Vehicle Program. Each of these components has issued supplementary mandatory guidance on processing of requests for, as well as allocation and use of, these scarce assets.

C21.8.4.3.4. HAVs are complex systems requiring specialized maintenance and operation. As a general rule, HAVs shall be assigned to DoD personnel with a driver who has been properly trained in the operation and maintenance of the vehicle. The operator is not a chauffeur; he or she is an integral part of a supplemental security package provided by the Department of Defense to meet its obligations to protect its key assets. HAVs are only justified where highly unusual circumstances present a clear and present danger to the health and safety of a nominated protectee, or compelling operational considerations make such transportation essential for the conduct of official business.

C21.8.4.3.5. LAVs may also be provided by the U.S. Government to DoD executives where "highly unusual circumstances present a clear and present danger to the health and safety of a nominated protectee or compelling operational considerations" warrant their use. This category of non-tactical armored vehicle features "add-on" or “kit” armoring. While a less complex armoring system than those used in heavy NTAVs, "light" NTAVs afford substantial protection to occupants against a wide variety of threats. New developments in after-manufacture armoring kits for vehicles are occurring at a rapid pace, increasing the number of vehicle manufacturers and models for which "other NTAV" modifications are suitable.

C21.8.4.3.6. The use of Privately Owned Vehicles (POVs) by High Risk Personnel is not recommended during periods of high risk. Armored non-tactical vehicles shall be used when available. High Risk Personnel and their protective details should take the appropriate measures identified in appendixes 12 and 13.

## C21.9. AT TRAINING FOR EXECUTIVES

Chapter 18 provides specific information on the training programs available for DoD executives.

## C21.10. PROTECTIVE SECURITY OPERATIONS

C21.10.1. Each Department is authorized to provide Protective Security Details (PSD) for key senior military officers, DoD civilians, other U.S. Government officials or foreign dignitaries requiring personal protection.

C21.10.2. Each Department's Secretary upon recommendations of their counterintelligence and/or law enforcement investigation staffs makes assignment of PSDs to executives. PSDs are assigned to DoD personnel who meet requirements established by Service regulations. In general, PSDs may be assigned only to those executives whose position or assignment places them at risk and whose continued availability to the President, Secretary of Defense, and Combatant Commanders is vital to the execution of DoD missions. Appendix 15 provides further detailed information on the use of protective security details.

C21.10.3. General Security Concept. Protective Security Details provide high levels of security to an executive (protectee) by establishing a series of protective cordons around the executive. The establishment of defense in depth often means that the innermost protective layer is in close contact with the protectee at all hours of the day and night.

C21.10.4. Maintenance of Low Profiles. PSDs are trained in the art of maintaining low profiles. Not only are they concerned about the visibility of the protectee, they are also concerned about their ability to blend the protectees into the surrounding environment. The security of a protectee is severely damaged when the presence of the PSD is obvious and detectable, when all other measures to blend the protectee into the local environment have been successful.

C21.10.5. PSDs shall strive to limit the publication of the protectee's travel routes and means of transportation. If the protectee's travel routes and means of travel must be published, the PSD may suggest editorial changes to the itinerary scheduled for public release in order to limit details of the protectee's travel. For example, routes to and from announced appointments usually do not need to be released to the public.

C21.10.6. PSD Mission Duties.

C21.10.6.1. During the course of a PSD mission, members of the PSD may be asked to perform several different security functions. They may, for example, perform direct or indirect protection or escort duties. Direct protection is open and obvious; indirect protection is generally a surveillance measure. The security guard unit may operate as an interior guard and may consist of one or more PSD members stationed at fixed posts. PSD members should know the identity of each individual in the protectee's party; protectees can assist PSD members in the performance of their duties by introducing PSD members to each member of the official party.

C21.10.6.2. The attitude of the protectee is critical to the success of the PSD mission. Protectees do have a right and a responsibility to make their wishes known with respect to their personal security; they also have an obligation to listen carefully to the head of the PSD who is trained and highly qualified to assist the protectee in making reasonable judgments about manageable risks. PSD members understand their function is inherently intrusive, and that protectees can easily resent the loss of privacy that accompanies the protection offered. On the other hand, PSDs must accomplish their mission, not merely to protect executives, but to help safeguard mission critical assets—DoD executives.

C21.10.6.3. One of the PSD's most demanding functions is to limit the ability of individuals to circulate and approach the protectee. This is often very frustrating to protectees who wish to shake hands, engage in close conversations with visitors, and move freely without impediment in a social situation. PSDs are trained to strictly enforce limitations on the circulation of individuals, carefully checking each person for identification and ascertaining they are authorized to be present at the event.

C21.10.6.4. Executives with PSDs who must conduct official business or hold social engagements in large rooms can take several steps to minimize the potential disruptions that may occur as a result of good security practices.

C21.10.6.4.1. Executives should provide PSDs an attendee list prior to the function.

C21.10.6.4.2. One or more members of the executive's staff who know the attendees should be stationed with PSD members to identify the attendees as they arrive.

C21.10.6.4.3. Executive staffs should inform attendees that they shall be admitted only at specified entrances.

C21.10.6.5. PSD members are highly trained security specialists. While in the company of protectees, PSD members must be fully alert (no alcoholic drinks and/or drugs and medications), accommodating and helpful. Protectees should remember, however, that the PSD member's primary duty is the executive's protection, not to perform errands or to accomplish personal services for the executive. PSD members performing valet or other chores cannot effectively protect the executives.

## C21.11. EXECUTIVE PROTECTION SYSTEM INTEGRATION

C21.11.1. The previous sections focused on supplemental security measures used to address terrorist threats to executives or High Risk Billets and High Risk Personnel.

C21.11.2. Various methods and measures have been discussed to provide incremental security over and above the base level of security provided to all DoD personnel assigned to an installation, facility, activity, or a unit. The decision to allocate protective resources to enhance the security of DoD executives must be applied systematically to provide executive protection in the office, residence or while the executive is in-transit.

C21.11.3. Additional security measures implemented to protect executives in their offices or residences must be extended to official functions conducted. The security measures must also be extended to the executive's private life and depending upon the nature of the threat, the lives of their family members as well.

C21.11.4. The decision to provide executives domicile-to-duty transportation should be accompanied by additional security protection at the executives' residence, office, and official business and social functions. In view of the total costs of security measured in dollars, time, inconvenience to protected persons, their staffs, colleagues, and families, it may be prudent to radically alter living and working arrangements than to try to augment security in a piecemeal manner. For example, it might be prudent to house high-risk personnel within a DoD installation rather than to try to secure a detached, private residence at substantial distance from the operations base of a response force.

C21.11.5. The key to successful executive protection is to ensure the level of protection afforded, by AT measures, operational procedures in the office and at home, and protective security details, is constant. The level of protection must be matched to the threat, and must be sustainable.

C21.11.6. Executives have a special responsibility to set a personal example of combating terrorism awareness, attention to personal, family, office, information and operations security concerns, and of AT security measures implementation. By doing so, they make their colleagues and subordinates more aware, more conscious of their security environment, and less likely to be victimized by terrorist attacks.

# C22. CHAPTER 22
# PHYSICAL SECURITY

## C22.1. INTRODUCTION

C22.1.1. The physical security systems installed in and around DoD installations and facilities form the physical backbone of DoD AT efforts. The facilities, equipment, and personnel making up the installation security force are the first lines of defense against terrorist attack. DoD installation civilian managers and military commanders should develop an integrated physical security system in order to achieve the necessary levels of protection of DoD assets. The physical security system is built on the foundation that baseline security and preparedness posture is established based on the local threat, site-specific vulnerabilities, identification of critical assets, and employment of available resources. Further, these systems are scalable and proportional to increases in the local threat and/or unit operational capability. Physical security systems should be designed employing a layered "defense in depth" concept. The application of physical security systems and measures play an integral role in establishing a baseline security and preparedness posture in support of AT operations. This chapter provides an over-arching physical security concept. The AT officer should consult with Services', Combatant Commanders', and the Heads of the DoD Components' physical security and AT program guidance when developing a unit physical security system.

C22.1.2. DoD FPCON measures, RAM, and other AT measures are implemented based on the current threat, and vulnerability and criticality assessments. Such assessments are used to identify potential terrorist threats and vulnerabilities that may be exploited by terrorists, prioritize critical resources, and support the Commander's risk management decisions.

C22.1.3. The Installation Commander is responsible for incorporating physical security systems into the AT plan. Where there are multiple units located at an installation, the Installation Commander is responsible for coordinating unit physical security plans into the AT plan. Physical Security measures should integrate facilities, equipment, trained personnel, and procedures into a coordinated, synchronized effort to provide maximum AT protection. As a minimum and as applicable, Physical Security measures should address the following.

C22.1.3.1. The DoD FPCON System.

C22.1.3.2. RAM.

C22.1.3.3. Physical Security Measures for an Installation.

C22.1.3.4. Physical Security Measures for Facilities.

C22.1.3.5. Physical Security Measures for Ports.

C22.1.3.6. Physical Security Measures for Airfields.

C22.1.3.7. Physical Security Measures for Residential Security.

C22.1.3.8. AT Construction Standards.

C22.1.3.9. AT Considerations for Deployed/Expeditionary Forces (in-transit units).

C22.1.3.10. AT Considerations for Installation Infrastructure.

C22.2. PHYSICAL SECURITY CONCEPTS

C22.2.1. Policy. DoD 5200.8-R and DoD Directive 5200.8 (references (au) and (av)) prescribes standards and policy relating to the physical protection of military installations and assets of the Department of Defense.

C22.2.2. Policy Goals. The goal of a security system is to deploy security resources to eliminate or mitigate the potential for terrorism.

C22.2.3. Physical security system major components include:

C22.2.3.1. Integrated electronic systems.

C22.2.3.2. Entry and circulation controls.

C22.2.3.3. Barrier systems.

C22.2.3.4. Access delay and denial security systems.

C22.2.3.5. Dedicated security forces.

C22.2.3.6. Designated immediate response forces.

C22.2.4. Physical security measures are a combination of active and passive systems, devices, and security forces used to protect an asset or facility from possible threat. These measures include:

C22.2.4.1. Security forces and owner/user personnel.

C22.2.4.2. Military working dogs.

C22.2.4.3. Physical barriers, facilities hardening, and active delay or denial systems.

C22.2.4.4. Secure locking systems, containers, and vaults.

C22.2.4.5. IDS.

C22.2.4.6. Access or surveillance systems such as closed-circuit television or thermal imaging systems.

C22.2.4.7. Protective lighting.

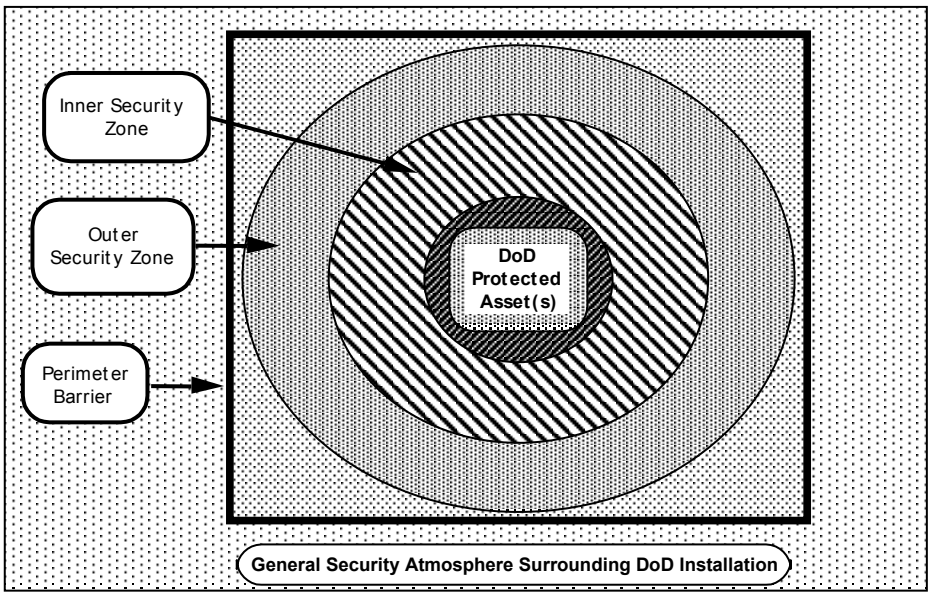
C22.2.4.8. Badging systems, access control devices, material or asset tagging systems, and contraband detection equipment.

C22.3. LAYERED SECURITY CONCEPT

C22.3.1. Reference (au) emphasizes the need to think of physical security as a system that provides defense in depth. In some cases, defense in depth can be obtained by constructing "islands" of extreme or high security within a "sea" of moderate security. This concept is also referred to as "enclaving."

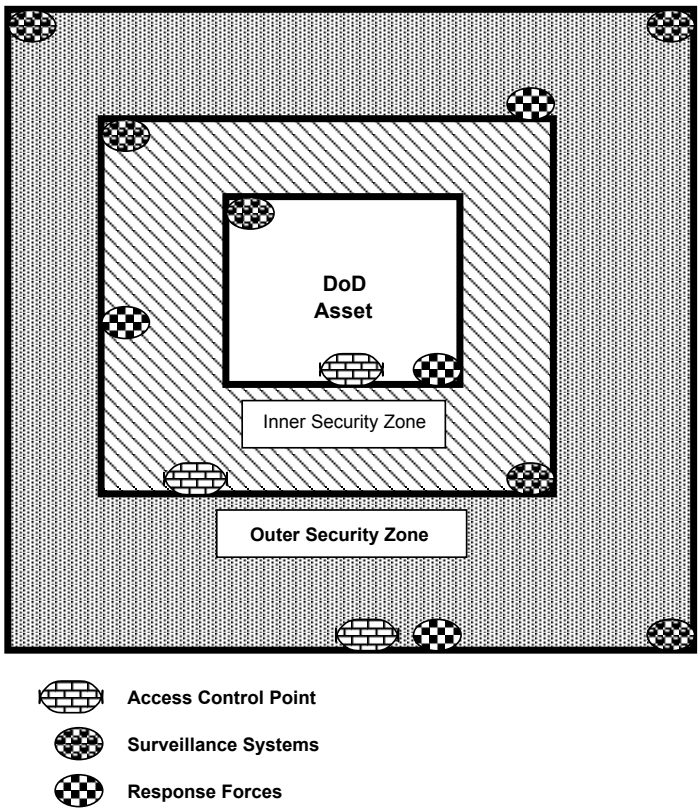
C22.3.2. Figure C22.F1. illustrates the general, layered defense approach to the implementation of a physical security system. The DoD assets to be protected are located within an innermost ring of security. Additional layers of security are provided at increasing distances from the asset to be protected. The number of layers, the components that comprise them, and their resistance to penetration depend on the threat and the importance of the asset to be protected.

**Figure C22.F1. A layered approach to protection of DoD assets.**




C22.3.3. Figure C22.F2. illustrates the concept of layered security with integrated physical security system components contributing to the security of a DoD asset. An outer perimeter is established and clearly marked. Just inside the outer perimeter is an outer security zone. Within this zone are surveillance systems to monitor activities within the zone and beyond the perimeter. Access control points have been constructed to control access from outside the perimeter to the outer security zone. A response force is positioned in the outer security zone to respond to intrusions or other security matters within the outer security zone and at the perimeter boundary if necessary.

**Figure C22.F2. High-security example of the layered security concept.**




C22.3.4. Figure C22.F2. illustrates a generic physical security system configuration that might be used to protect Level A assets (as defined by reference (au)) against advanced or maximum physical security threat levels. This configuration represents the typical case—integration of multiple technical and human physical security system components. It represents a physical security system that can provide high resistance to penetration and delay attackers long enough to permit a response force to arrive in time to apprehend or detain the perpetrators and recover assets and restore them to their secured status.

C22.3.5. Figure C22.F2. also depicts key security system components and an approach to integrating these elements into a physical security system. These components should detect threats; identify, classify, and assess intrusions; and delay intrusions long enough to permit response forces to arrive and complete containment and/or apprehension. If all else fails, these

security systems should delay intruders until overwhelming force arrives to rescue or recover the asset.

C22.3.6. The concept of a layered defense also includes protection from threats launched against DoD assets from any direction. Threats could come from below or above, and/or through perimeter fences, walls, or other barriers. Underground parking garages in office buildings, high-rise apartments, and hotels can harbor terrorists, as can large utility service structures such as tunnels, culverts, canals, or spillways. Ceilings or roofs can be penetrated and must also be protected. Even wide-open spaces on a large installation can represent potential danger for terrorists equipped with hang gliders, ultra-light aircraft, parachutes, or even helicopters.

C22.4. PHYSICAL SECURITY SYSTEM FUNCTIONAL REQUIREMENTS

For a physical security system to protect DoD assets, certain security functions must be performed.

C22.4.1. Threat Detection. As a rule, the earlier the detection of threats and the longer the range that they are detected, the greater the opportunities are to protect DoD assets and minimize the impact of terrorist acts against DoD personnel, materiel, and facilities. A wide variety of systems can be used to detect the presence of activity at a distance from the facility. Several factors can influence surveillance system performance.

C22.4.1.1. Seasonal and/or ambient weather conditions.

C22.4.1.2. The type of background against which surveillance systems are attempting to operate can also affect their sensitivity. Systems that rely on motion for cues to activity work well in rural environments; these same systems suffer data overload in an urban environment and cease to be very useful in short order.

C22.4.1.3. Environmental and/or geographical considerations regarding where the systems are placed. Systems can be placed making use of key terrain (hills, ditches, roads) or on fixed man-made barriers (fences, walls, barriers).

C22.4.1.4. The number and variety of systems based on where the detection of the threat is to occur.

C22.4.1.5. If the geography and siting of an installation does not permit detection of a threat at its periphery, as is the case when DoD facilities occupy only a portion of a commercial office building, then threat detection must occur at close quarters to the protected DoD asset. Under such circumstances, multiple IDS, based on different detection principles, can be

employed to provide threat detection and additional information needed for classification and assessment as discussed below.

C22.4.2. Threat Annunciation. The threat detected by the security system must be reported to a central location from where security forces can be dispatched. Responding security forces assess the on-scene situation and, if necessary, the on-scene commander can classify and/or request additional assistance. This capability should have redundancy.

C22.4.3. Threat Classification and Assessment. The presence of a threat is usually detected as a result of an alarm. Surveillance systems, including but not limited to visual surveillance systems and IDS, transmit data to an information-processing center where detection data is assessed. The purpose of such assessments is to determine whether the alarm is real or false, and if the intrusion is hostile or benign. Often, security personnel use Closed Circuit Television (CCTV) to assist them in their assessment role. CCTVs can also be slaved to the IDS. When a sensor alarm is activated on a slaved system, a CCTV camera is immediately focused on that area for the security guard assessing the IDS. IDS can help classify intruders, but rarely can they do so without human intervention and direct observation of the intruder via CCTV, a night-viewing device, an imaging infrared device, the human eyeball, or human interrogation.

C22.4.4. Threat Delay.

C22.4.4.1. Perimeter, exterior and interior physical barriers (erected or installed) such as fences, gates, walls, windows, doors, locking systems, ceilings, and floors provides delay. These physical barriers are evaluated as a system. The effectiveness of a barrier system is measured by the minimum total delay time it provides on any path into the protected area. Delay time is measured from the time the intruder is detected until the intruder has penetrated all of the barriers, including the time it takes to travel from barrier to barrier, and the protected area.

C22.4.4.2. Delay has three purposes: facilitate definitive threat classification and assessment; facilitate response by physical security response forces; and facilitate evacuation of protected DoD assets if evacuation is the most appropriate, cost-effective AT remedy.

C22.4.4.3. Delay of potential threats can be essential in making definitive threat classifications and assessments, and allows the response force an opportunity to take up defensive positions to protect DoD assets, defend facilities and personnel, counterattack, and conclude an incident with arrest and apprehension of the perpetrators.

C22.4.5. Threat Response. Response to threats begins immediately upon detection and is designed to:

C22.4.5.1. Stop further intrusion by the threat at the greatest distance possible from protected assets.

C22.4.5.2. Slow the rate of advance toward the protected asset as much as possible.

C22.4.5.3. Facilitate the evacuation of the protected asset to safe areas.

C22.4.5.4. Secure the protected asset and contain the threat.

C22.4.5.5. Contain the threat, prevent additional hostile resources from arriving, and prepare to apprehend the threat and relieve the protected asset.

C22.5. INTRUSION DETECTION SYSTEMS

C22.5.1. IDS are used to accomplish the following:

C22.5.1.1. Permit more economical and efficient use of security personnel through the employment of mobile responding security forces instead of fixed guard posts or patrols.

C22.5.1.2. Provide additional controls at critical areas or points.

C22.5.1.3. Substitute for other physical security measures that cannot be used because of safety regulations, operational requirements, building layout, cost, or similar reasons.

C22.5.1.4. Provide insurance against human error.

C22.5.1.5. Enhance the security force capability to detect and defeat intruders.

C22.5.1.6. Provide the earliest practical warning to security forces of any attempted penetration of protected areas.

C22.5.2. Types of IDSs. There are four types of IDS: local alarm, central station, police connection, and proprietary station.

C22.5.2.1. Local Alarm. In this system, the protective circuits and alarm devices activate a visible or audible signal in the immediate vicinity of the detected intrusion, usually on the exterior of the building. The alarm transmission or communication lines do not leave the building. Response is by local security forces that may be in the area when the alarm is sounded; otherwise, the security force shall know of the alarm only if a passerby reports it or if it is found during routine checks. The disadvantage of this system is that intruders know exactly when the alarm is activated and can easily elude capture. A local alarm system should be used only when guards are able to respond in a timely manner.

C22.5.2.2. Central Station. In this type of system, the operation of alarm devices and electrical circuits is automatically signaled to, recorded, maintained, and supervised from a central station owned and managed by a commercial firm with guards and operators in attendance at all times. These personnel monitor the signals and provide the response force to any unauthorized entry into the protected area. Connection of alarm equipment to the central station is usually over leased telephone company lines.

C22.5.2.3. Police Connection. In this type of system, the alarm devices and electrical circuits are connected via leased telephone company lines to a monitoring unit located in nearby civilian police stations. An agreement with the local police department must be arranged prior to establishment of this type of system.

C22.5.2.4. Proprietary Station. This system is similar to a central station operation, except that the IDS monitoring or recording equipment for all IDS at the installation is located within a constantly staffed security force communications center maintained and owned by the government installation. The installation security force responds to all IDS activations. Connection of the alarm sensor equipment to the security force central monitoring station is normally over leased telephone company lines or by separate cable owned and installed by the installation. A computerized IDS must be safeguarded against tampering.

C22.5.3. IDS Sensors.

C22.5.3.1. IDSs have several components, including sensors, data transmission subsystems, display and assessment subsystems, power subsystems, communications subsystems, and maintenance systems. IDS sensors are divided primarily into two groups—exterior sensors and interior sensors—depending on their environmental capability.

C22.5.3.2. Exterior sensors are those that function in an outside environment. These sensors and their associated processing equipment are weatherproofed and are less sensitive than interior sensors to changes in climatic conditions. Exterior sensors are used for early detection of intruders before they reach a protected structure. They are designed to provide fairly uniform protection coverage in outdoor areas. Exterior sensors are used to establish an intrusion detection line along fences, walls, and water or other land boundaries surrounding a protected structure.

C22.5.3.2.1. Perimeter sensors are exterior sensors normally installed on fences, walls, or gates. They detect different types of fence movement from an intruder climbing,

cutting, lifting up, or otherwise violating the fence. They can also be used within structures to establish inner security zones or to monitor movement within a large, open structure.

C22.5.3.2.2. Line sensors are exterior sensors that form an extended boundary through which intrusion can be detected upon a break in or interference with the sensor line, an object passing through a magnetic field, or a change in the pattern in an electronic field.

C22.5.3.2.3. There are various types of exterior sensors:

C22.5.3.2.3.1. Fence-strain sensitive cable sensor.

C22.5.3.2.3.2. Fence-mechanical sensor.

C22.5.3.2.3.3. Electric field sensor.

C22.5.3.2.3.4. Taut wire on chain-link fence.

C22.5.3.2.3.5. Taut wire on brick or masonry wall.

C22.5.3.2.3.6. Microwave sensor.

C22.5.3.2.3.7. Active infrared barrier sensor.

C22.5.3.2.3.8. Exterior balanced magnetic switch.

C22.5.3.2.3.9. Ported coax sensor cable.

C22.5.3.3. Interior sensors require a sheltered environment. They are designed for use in environments with small variations in temperature and relative humidity. Interior sensors are not weatherproof and are best suited for well-defined volumes along the interior perimeter of the structure. Interior sensors should be used for secondary layers of intrusion detection within the structure.

C22.5.3.4. Sensors use various methods of detection. Exterior sensors commonly use seismic, magnetic, microwave, infrared, electric field, electromagnetic, and vibration detection methods. Interior sensors primarily use capacitance, magnetic, ultrasonic, shock or vibration, and infrared techniques. Combinations of these methods may also be designed into individual sensors. They can be configured in electronic tiers, requiring an intruder to pass through each tier in progressive succession, thereby increasing the likelihood that the intruder shall be detected.

C22.5.3.4.1. Penetration sensors are interior sensors designed to react to mechanical or acoustical vibration, sensor movement, or sensor destruction.

C22.5.3.4.2. Volumetric sensors are interior sensors designed to react to the motion of an intruder. They may be based on infrared, seismic, acoustic, or sensing technologies.

C22.5.3.4.3. Duress switches similar to those used in banks set off an alarm at the touch of a button. They allow individuals to communicate situations of duress to forces that can render assistance. Both fixed and portable switches can be used in this application. Fixed duress switches are normally wired to the IDS duress circuit and are permanently mounted for activation of the duress alarm when needed. Portable hand duress switches electronically transmit to a receiver that is wired to the IDS duress circuit. Upon activation of a switch button, the small, wireless transmitter sends a radio signal to the receiver, triggering a duress alarm. Transmitters are designed to be either carried or mounted in suitable locations.

C22.5.3.5. Table C22.T1. lists several types of interior intrusion-detection sensors, the purposes for which such sensors are appropriate, the principles by which each sensor operates, common false alarm causes, and appropriate applications.

**Table C22.T1. Selected Interior Intrusion Detection Sensors.**

| Type of Equipment | Purpose | Principle of Operation | Common Causes of False Alarms | Appropriate Applications |
|---|---|---|---|---|
| Interior capacitance | Proximity sensors | Used in conjunction with metal objects such as files. The metal becomes part of the tuned circuit and any change in the capacity of the tuned circuit (e.g., a body touching the object) causes an alarm. | Relatively free of false alarms; protected items must be kept clean and mounted off the floor on blocks. | File cabinets, safes, metal grates or screens, hardware or machinery. |
| Vibration sensors | Point protection | Sensors are mounted within or upon walls to detect (via vibration) forced entry. | Vibrations caused by large machinery, HVAC equipment, thunder or heavy wind. | Storage areas, vault-like rooms; controlled access areas. |

| Type of Equipment | Purpose | Principle of Operation | Common Causes of False Alarms | Appropriate Applications |
|---|---|---|---|---|
| Door and window sensors, balanced magnetic switch | Entry and point protection | Recessed and surface-mounted sensor establishes an electromagnetic contact between the fixed frame and the movable door or window unit. | Normally low susceptibility to false alarm. Poor installation or maintenance can lead to reduced effectiveness or bypass. | Interior and exterior doors; windows; overhead doors. |
| Foil | Entry and point protection | Surface-mounted on glass. Intrusion by breaking glass breaks contact and activates alarm. | Poor installation, old varnish breaks down, cleaners break foil, corrosives on connectors. | All windows and glass doors. |
| Glass breakage detectors | Entry and point protection | Surface-mounted on glass. Uses ultrasonic signal generated by glass breakage to signal an alarm. | Some products can be activated by window vibration. | All windows and glass doors. |
| Switch mats | Point protection | Pressure-sensitive floor mats activated by intruder's body weight. | Low false-alarm potential. Moisture could cause short circuit. | In front of safes, files, and cash registers; in doorways and stairwells; under windows; under carpeting; in executive or other offices. |
| Wireless duress alarms | Point protection | Wireless alarm-activating systems send alarm signals over the air to a remote central receiver. | Accidental activation by the user. Walls and other barriers shall reduce effective range. | Guards on patrol without communications; as a money clip in retail or cash depositories; local couriers; VIPs. |

| Type of Equipment | Purpose | Principle of Operation | Common Causes of False Alarms | Appropriate Applications |
|---|---|---|---|---|
| Ultrasonic sensors | Space protection | Emits inaudible sound waves that are sensed by a receiver. Intruder alters wave pattern, activating an alarm. | Areas containing rotating or moving machinery; escaping air or steam; large glass windows or thin walls that can vibrate; radio transmitters; magnetic fields from generators; motors or fluttering drapes. | Rooms with unbroken line of sight. Large objects such as stacks of boxes or furniture can create shaded areas on the side away from the transceiver. |
| Photo-electric (active infrared sensors) | Space protection | Directs invisible infrared light beam at a receiver. Any interruption of the beam results in an alarm. | Alignment between transmitter and receiver is critical; frequent checks required. Heavy dust, headlights. | Multiple units to be used in doorways; loading corridors, along inventory stacks; a line-of-sight sensor using a pencil zone of protection. |
| Microwave sensors | Space protection | Transmits an electromagnetic field into the area to be protected. Intruder motion activates alarm. | Areas containing small openings that can allow escape of microwave energy to outside areas; fluorescent lights; heavy machinery; wall vibration; thin walls or glass; radiated or conducted electro-magnetism. | Long corridors, aisles, or totally enclosed areas, or areas in which a sensor can be directed away from windows and thin walls in well-constructed buildings. Protection not affected by air currents or temperature differential. Good for large spaces. |

| Type of Equipment | Purpose | Principle of Operation | Common Causes of False Alarms | Appropriate Applications |
|---|---|---|---|---|
| Passive infrared sensors | Space protection | Combination of heat generated by a body plus motion of the body activates the sensor. | Objects in a room heated by sunlight through windows; space heaters; rodents and other animals; passive infrared sensors have high resistance to false alarms | Rooms or areas with high air turbulence, all interior spaces. Sensor should be mounted so that direct sunlight is not in the sensor's direct field of view. |
| Sonic (audio) sensors—active | Space protection | Fills the area with sound waves. Disruption of these waves by an intruder activates the alarm. | May be activated by extraneous sounds from outside the protected area; objects that can move, such as fans or equipment; sound waves can be disturbing to persons. | Interior spaces where stay-behinds are a threat or where items in the area may be in different locations from day to day, such as warehouses or shipping in adjacent areas. |
| Remote audio (listen-in)—passive | Space protection | Uses leased telephone line and microphone to provide remote listening to detect intruder movement. However, federal wiretap statute may be implicated if it picks up conversations. | Extraneous noise (passing vehicles, machinery, and noise in adjacent areas) mistakenly classified as an intrusion. | Provides a means to verify other intrusion systems prior to response. |

C22.5.3.6. Data or signal transmission subsystems link sensors with control and monitoring consoles. The transmission medium is used to send control signals and data to and from all sensors, control points, and annunciator panels. These subsystems may be hardwired landlines, radio-frequency links, fiber-optic cables, or any combination thereof. Most recently, transmission of data-encrypted alarm signals via satellite has been developed and is now available commercially.

C22.5.3.7. Annunciator, control, and display subsystems provide equipment for central operational control and monitoring of the IDS. Through this equipment, security force personnel are instantly alerted to the status of any protected area. These subsystems should be located in a restricted area and closed off from public view. Alarmed spaces should be designated by zones to facilitate identification of penetrated areas, assessments of vulnerability resulting from intrusions, and dispatch of response forces in a timely manner.

C22.5.3.8. The primary power source plays a vital role in the selection process. A planner must ensure that an IDS is capable of operation on the power (frequency and voltage) that is available. Within the United States, 60 Hz (cycles) and 110 V alternating current is the standard. Outside the United States, frequencies may be 50 Hz or 60 Hz and voltages can range from 110 V to 440 V, in any combination.

C22.5.3.9. In many overseas areas, line voltages can fluctuate widely and voltages for a 240 V system can drop to 180 V, then surge to near 300 V. Where this occurs, surge arrestors and line conditioners shall be required to protect the IDS equipment. If the system selected is not capable of operating on available power, then some means of converting the power to a usable form must be provided. Sufficient power must be available to operate the equipment in each area to be protected as well as to operate the control-monitoring station. The power required by each item of equipment must be included in determining the total system load.

C22.5.3.10. Many sensors and display units operate on direct current. When these units are used, it is necessary to provide sufficient direct current rectifiers at each location to convert locally available alternating current to the direct current required by the sensors and display units. Many of today's control units and sensors use microprocessors to accomplish their function. Although powerful in performance, they are susceptible to damage from electrical transients such as surges or spikes that result from interference or noise on the power line. This vulnerability can be reduced through the incorporation of surge protectors or lightning arrestors in the design.

C22.5.3.11. Emergency backup power provides protection to the IDS even when the primary power fails or is cut off. It is crucial that an alternative power source be provided to support the IDS. If there is an uninterrupted power supply available, then connecting the IDS to it should be a prime consideration. Most systems contain a backup battery that is continuously trickle-charged by the primary power system. An 8-hour battery backup is mandatory. However, if the primary power is subject to being out for longer periods, a 16- or 24-hour

backup should be procured or arrangements made to provide a guard force as additional protection.

C22.5.3.12. Use of an emergency backup generator can provide the necessary power when the primary power fails. Battery backup is still required to keep the system up until the generator is started. Expected power outages, system load requirements, and fuel availability shall determine the capacity and type of generator required.

C22.5.3.13. Protection from tampering with the IDS, the access system, and the assessment system should be designed into components of these systems so that their effectiveness cannot be compromised. In typical applications, a switch is located within equipment covers or doors that are vulnerable to unauthorized entry. A tamper alarm is registered at the annunciator panel when a cover or door is pried off or removed.

C22.5.3.14. Alarm assessment is an essential function of a physical security system relying on IDSs. It is imperative that the cause of the alarm be investigated. Accurate and rapid assessment is essential to prevent the commitment of response forces as a result of false or nuisance alarms.

C22.5.3.15. When an intrusion alarm is received, security personnel must assess the validity, severity, and nature of the event causing the alarm. Visual methods are commonly used, either by direct sighting or by CCTV.

C22.5.4. IDS Problems. There are problems inherent in any IDS. Predominant problems include false and nuisance alarms, vulnerable sensor location, incomplete sensor coverage, and, to a lesser degree, system compatibility. Poor sensors, IDS design, or installation shall generate a major cost penalty where a large guard force is required for assessing nuisance alarms.

C22.5.4.1. Communications Link Considerations. Information concerning intrusion or intrusion attempts must be reliably transmitted from the sensor to the control unit in a manner that is resistant to compromise, manipulation, and degradation. Line security and secure communications are terms used to describe this capability, and the need may exist to consult personnel who are qualified in their application.

C22.5.4.2. Line Security. There are various line supervision techniques available that shall detect or inhibit the resulting interception and manipulation of signals. In direct current circuits, the use of end-of-line resistors shall make it more difficult to breach or tap the line without triggering an alarm. Data links between control units and sensors or remote display can be protected by use of polling schemes, time-division multiplexing, data encryption, and

frequency modulation of information. The most effective line security is provided by encrypted data transmission.

C22.5.4.3. Physical Protection of System Components. Wiring should be protected from exposure to physical damage and manipulation. Use of conduit or metallic tubing is recommended. Tamper detection devices should be installed on all junction boxes.

C22.5.4.4. Environmental Influences. IDS components are commonly exposed to environmental influences, both natural and manmade, that can have an adverse effect on system operation. Protection from electromagnetic interference can be provided by means of proper shields, grounding, conduit, and physical separation. Other factors, including high humidity, saltwater-laden atmosphere, dust, temperatures, and animal and insect pests, should also be evaluated during system design to assure a system best suited to local conditions.

C22.5.5. IDS Maintenance. Maintenance and testing of systems is essential. Service and manufacture warrantees should be consulted for specific maintenance and testing requirements.

C22.6. LIGHTING SYSTEMS

C22.6.1. Protective lighting should enable guard force personnel to observe activities around or inside an installation without disclosing their presence. Adequate lighting for all approaches to an installation not only discourages attempted unauthorized entry but also reveals persons within the area. However, lighting should not be used alone. It should supplement other measures such as fixed security posts or patrols, fences, and alarms.

C22.6.1.1. Protective Lighting Approaches. Good protective lighting is achieved by adequate, even light upon bordering areas, glaring light in the eyes of the intruder, and relatively little light on security patrol routes. In addition to seeing long distances, security forces must be able to see low contrasts, such as indistinct outlines of silhouettes, and must be able to spot an intruder who may be exposed to view for only a few seconds. Higher levels of brightness improve all of these abilities.

C22.6.1.2. In planning protective lighting, high-brightness contrast between intruder and background should be the first consideration. The volume and intensity of lighting shall vary with the surfaces to be illuminated. Dark, dirty surfaces, or surfaces painted with camouflage paint require more illumination than installations and buildings with clean concrete, light brick, or glass surfaces. Rough, uneven terrain with dense underbrush requires more illumination to achieve a constant level of brightness than do manicured lawns.

C22.6.2. Types of Lighting.

C22.6.2.1. Continuous Lighting (Stationary Luminary) is the most common protective lighting system. It consists of a series of fixed lights arranged to flood a given area continuously with overlapping cones of light during the hours of darkness. Two primary methods of employing continuous lighting are glare projection and controlled lighting.

C22.6.2.2. Standby Lighting (Stationary Luminary) is similar to continuous lighting. However, the luminaries are not continuously lighted, but are either automatically or manually turned on only when suspicious activity is detected or suspected by the security force or alarm systems.

C22.6.2.3. Emergency Lighting. Emergency lighting may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on alternative power sources, such as installed or portable generators or batteries.

C22.6.2.4. Motion Activated Lighting. Modern activated lighting can be very effective in deterring intruders and drawing to an area where as intruder has tripped a motion activated light.

C22.6.3. Wiring Systems.

C22.6.3.1. Both multiple and series circuits may be used to advantage in protective lighting systems, depending on the type of luminary used and other design features of the system. The circuit should be arranged so that failure of any one lamp shall not leave a large portion of the perimeter line or a major segment of a critical or vulnerable position in darkness. Connection should be such that normal interruptions caused by overloads, industrial accidents, and building or brush fires shall not interrupt the protective system. In addition, feeder lines should be located underground (or sufficiently inside the perimeter in the case of overhead wiring) to minimize the possibility of sabotage or vandalism from outside the perimeter. The design should provide for simplicity and economy in system maintenance and should require a minimum of shutdowns for routine repairs, cleaning, and lamp replacement. It is necessary in some instances to install a duplicate wiring system.

C22.6.3.2. Power sources should meet the following criteria:

C22.6.3.2.1. Primary—usually a local public utility.

C22.6.3.2.2. Alternative—the following should be provided:

C22.6.3.2.2.1. Standby batteries or petroleum-driven generators.

C22.6.3.2.2.2. If cost-effective, the ability to start automatically upon failure of outside power.

C22.6.3.2.2.3. Continuous lighting.

C22.6.3.2.2.4. Additional security precautions, since security may be inadequate for sustained operations.

C22.6.3.2.2.5. Testing to ensure efficiency and effectiveness; the frequency and duration of test depend on:

C22.6.3.2.2.5.1. Mission and operational factors.

C22.6.3.2.2.5.2. Location, types, and condition of equipment.

C22.6.3.2.2.5.3. Weather (temperature affects batteries very strongly).

C22.6.3.2.2.6. A controlled location for additional security.

C22.6.3.2.2.7. Generator- or battery-powered portable or stationary lights:

C22.6.3.2.2.7.1. For use in a complete power failure.

C22.6.3.2.2.7.2. Includes alternative power supply.

C22.6.3.2.2.7.3. Available at designated control points for security personnel.

C22.6.3.3. Under ideal circumstances, power supplies related to physical security systems should be routed to the installation separately from other utility services. In addition, power supplies for physical security systems should enter each protected facility as well as each protected enclave or restricted area within a facility separately from other power and utility services.

C22.6.4. Control Systems. Controls and switches for protective lighting systems should be inside the protected area and locked or guarded at all times. An alternative is to locate controls in a central station similar to or as a part of the system used in intrusion-detection alarm central-monitoring stations. High-impact plastic shields may be installed over lights to prevent destruction by stones or air rifles.

C22.7. INCIDENT RESPONSE FORCES

C22.7.1. Response forces are an integral part of your installation physical security plan. Response forces are briefly discussed below. For detailed reading, consult Combatant Commander, Service, or Agency guidance. Use of security forces as part of the physical security system can be very effective but also very expensive. Security forces have three interrelated but very different functions to perform as part of their role in the physical security system.

C22.7.1.1. They function as barriers. Their presence is a visible and often tangible reminder of harm that could befall an intruder who ventures onto a DOD military installation without proper authorization.

C22.7.1.2. They are an essential element in the IDS. Typically, they are responsible for making an on-the-spot assessment of initial alarms. Their judgment shall figure prominently in installation responses.

C22.7.1.3. They are usually the initial response force, local augmentation forces, and regional/national special capability response forces. Therefore they are responsible for initial incident control and containment, as well as augmentation and more specialized functions in the event of a terrorist incident.

C22.7.2. Security forces are an essential element of the physical security system. Services, Combatant Commanders, and agencies promulgate extensive criteria for selection and employment of security forces and should be consulted for specific guidance.

C22.8. PARKING

C22.8.1. As a rule, parking should be restricted to the areas that provide the least security risks to DoD personnel.

C22.8.2. If possible, a visitor parking facility should be established outside the installation perimeter. If space does not permit this, visitor parking should be restricted to an area as close to the main installation gate as possible, without endangering the gate security personnel and others awaiting access. Pedestrian screening should be conducted between the visitor parking area and other sections of the installation if possible.

C22.8.3. All parking within the perimeter walls should be restricted to employees, with spaces limited to an area as far from the building as possible. Parking for patrons and visitors, except for pre-designated VIP visitors, should be restricted to outside of the perimeter wall. If

possible, parking on streets directly adjacent to buildings, especially those housing highly valued assets should be forbidden. There should be no underground parking areas in building basements or ground-level parking under building overhangs. Such space should be converted to secured storage; monitored employee, staff, or dependent recreational areas; or additional office space if possible.

C22.8.4. When parking areas are established, security of visitors as well as DoD personnel should be considered:

C22.8.4.1. Avoid extremely remote parking for visitors.

C22.8.4.2. Install an emergency communication system (intercom, telephones, etc.) at readily identified, well-lit, CCTV-monitored locations to permit direct contact with the security department.

C22.8.4.3. Provide parking lots with CCTV cameras capable of displaying and videotaping lot activity on a monitor in the security control center. Lighting must be of an adequate level and direction to support cameras while giving consideration to energy efficiency and local environmental concerns.

C22.8.4.4. Channel pedestrians toward a pedestrian access control checkpoint or installation facility or building access control point.

C22.8.4.5. Fences; Jersey barriers; low, thorny hedges; and other barriers may be used to guide pedestrians and maintain control over their movements.

C22.8.5. Although in-building or underground parking is strongly discouraged, there are circumstances in which there is no alternative. The following recommendations are made to enhance the security of building occupants.

C22.8.5.1. A complete vehicle control system should be provided for those buildings in which the parking garage is part of the building itself.

C22.8.5.2. Nondescript vehicle identification should be provided that must be displayed before entering the garage; CCTV surveillance should be provided for employee safety and building security.

C22.8.5.3. Access from the garage or parking structure into the building should be limited, secure, and well lit, and have no places of concealment.

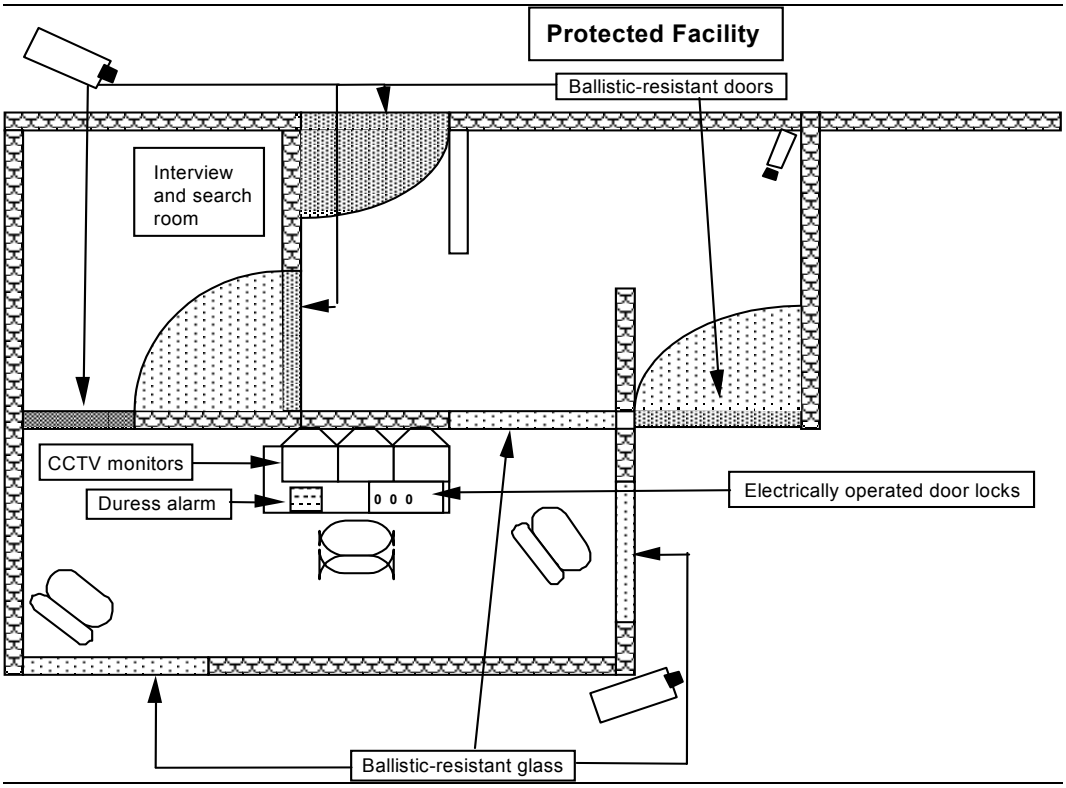
C22.8.5.4. Elevators, stairs, and connecting bridges serving the garage or parking structure should discharge into a staffed or fully monitored area. Convex mirrors should be mounted outside the garage elevators to reflect the area adjacent to the door openings.

## C22.9. PEDESTRIAN ACCESS CONTROLS

C22.9.1. Access control is primarily directed at decreasing exposure to criminal activity. Criminal opportunity can be reduced through design of a facility that restricts persons from areas where they do not belong. Access to an installation, a group of buildings, or a single building can be designed to facilitate surveillance, control, and segregation of traffic by function. Depending on the functions to be accomplished by the occupants, access points can be designed either to be closed during non-duty hours, or to be subject to surveillance and control for all-hours entry.

C22.9.2. Figure C22.F3. illustrates an approach to pedestrian access control applied at an installation perimeter. In this figure, pedestrians enter the control point through a ballistic-resistant door located at the bottom right corner of the drawing. Their approach to the facility can be observed by guards looking through two ballistic-resistant viewing ports as well as by CCTV cameras. Once inside the checkpoint, visitor's present identification, pass through a screening area that may contain a magnetometer, and can be invited into a separately secured interview room for further inspection. Upon approval, visitors pass through another ballistic-resistant door into the protected facility.

**Figure C22.F3. Generic pedestrian access control point.**



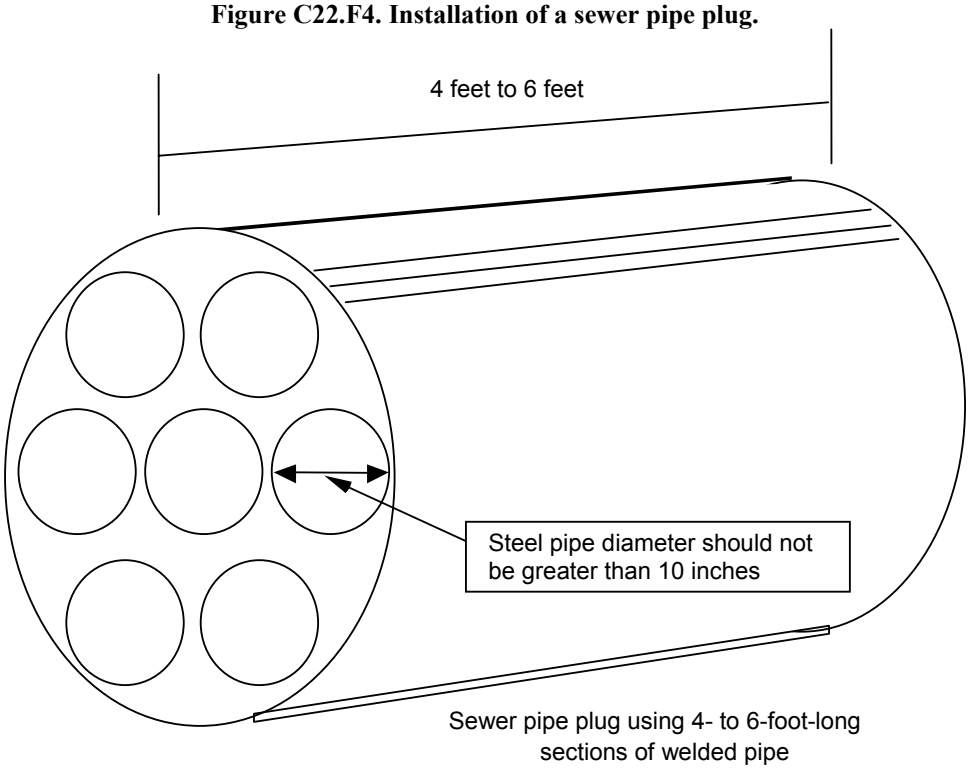

C22.10. UTILITY PENETRATIONS AND SECURITY

C22.10.1. The installation physical security survey should identify all utility service to the DoD installation, as well as all utility lines, storm sewers, gas transmission lines, electricity transmission lines, and other utilities, that may cross the installation perimeter. Detailed knowledge of such service is important for public health and safety considerations as well as installation security concerns.

C22.10.2. All penetrations of the installation's perimeter should be clearly marked. All penetrations in fences, walls, or other perimeter structures should be screened, sealed, or secured to prevent their use as access points for unlawful entry into the installation. If access is required for maintenance of utilities, all penetrations should be secured with screening, grating, lattice work or other similar devices so that no opening is greater than 10 inches in diameter. Attach intrusion detection sensors and consider overt or covert visual surveillance systems if warranted by the sensitivity of DoD assets requiring protection.

C22.10.3. Under some circumstances, it may be necessary to insert a large sleeve composed of multiple sections of pipe each no more than 10 inches in diameter into large storm sewer culverts or tunnels. This approach is illustrated in Figure C22.F4 and should be employed to block all other penetrations through the perimeter barrier that are large enough for a person to crawl through (that is, more than 10 inches in diameter) but cannot be sealed closed for any reason. All such penetrations should be equipped with intrusion detection sensors or placed under surveillance.

**Figure C22.F4. Installation of a sewer pipe plug.**




C22.11. EXTERIOR SURVEILLANCE AND INTRUSION DETECTION SYSTEMS

C22.11.1. The physical security system's initial task is to detect the presence of threats to DoD personnel and materiel protected within the facility. A wide range of surveillance options should be considered based on the following.

C22.11.1.1. Identified threats to the facility.

C22.11.1.2. Types, function, operating characteristics, and missions of DoD assets.

C22.11.1.3. Legal and diplomatic limitations on surveillance activities.

C22.11.1.4. Overall resource constraints.

C22.11.2. Technology offers physical security system planners a wide range of sensors and phenomenology from which external surveillance systems can be assembled. Table C22.T2. indicates that surveillance systems readily available to local military installation commanders capable of providing detailed visual images are somewhat less abundant than systems that detect the presence of a target but may not be able to report back the full particulars on the detected target. As the target of surveillance moves closer to the facility, it becomes possible to use guards with binoculars, CCTV or other electro-optical systems, or imaging infrared systems to detect the presence of terrorist threats.

**Table C22.T2. External Installation Surveillance Technologies.**

| | **Visual Observation and Detailed Assessment Surveillance** | | | **Presence and Non-Visual Target Characterization** | | | |
|---|---|---|---|---|---|---|---|
| Surveillance Target Location | Binoculars, Night Vision Devices | Electro-Optical | Infrared Sensors | Millimeter Wave | Acoustic Sensors | Seismic Sensors | Electro-Magnetic, Radar, Lidar, Sonar, Infrared Sensors |
| Beyond the Perimeter (detection range: 1000s of yards) | • | • | • | | | | • |
| Just Outside the Perimeter (detection range tens of yards) | • | • | • | • | • | • | • |
| At the Perimeter Barrier (detection range: less than ten yards) | • | • | • | • | • | • | • |

C22.11.3. Electromagnetic energy sensor systems use radar to detect aircraft, sonar to detect water vehicles and swimmers, and laser radar to detect humans or vehicles. These systems can report surveillance targets in digital or analog formats. Such reports usually require additional interpretation by operators. Visual surveillance systems report data in image or photographic form, requiring less interpretation by surveillance system operators before surveillance information is assessed as threatening or benign. Visual surveillance systems are usually more limited in detection range than electromagnetic sensors. Many visual surveillance systems are passive devices. Their use does not require the emission of energy, which could alert an intruder to the presence of surveillance systems. Visual surveillance systems have performance limitations, due in part to ambient weather conditions, which may require use of additional passive sensors. Such systems report information in a form that may necessitate more complex analysis before the detection of an intrusion can be classified as a threat.

C22.11.4. Surveillance system monitors need to be given information or decision rules, that they can use to interpret data, provided by all surveillance systems in use.

C22.11.5. Table C22.T3. indicates some of the surveillance problems that installation guards and security officials routinely confront. External surveillance may detect the presence of general activity hostile to DoD assets; it may also detect the presence of activity or targets at, near, or beyond the perimeter barrier, which behave in a peculiar manner. For the most part, however, it seems unlikely that external surveillance shall detect the presence of terrorists in the vicinity without further assistance and guidance from the subset of the intelligence, counterintelligence, and law enforcement communities.

**Table C22.T3. External Installation Surveillance Functions.**

| External Surveillance Problem | Indicators | Response |
|---|---|---|
| Detect presence of criminal activity directed at installation | Attempts at unauthorized entry to installation; tampering with locks, security devices at infrequently used gates | Notify guard forces; contact local law enforcement agencies IAW liaison arrangements and SOFA provisions if overseas |
| Detect hostile surveillance | Watchers, unexplained parked cars | Contact Counterintelligence |
| Detect civil disturbances | Sudden changes in social behavior in indigenous population | Notify guard force; contact Embassy if overseas |
| Detect presence of unauthorized | Aircraft noise overhead | Notify Counterintelligence |

| External Surveillance Problem | Indicators | Response |
|---|---|---|
| aviation over-flights | | |
| Detect vehicle bomb threat | Vehicle approaching facility at high speed; sudden evacuation of area around facility by indigenous population | Notify guard force and activate vehicle barriers; notify Operations or Command; notify Intelligence and Counterintelligence |
| Detect preparation of sniping positions outside facility | Changes in appearance of buildings opposite DoD installation | Notify Intelligence and Counterintelligence |

C22.11.6. Table C22.T3. also suggests that even with additional preparation and guidance, the guard at the gate or a centralized CCTV monitoring station conducting external surveillance shall have a difficult time detecting a terrorist threat beyond the installation perimeter. Detection can be enhanced if the terrorists undertake an overt act such as clearing windows in the upper stories of buildings across the street from a DoD facility.

C22.11.7. On the other hand, it is clear that if external surveillance detects the presence of the threat at the perimeter barrier and is able to maintain contact with the threat, then classification of the threat and preparing an immediate response if the perimeter is penetrated are both easier and quicker.

C22.11.8. Surveillance systems that combine detection systems registering the presence of a threat as well as detection systems that permit direct visual monitoring of the threat provide considerable information to installation threat-assessment personnel. Multiple sensors arrayed in a grid pattern from the perimeter barrier stretching in toward the center of the facility can provide the security force with information necessary to classify and characterize the threat without forcing the guard force to leave secure positions. Surveillance systems often have a lower life cycle cost. They can be hardened against the elements to a substantial degree. It is not surprising to see more DoD Components placing greater emphasis on IDS and other technical surveillance systems to meet their physical security system protection requirements. The advantages of technical surveillance are lost, however, unless IDS and other systems remain in top-notch repair.

C22.12. AIRFIELD COMBATING TERRORISM SECURITY CONSIDERATIONS

C22.12.1. Airfields represent special security challenges because of the unique character of the facilities and the DoD assets that they support. All of the foregoing discussion applies to

airfields. Airfield security planners may also wish to consider the establishment of multiple internal security perimeters, hardening of selected buildings against terrorist attack, hardening of petroleum storage, aircrew facilities, maintenance facilities, and other facilities collocated on the installation. Security planners are fully aware of DoD regulations and instructions, Service regulations and instructions, and Combatant Commander requirements for enhanced physical security protection for many types of munitions stored at DoD airfields.

C22.12.2. In securing structures and facilities, however, it is important to examine runways and taxiways with great care. These are not merely slabs of asphalt and concrete poured on the ground; they are intricate, complex architectural structures containing all the building elements normally associated with complex high-rise office or apartment buildings. Runways and taxiways are crisscrossed with electrical, water, and sewer lines. Often there are petroleum, oil, and lubricants distribution systems buried adjacent to, if not underneath, portions of runway and taxiway structures. Constructing 2- to 3-mile-long stretches of pavement often requires substantial reconfiguration of the local topography, creating the need for extensive drainage and storm water management systems.

C22.12.3. Therefore, airfields abound with utility penetrations not often seen in urban office building environments.

C22.12.4. Airfields are often adjacent to areas with substantial wildlife activity. Exterior intrusion alarm systems are prone to provide much data on movement that is regarded as false—that is, non-human. Exterior intrusion alarms applied without great care to airfield perimeter security barriers can actually degrade security by desensitizing security personnel responsible for classification and assessment of threat information reported. High false-alarm rates triggered by roaming wildlife can lull guards and IDS monitors into a false sense of security.

C22.12.5. Use of multiple phenomenology intrusion sensors is essential to the effective management of limited security personnel resources at airfields. Use of line detectors, motion detectors mounted on fences, and seismic or acoustic sensors sown in patterns are critical. Multiple- phenomenology IDS can permit alert center personnel to classify and identify an intrusion by looking at reports from each type of sensor. Subtle differences are reported between human and animal interactions among different types of sensors. By laying out multiple sensors across a wide area, the differences between human and animal activity can be magnified, allowing alert center personnel to determine whether the intrusion is human or animal as well as the intruder's direction and rate of advance. This information can be used to determine whether

the security force must be dispatched, to what point it should go, and how quickly it must arrive at the designated interception point.

C22.12.6. Another unique aspect of airfield security is the nature of the activity and the type of assets to be found there. Aircraft generally are most vulnerable to mechanical problems, human error, or ground-to-air attack during landings and takeoff. The requirement to maintain lift at low speeds generally restricts aircraft operation to a fairly narrow corridor within a few degrees of the direction of the airfield runways. The performance envelope of aircraft also restricts the volume of airspace in which an aircraft can operate within a few miles of an airfield.

C22.12.7. The introduction of sophisticated electronic systems to support aircraft takeoffs and landings in all weather and visibility conditions has added vulnerabilities to airfield activities. Attacks on airfield electronics could be devastating.

C22.12.8. Hence, airfields have an exceptional requirement for beyond-the-perimeter surveillance. They may also have an exceptional requirement for beyond-the-perimeter response.

C22.12.8.1. Consider establishing observation posts in off-base areas beneath or adjacent to flight paths for landings and takeoffs. Use of DoD personnel for law enforcement and security operations outside the perimeter of a DoD installation is tightly constrained by Federal statute within the United States, its territories, and its possessions, and by SOFAs overseas.

C22.12.8.2. In many instances, it may be permissible to establish observation posts staffed jointly by DoD personnel and local law enforcement officers. The purpose of such observation posts is merely to detect the presence of potential dangers to flight operations and report such threats to designated local authorities so that they can respond.

C22.13. AT MITIGATION MEASURES AGAINST MAN PORTABLE AIR DEFENSE SYSTEMS (MANPAD) THREAT

C22.13.1. The November 28, 2002 terrorist attack on an Israeli airliner in Kenya highlights the potential MANPAD threat to U.S. aviation interests, both in CONUS and OCONUS. Commanders who own and/or are supported by air assets should consider the level of risk and make decisions to alter, divert, or cancel air missions if the MANPAD threat is too great or cannot be mitigated. This is especially critical for locations transited by commercial air carriers moving U.S. forces and equipment.

C22.13.2. Air Mobility Command (AMC) maintains a worldwide database in their secure web site with current intelligence and operations information that can assist commanders in making prudent decisions pertaining to a MANPAD threat. The AMC Intelligence Combined Risk Assessment database offers both automated risk assessments known as the Virtual Threat Assessor program and formal TWG virtual RA. Both products offer such items as airfield information, terrorist, medical, military, information operations, and other threat information, along with archived briefings and open source information.

C22.13.3. Airfield security and local area assessments should be conducted to identify the areas of vulnerability to a MANPAD threat (in terms of possible launch sites) to include the airfield arrival and departure corridors as well as potentially vulnerable ground targets such as parked aircraft or ground vehicle motor pools. A thorough assessment could include security force, intelligence, counterintelligence, and operational personnel as well as local/host nation authorities.

C22.13.3.1. The DIA missile and space intelligence center has flight path threat analysis simulation (FPTAS) software in their secure web site that allows the local commander to quantify the areas of greatest MANPAD threat. FPTAS uses aircraft performance, flight path data, missile characteristics, and digital terrain elevation data to generate maps depicting areas from which MANPADs could engage U.S. and allied aircraft. Commanders have used these maps to identify flight paths with minimum exposure to the MANPAD threat and have adjusted take-off/landing patterns to limit aircraft exposure and utilize areas readily secured by ground troops.

C22.13.3.2. Criteria to identify possible MANPAD launch sites include but are not limited to:

C22.13.3.2.1. Cover and concealment – the ability of an object to provide protection for the terrorist from return fire and prevent detection by security force personnel.

C22.13.3.2.2. Line of sight providing unobstructed view of the target.

C22.13.3.2.3. Exposure time – the amount of time the intended target is vulnerable from an operational attack.

C22.13.3.2.4. Distances to target and target recognition for the terrorist to positively identify the intended target.

C22.13.3.2.5. Accessibility of the location for ease of ingress/egress, set up time required for a terrorist fire team to get into position to attack, and the time to discovery in terms of the amount of time it takes to detect a fire team once their weapons are exposed.

C22.13.4. There are two areas where commanders and antiterrorism officers should employ mitigation measures to counter the MANPAD threat: airfield/installation defense and reducing aircraft in-flight susceptibility.

C22.13.4.1. The following are points to consider in developing AT plans for airfield/installation defense to counter the MANPAD threat.

C22.13.4.1.1. Once an analysis of possible launch sites is accomplished, prime MANPAD launch sites and vulnerable areas can be isolated by expanding the airfield area of control and reducing areas of vulnerability. The following mitigation measures may require coordination with local/host nation authorities:

C22.13.4.1.1.1. Increased physical presence at prime launch sites. Visual observation of security teams is a strong deterrent.

C22.13.4.1.1.2. Focused and random patrols of vulnerable areas. Random patrols should be part of the installation random AT measures program.

C22.13.4.1.1.3. Implementation of technical surveillance of vulnerable areas to include both launch sites and potential targets.

C22.13.4.1.2. Ensuring personnel are educated on the MANPAD threat (to include component recognition), areas of vulnerability, and reaction plans. Develop and provide MANPAD awareness training for security force personnel and local/host nation law enforcement. Develop a MANPAD awareness program for neighborhood watch groups and local businesses/installation facilities in close proximity to airfields or along flight paths. The Defense Intelligence Agency's Missile and Space Intelligence Center has a secure web site in their Enduring Freedom section that has a MANPADs link that is a good source for information on MANPAD systems.

C22.13.4.1.3. Ensuring tight airfield access control procedures are in place for airfield operations. Consider dispersal of parked aircraft to reduce damage from a MANPAD or rocket propelled grenade attack.

C22.13.4.1.4. Developing and exercising contingency plans for responding to an incident of a MANPAD threat. Rapid reaction plans shall facilitate the immediate capture of a

terrorist team, even post attack, to deter/prevent future attacks and ease concern for air travel safety by the public at large.

C22.13.4.2. The following are points to consider in developing AT plans to reduce aircraft in flight susceptibility due to the MANPAD threat.

C22.13.4.2.1. Establishing airfield specific procedures for the use of aircrew tactical countermeasures and/or tactics. Development and dissemination may require coordination with local/host nation authorities. Ensure aircrew awareness of possible effects of MANPAD on their aircraft. Ensure aircrews and flight operations are tied into the AMC intelligence combined risk assessment database to obtain current information on airfield security assessments.

C22.13.4.2.2. Varying arrival and departure times of aircraft. Stagger the arrival times of normal scheduled missions to make arrival, departure, and ground times harder to predict for the terrorist.

C22.13.4.2.3. Randomly changing approach and departure routes as a deterrent (in accordance with current TSA guidelines).

C22.13.4.2.4. Limiting or discontinue use of landing lights within identified threat zones to reduce heat producing/targeting options.

C22.13.4.2.5. In high threat areas or when intelligence has indicated a high alert status, coordinating and developing plans for engine running offloads to minimize ground time.

C22.14. WATERSIDE SECURITY

C22.14.1. Securing DoD facilities located astride waterways is an especially challenging task. Like airfield security, port security begins with the basic problem of securing the facility and assets housed or contained therein by erecting appropriate perimeters and installing physical security devices to detect attempted or successful perimeter penetrations.

C22.14.2. The problem of securing the waterside of a DoD installation is equally challenging. There is substantial difficulty in distinguishing friend or foe even under the best of circumstances. Rules of navigation make strict enforcement of perimeters difficult, as these rules allow for emergencies, tidal and wind action, and even errors by eager but less-skilled operators of vessels or craft. Background activity outside the perimeter of a DoD installation makes detection, classification, and identification of terrorist threats very difficult.

C22.14.3. Securing ports against terrorist attack is further complicated by two factors.

C22.14.3.1. The quantity of materiel in transit to and from port areas is enormous. The quantities are so large that it is physically impossible to inspect each container or bulk cargo shipment for weapons, explosives, or other terrorist contraband.

C22.14.3.2. Port facilities are notoriously accessible from the waterside of the facility. Hence, waterside security must include the establishment of a security perimeter at the water's edge to detect presence of terrorist threats. The security perimeter must be extended into the water if terrorists are assessed as having the capability to launch attacks using standoff weapons from boats or other craft.

C22.14.4. External surveillance must monitor traffic on the surface of the water adjacent to the facility, extending from the barrier to a range exceeding that of identified terrorist threats. As illustrated by Figure C22.F5., the outer limit of the surveillance area extends well beyond the estimated outer range of terrorist waterborne weapons. A security zone is established within the surveillance area extending from the high-water mark to a distance at least 1,000 meters from shore if possible. In some port areas, the security zone shall be constrained, while in other areas the security zone may be extended farther, especially if the terrorist threat includes longer-range standoff weapons such as man-portable antitank missiles. Within the security zone exists a reaction zone. Here aggressive actions may be undertaken to isolate, delay, and resolve potential threats to DoD assets from waterside terrorist action.

C22.14.5. Figure C22.F5. shows security zones inscribed around a land-based facility. The principle can be extended to one or more warships at anchor; security zones may also be declared around navigation aids mounted on structures in shallow water, as is the case for airfield navigation aids in bays or rivers.

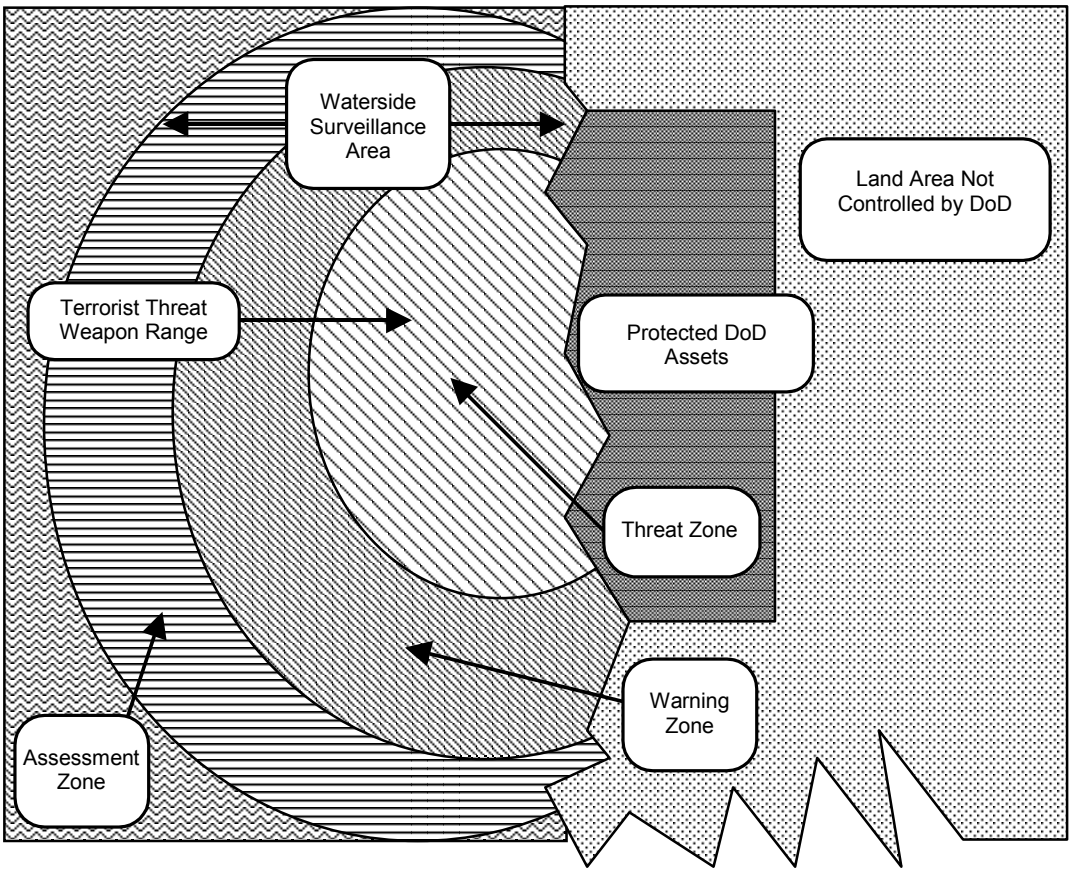
C22.14.6. Specific recommendations on implementation of waterside security measures are described in Appendix 17.

C22.14.7. It should be emphasized that DoD facilities bordering bodies of water should include waterside protective measures as part of the facility physical security plan, even if there are no active waterside commercial, military, or recreational facilities at the facility or installation. Appendix 17 provides measures for DoD facilities adjacent to bodies of water.

C22.15. STRATEGIC SEA AND AIR PORT, SEA AND AIR PORT, AND DEPLOYED LOCATIONS

C22.15.1. The physical security of locations off military installations presents unique challenges that often, at best, can only be mitigated and never eliminated. Though these locations are not under the direct control of the Commander/agency head, adequate physical

**Figure C22.F5. Waterside terrorist surveillance and engagement zones.**




security can be achieved through active liaison with local officials and/or host nation authorities. As discussed extensively throughout this manual, it is essential to develop a local threat assessment, identify vulnerabilities, prioritize critical assets, complete a risk analysis, and develop an AT plan. Care should be taken to go through this process for each location forces shall be embarking/debarking, transiting through, and deploying to.

C22.16. EVACUATION OF FACILITIES/CURTAILMENT OF FACILITY ACTIVITY

C22.16.1. The purpose of a physical security system is to prevent the loss, destruction, or compromise of DoD assets. Under some circumstances, moving the asset to a more secure environment or closing the activity until the threat has abated best achieve this purpose.

C22.16.2. Security personnel should survey the area adjacent to DoD installations or facilities to identify potential sites for helicopter landing zones. If no appropriate site is available near DoD installations for facilities, appropriate alternatives should be identified.

C22.16.3. In preparing plans for evacuation of DoD assets requiring maximum protection, the security personnel should consider construction of one or more safe havens in the vicinity of the emergency evacuation site. Such structures should be well camouflaged and knowledge of their existence kept on a strict "need-to-know" basis.

C22.16.4. Erecting or constructing special safe havens near emergency evacuation sites should be considered when circumstances are such that helicopter evacuation might require several hours to execute after requested. Plans should be prepared that would permit dispersal of DoD personnel to several safe havens, including those adjacent to emergency evacuation sites, before local travel becomes too dangerous. Relocation of DoD personnel to remote safe havens to await evacuation may be an effective alternative in some circumstances, especially those in which the number of DoD personnel and dependents is small.

C22.16.5. Curtailing activities require a survey of all essential/nonessential functions performed at the location and deciding which of those can be temporarily halted without mission degradation. Examples of activities that could be curtailed are base exchange; morale, welfare, and recreation activities; and DoD schools. Curtailing activities can be linked to FPCON and curtailment procedures can be outlined in the AT plan.

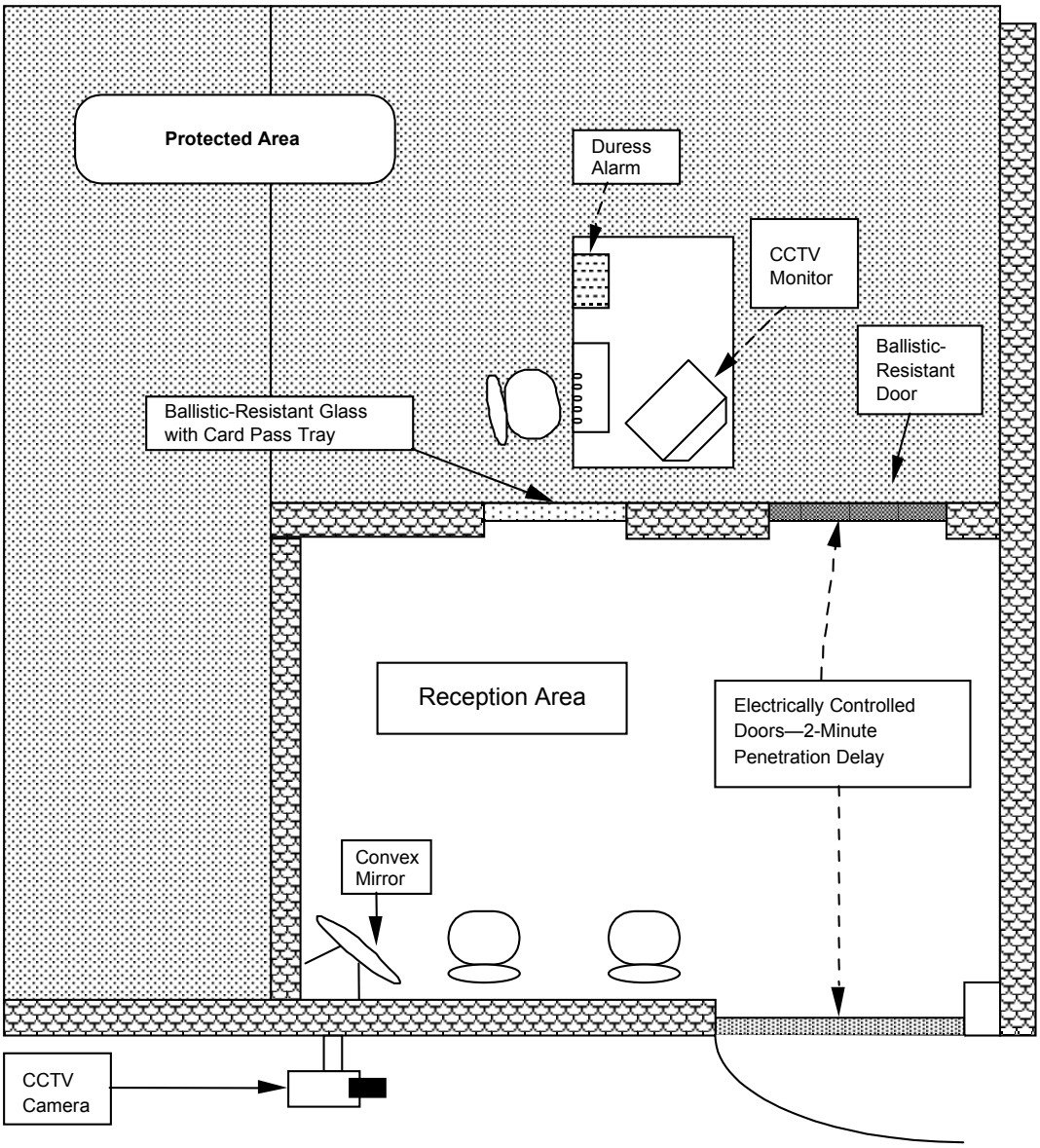
C22.17. ACCESS CONTROLS

C22.17.1. Access controls are intended to increase the amount of time needed to go from one area of a facility to another, to allow security personnel to sound alarms and take immediate protective actions in the event of attack. Some access control systems can both delay attackers in reaching protected areas and inhibit egress from a facility. These systems aid in containing and resolving the incident as well as aid in the apprehension of the perpetrators. Figure C22.F6. illustrates one approach to controlling access to a secure area within a building. Depending on the threat, the asset to be protected, and the availability of protection and security resources, access control points as illustrated can be established in a series. The greater the value of the

protected asset, the larger the number of checkpoints that must be passed before access is granted.

C22.17.1.1. Figure C22.F6. illustrates several important features of a secure area access control point. A CCTV camera provides surveillance of the initial entryway. The door to the entryway is hardened and provides two minutes of delay against penetration. The waiting area is hardened, and is subject to surveillance by a guard. The guard is protected from the waiting area by ballistic-resistant glass and an electrically controlled ballistic- resistant door. The guard also has a hidden duress alarm.

**Figure C22.F6. Reception area to access controlled facility.**




C22.17.1.2. The access control checkpoint can screen employees and visitors and can complicate entry; however, visitors and employees shall have legitimate business activities to conduct within the secure area. Therefore, additional procedural safeguards must be incorporated into the physical security system to prevent theft of valuable items or information, as well as to protect individuals in the secure area against direct assault or explosive devices left behind by authorized visitors.

C22.17.2. Access Control Procedures. The systems approach to physical security includes an assessment of day-to-day operations within the secured area. In order to maintain adequate security throughout a DoD installation, within a facility, within an activity, and within an organization without unduly interfering with day-to-day work, it is necessary to permit personnel to move about. On the other hand, the physical security system has a responsibility to ensure that protected assets remain protected throughout the regular workday. Accordingly, the following measures can be implemented to maintain positive control over access to protected DoD assets.

C22.17.2.1. A Pass-and-Badge System. Where the area is large or where the number of personnel exceeds a number that can be recognized personally by the guard or persons charged with security responsibility for the area, a pass-and-badge identification system should be used. Security badges shall be used primarily for access control. Badges should contain a picture of the individual who has authorized access, and it may contain additional information about the individual, communicated through such things as badge borders, color, and photograph background color. Information that should not be printed on the badge includes the home address, the specific work location address and telephone number, security information, and, in some areas, information identifying the badge holder as a DoD or U.S. Government employee.

C22.17.2.2. An Access List System. Admission of personnel to very high-security areas should be granted only to persons who are positively identified. One approach is to prepare access lists containing the names of those individuals specifically authorized access to a facility. Access lists should be maintained under stringent control of an individual who is formally designated by the commanding officer or manager of the facility. That person should be responsible for updating and confirming the need for access on a regular, frequent basis. Admission of persons other than those on the authorized access list should be approved by the commanding officer, manager, or designated representative. Access lists should always be controlled carefully and never displayed to the public. If a computerized access list system is used, the computer files used to generate such a list must be safeguarded against tampering.

C22.17.2.3. An Exchange Pass System. The exchange pass identification system may be employed in highly sensitive areas to ensure stringent access control. It involves exchanging one or more identification media (such as badges or passes) for another separate type of identifier (such as badges or passes). This system is particularly useful where visitors must gain access to a high-security facility. The process of exchanging passes is a personal one, permitting security

personnel an opportunity to examine all personnel both upon entering and upon exiting the secured facility.

C22.17.2.4. An Escort System. Escorting is a method to control visiting personnel within a secured facility. The escort must remain with the visitor at all times while within the restricted areas. If local written policy determines that an individual does not require an escort within the area, the individual must meet all the entry requirements for unescorted access. Escorts may be civilian or military personnel employed by or attached to the visited activity, and shall normally be from the office of the person being visited. A major objective in escorting visitors around a facility is to ensure that all material brought into the facility by the visitor is left with someone who can open and examine the contents and that visitors leave no packages or other materials behind on their departure.

C22.18. SAFEHAVENS

C22.18.1. The innermost layer of protection within a physical security system is the safehaven(s). Safehavens are not intended to withstand a disciplined, paramilitary attack featuring explosives and heavy weapons. Such structures generally should be expected to provide a minimum of 15 minutes of protection against a predetermined level of attack using hand attack tools or small arms.

C22.18.2. The safehaven should be designed such that it requires more time to penetrate by attackers than it takes for the response force to reach the protected area. Consider equipping the safehaven with minimal food, water, and medical supplies. Consult Service, Combatant Commander, or DoD Agency AT construction guidance for complete details on constructing a safehaven. Figure C22.F7. represents a sample safehaven layout.

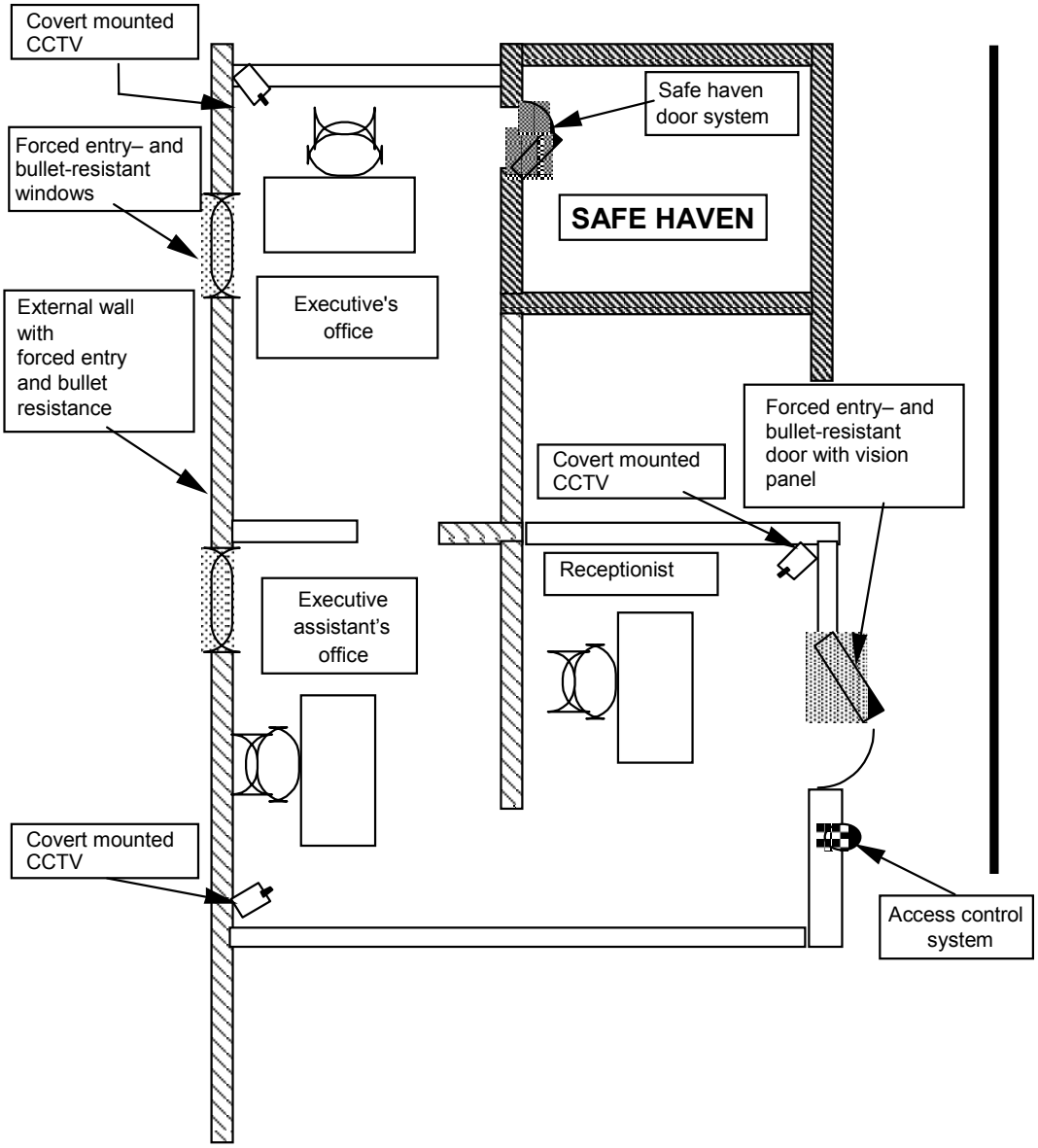
C22.18.3. Even though a safehaven is not intended or designed to provide penetration protection over an extended period, it may be necessary for occupants to remain in the safehaven for several hours while response forces converge on the site, contain and resolve the terrorist incident. Under such circumstances, occupants of the safehaven may be more secure and less likely to be injured or to compromise crisis management by remaining in the safehaven until the on-scene Commander directs them to evacuate or leave the facility.

C22.19. RESIDENTIAL PHYSICAL SECURITY CONSIDERATIONS

C22.19.1. The DoD Physical Security Regulation mandates the protection of all DoD assets just as are weapon systems, facilities, and bases. Residential security should be examined just

like the security of a DoD installation or facility. A layered defense or defense in depth, as discussed earlier in this Chapter, should be prepared.

**Figure C22.F7. Safehaven concept implemented in a high-rise office building.**




C22.19.2. Many senior military officers and DoD officials (referred to below as "executives") because of their specific assignments or positions of visibility and terrorist threat conditions, are designated High Risk Persons (HRP). Additional security measures for HRP are discussed in Chapter 21.

C22.19.3. Residency Selection.

C22.19.3.1. There are a number of general security atmosphere factors that should be considered when selecting a family residence.

C22.19.3.1.1. The general character of streets, sidewalks, lighting, pedestrian and vehicular traffic patterns.

C22.19.3.1.2. The presence and condition of parks, playgrounds, recreation areas.

C22.19.3.1.3. The existence of public or commercial enterprises intermingled with residential dwellings.

C22.19.3.1.4. The existence and condition of fire hydrants and police call boxes.

C22.19.3.1.5. Where the streets are paved, well lit, broad enough for at least two cars to pass one another, and lined with sidewalks filled with a variety of people, there is a strong possibility that the neighborhood is fairly secure. Where these favorable impressions can be reinforced by a walk through clean, well utilized parks, playgrounds, and recreational areas, a walk through clean, attractive, mixed-use neighborhoods, and areas with a visible presence of police and fire services, the initial impression is likely to hold up to further scrutiny.

C22.19.3.1.6. In general, the overall appearance of the area may often serve as an indicator of crime levels. Where property lines are well defined, homes appear well maintained, and the landscaping shows an obvious pride in the property, crime rates are likely to be low. While that may not eliminate the threat of terrorist attack, it does suggest an attractive general security atmosphere.

C22.19.3.1.7. Observe or make inquiries about the frequency and type of police patrols in a given neighborhood. Find out what type of police or which police jurisdiction responds to calls for assistance. Observe the general appearance of police security personnel on the street. The police who take pride in their appearance, the appearance of their vehicles, and who make themselves visible to the public in the performance of their duties can usually be relied upon to provide dependable police coverage throughout the community.

C22.19.3.1.8. Try to determine the attitude of the government and the populace toward other nationals, and particularly Americans. A strong anti-American attitude could be cause for you to have diminished faith in local police responsiveness.

C22.19.3.2. Specific Indicators of General Security Levels. Several observable security measures taken by residents of a neighborhood can provide specific indications about local security conditions. Look for specific indicators of security precautions taken by local residents such as:

C22.19.3.2.1. Presence of barred windows, security grills on doors.

C22.19.3.2.2. Security walls and fences.

C22.19.3.2.3. Security lighting.

C22.19.3.2.4. Large dogs or other watch animals.

C22.19.3.2.5. Presence of private security guards, especially during the day.

C22.19.3.2.6. Background Information on Local Criminal Activity. Investigate local crime activity in the area to which you are considering moving.

C22.19.3.2.7. The level of criminal or terrorist activity throughout a community is rarely uniform. Street crime can be expected to occur in lower income, crowded, and congested areas. It is generally recommended that residences not be selected in downtown, commercial, or especially isolated areas, especially when local data indicate that such areas are high crime areas.

C22.19.3.3. DoD personnel assigned to Defense Attaché Offices can contact the Embassy's Regional Security Office prior to overseas deployment for detailed information on high and low crime areas. The Defense Attaché's Office should also be able to obtain such information to assist personnel being assigned overseas on TDY/TAD status who may require residential housing in lieu of hotel-type accommodations.

C22.19.3.4. Other DoD affiliated personnel may obtain information by contacting the Country Desk in the Department of State, Washington, D.C. 20520 or on the WorldWide Web at http:\\www.state.gov.

C22.19.3.5. Utilities Service and Protection. Explore the reliability of local utility service in order to determine whether or not emergency or backup power and utility service shall be required. The availability and reliability of utilities in any given location should be a primary factor in the selection of a residential site. Reliability of utilities should be determined and in cases were they are erratic, acquisition and use of backup systems should be assumed. Disruption of utility service, particularly electricity and telephone, would facilitate unauthorized access to a residence by an intruder.

C22.19.3.6. Fire Protection. Consider the availability and effectiveness of local fire protection services in each neighborhood being investigated for potential residence. The proximity of prospective residences to and the effectiveness of the fire protection services are a major consideration in residential site selection. The availability of water or other substances to fight a fire should be determined. The locations of fire hydrants or other water sources and means by which they can be accessed and brought to the residence by its occupants before the arrival of the local fire brigade should be considered.

C22.19.3.7. Physical Environment Considerations.

C22.19.3.7.1. Investigate potential hazards in the physical environment in and around neighborhoods of potential residential interest.

C22.19.3.7.2. Residential areas under consideration should be well removed from known environmental hazards such as flood plains, active geological faults, and steep slopes of hills subject to mudslides and/or brushfires. Residential areas close to breeding areas for disease vectors such as insects or rodents should also be avoided if possible.

C22.19.3.7.3. Sometimes, housing availability restricts residential selection to areas at risk from at least some of the environmental hazards noted above. If placed in this situation, take the following measures, plan additional, necessary precautions to prevent loss or injury from environmental disasters in addition to potential terrorist actions.

C22.19.3.7.4. Be sure to include access to and storage of emergency rations, lighting, power, communications, and backup or alternatives to any other systems that could be disrupted as a result of an environmental disaster as part of your moving plans.

C22.19.3.8. Residence Access Routes. Select candidate residences with access routes that allow many choices of approach or departure. It is essential that access routes to and from residences allow occupants many choices of approach or departure to make detection of arrival and departure patterns difficult and to avoid ambush or attack once it is spotted. Some considerations should include:

C22.19.3.8.1. Clear delineation of the street or roadway.

C22.19.3.8.2. Sufficient street width to allow two cars to pass, even if vehicles are parked on both sides of the roadway.

C22.19.3.8.3. Sufficient neighborhood night lighting.

C22.19.3.8.4. Unobstructed road view from the residence.

C22.19.3.8.5. Of all considerations when contemplating the potential dangers of an access route, the most important is to select a residential location that shall not lock occupants into predictable patterns. Do not select a residence located on a dead-end or one-way street. Locations such as these provide terrorists ideal opportunities for ambushes that would be almost impossible to avoid.

C22.19.3.9. Parking.

C22.19.3.9.1. Consider the location and availability of parking for privately owned vehicles, motorcycles, and bicycles when examining candidate residences and their surrounding neighborhoods.

C22.19.3.9.2. In selecting a residence, consideration must be given to securing personal property including means of transportation. Bicycles, motorcycles, mopeds, and other two-wheeled vehicles are usually relatively easy to secure. Often they shall fit in a storage shed, or can be locked close to the residence where they can be observed.

C22.19.3.9.3. The family automobile, and in some cases, official vehicles have been approved for transportation between home and office, present another problem. The best solution is to store the vehicle in a garage that can be kept locked at all times. Carports and driveways within a fenced or guarded area are the next best alternative. Off-street parking alternatives represent another far less desirable alternative. Personal or official vehicles should not be parked on the street overnight in the vicinity of personal residences.

## C22.20. SECURITY COMPARISONS BETWEEN SINGLE AND MULTIPLE FAMILY RESIDENCES

C22.20.1. After a careful review of the general security atmosphere and specific indicators of local crime, there may be an opportunity to choose either a single family or a multiple family residence. Overall housing costs, availability of dependent care or playmates for dependents, and location convenience factors noted above can be important determinants of residential choice. There are some specific security considerations, however, that should also be evaluated in choosing between multiple or single-family residences:

C22.20.2. In most cases, apartments are generally preferred to single-family dwellings when security is a primary consideration. Apartments above the first floor are more difficult to get to, usually have only one entrance, and provide some degree of anonymity for the resident. Thus, they present a more difficult target for the terrorist or burglar, and are often less expensive to modify with security hardware. Living in an apartment provides benefit of close neighbors. In

the event of an emergency and loss of communications, neighbors can often be relied upon to provide assistance. At the very least, they can call the police if American occupants of apartments cannot.

C22.20.3. The advantages of an apartment, however, are often offset by a variety of disadvantages that should be considered when selecting a residence.

C22.20.3.1. Normally, apartments have a limited number of accesses. Most commonly, there is a main entrance through a lobby that leads to a bank of elevators or an internal stairwell. The lobbies, elevators, and stairwells many times are not secured and are areas where robberies often occur. Secondary entrances are often found leading from parking areas that may be located below ground level or to the rear of the apartment. Stairwells are often poorly lit and rarely secured.

C22.20.3.2. Common areas such as laundry rooms, meeting rooms, storage rooms and parking garages, which provide access to apartment areas, are usually not secured and could provide access to criminals or terrorists.

C22.20.3.3. Because many families share the same building, strangers have access to the building, and it is difficult to challenge their presence.

C22.20.3.4. Many newer apartments have been built of fire resistant materials reducing the threat of fire. However, this has eliminated the need for fire escapes as well, and limiting routes the occupant can take in the event of an emergency retreat from the apartment. On the other hand, the presence of a fire escape provides an alternate means of access for the intruder.

C22.20.3.5. To provide the apartment dweller an opportunity to get outdoors without leaving the immediate confines of his apartment, newer apartments usually have balconies that are often ideally suited to allow access to an intruder who may crawl across from another balcony, or lower himself from a higher balcony. In many cases, the security hardware found on doors leading to these balconies is less than desirable.

C22.20.3.6. A cooperative compound is the next most secure type of residential housing complex. Common in many overseas areas, a number of separate homes are clustered in the same general area. American or other foreign families often occupy these. Such arrangements offer excellent opportunities for cooperative security arrangements. These enclaves may or may not be fenced, and the families may share the costs for guards, lighting systems, and alarm systems described in the preceding chapter on physical security arrangements.

C22.20.3.7. A separate residence in a suburban neighborhood can be adequately secured, but is vulnerable to intrusion. The same can be said for a single family dwelling in an isolated environment.

C22.20.4. Apartment Selection Suggestions. The following features of apartment living are recommended as part of a good security foundation for a private residence.

C22.20.4.1. Features lobby and parking area security provided by guards, closed circuit television, or locking devices which can only be operated by the tenants.

C22.20.4.2. Does not have fire escapes, balconies, or overhangs that could be used to gain surreptitious entry to the building. If fire escapes and balconies exist, they should be properly installed and include intrusion detection or other security systems to preclude unauthorized access.

C22.20.4.3. Have only one door for general ingress and egress and one door for services and deliveries; both have controlled access via guards, keys, or key-card devices.

C22.20.4.4. Has well lit hallways and stairwells, preferably monitored by closed circuit television, which cannot conceal intruders.

C22.20.4.5. Although most families usually prefer apartments on higher levels, apartments should not be selected above the third floor unless the building has a minimum of two completely enclosed fire resistive emergency escape stairwells. Because most fire department ladder trucks do not reach above the eighth floor do not select an apartment above this level unless the building has a minimum of three completely enclosed fire resistive emergency-escape stairwells. A complete fire alarm and detection system installed throughout the building is also preferred.

C22.20.4.6. If adequate security measures are not present, apartment living affords the opportunity to provide necessary security at a reasonable price, as a shared expense.

C22.20.5. Single Family Home Selection Suggestions.

C22.20.5.1. Although a well-designed and well-managed apartment is more secure than a separate house there are often other reasons that result in the selection of a single-family residence by DoD-affiliated personnel. Need for three or four bedrooms to accommodate children or other dependents, an exercise area for pets, or large areas for official entertaining are examples of considerations that may eliminate an apartment as a residential choice.

C22.20.5.2. The main ingredient to be used in selecting a single dwelling residence is finding an established residential development or neighborhood where income levels and lifestyles are compatible. Neighbors routinely looking out for each other are a critical factor in a well-protected residential area. A good overview of the entire neighborhood such as streets, sidewalks, lighting, home is necessary. Each of these features affects the security of the neighborhood and therefore, the natural protection afforded the residence.

C22.20.5.3. In selecting a single-family residence, seek out residences with the following characteristics.

C22.20.5.3.1. Has architectural and natural features that provide opportunities for occupants to observe activities on the street, the sidewalks, adjacent yards, and public areas.

C22.20.5.3.2. Is placed in the neighborhood such that neighbors shall readily observe a stranger or potential intruder.

C22.20.5.3.3. Is situated within clearly defined boundaries, making an inadvertent intrusion virtually impossible.

C22.20.6. Apartment Security Enhancements.

C22.20.6.1. The apartment should possess a good solid door and the doorframe should be well constructed. Most residential security hardware that is suitable for single-family dwellings is also suitable for apartments. Most essential of these is a 190-degree optical viewer and a strong secondary deadbolt lock. In the absence of a fire escape, there are a variety of devices sold commercially that shall facilitate exiting an apartment from a window. The devices include rope or chain ladders, and mechanical rope slings that provide a controlled descent to the ground.

C22.20.6.2. Additional security measures employed in single-family residences described below can be added to apartments as well if necessary.

C22.20.7. Single-Family Residence Security Enhancements. Most of the common enhancements to single family residence security focus on improving resistance to intrusion and penetration. Following the general approach presented above with respect to enhancing the security of an installation or a facility, consider the following measures.

C22.20.7.1. Ensure a barrier that clearly delineates the property from adjacent homes surrounds the single-family residence. An aesthetically acceptable barrier such as a picket fence can provide a good psychological deterrent to intrusion. Other fencing materials such as split

rail, board-on-board, decorative wire mesh, decorative walls constructed of masonry or stone can serve the same purpose.

C22.20.7.2. Ensure all perimeter barrier penetrations greater than 10 inches in diameter are secured. The perimeter barrier should be designed and constructed such all barrier penetrations in excess of 10 inches in diameter can be closed, locked, gated, or otherwise secured against human penetration. The mechanisms used to secure such penetrations should be comparable in their resistance to penetration as the perimeter barrier itself.

C22.20.7.3. Increase the resistance of doors, windows and exterior walls to penetration.

C22.20.8. Common Security Enhancements for Residences.

C22.20.8.1. Do not leave utility connections including telephone terminal boxes, electrical service wiring, potable water connections, natural gas connections, etc. accessible from the exterior of the house. Consider relocating utility service or placing the utility connections inside secured enclosures to prevent tampering or unauthorized access. Add internal backup systems such as batteries, bottled gas, and two-way radios. Consider finding an alternative residence as well.

C22.20.8.2. Select a residential structure that is not vulnerable to fire. Residences should be constructed from materials that are not readily combustible. Furthermore, electrical wiring and fixtures as well as and natural gas and/or propane ovens, ranges, water heaters, and other appliances should be in good condition. Be sure that the residence has sufficient numbers, and accessibility of potential emergency exits that can be used in the event of a fire. If necessary, acquire hinged high security window grills to permit use of windows as a fire escape. Be sure to keep fire extinguishers charged and available; install a smoke detector in the residence if it does not already have one.

C22.21. SUPPLEMENTAL RESIDENTIAL SECURITY MEASURES FOR HIGH RISK BILLETS AND HIGH RISK PERSONNEL (HRP)

C22.21.1. Before supplemental security measures are provided, a risk assessment must be completed as described in Chapters 4 through 8. Risk assessments dealing with DoD personnel assigned to the Combatant Commander or a Component Command should be coordinated with the chain of command through the Combatant Commander to ensure that all echelons of command are fully informed and have the opportunity to comment

C22.21.2. Enhanced Protective Measures for HRP Residences. Consider the following:

C22.21.2.1. Upgrading security perimeter barriers.

C22.21.2.2. Hardening doors to withstand penetration.

C22.21.2.3. Hardening window against ballistic and blast threat.

C22.21.2.4. Make sliding glass doors as resistant to forcible entry as possible.

C22.21.2.5. Installation of comprehensive intrusion detection system.

C22.21.2.6. Installation of a secondary security wall equipped with a medium security door separating family sleeping areas from the rest of the residence.

C22.21.2.7. Adding appropriate external security lights.

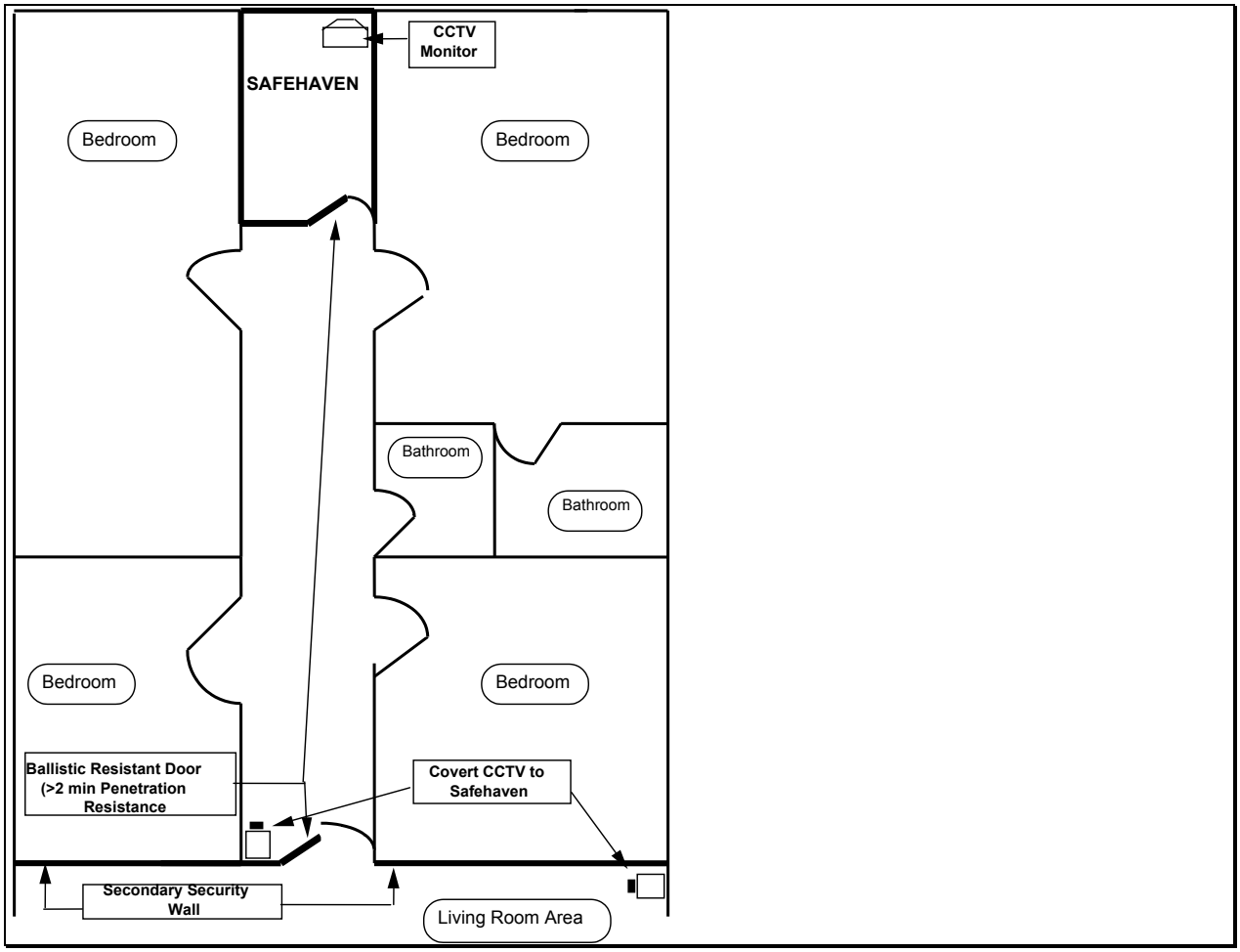
C22.21.2.8. Installing a safe haven, especially if there is no response force living in or immediately adjacent to the residence. See Figure C22.F8. for a visual representation.

C22.21.2.9. Assignment of a residential security force.

C22.21.2.10. Use of animals.

C22.21.2.11. Relocating HRP to a more secure location.

**Figure C22.F8. Safehaven concept including residence hall security barrier.**



# C23. CHAPTER 23
# BARRIERS

## C23.1. INTRODUCTION

C23.1.1. Barriers are an integral part of all physical security systems. They are used at the perimeter of DoD installations to perform several functions such as establishing boundaries and deterring and intimidating individuals from attempting unlawful or unauthorized entry. Barriers become platforms on which more sophisticated sensors can be placed to aid in threat detection and classification. Some barriers at the perimeter of DoD installations help shield activities within the installation from immediate, direct observation.

C23.1.2. Barriers are also used at the perimeter of DoD installations to facilitate pedestrian and vehicle ingress and egress control. Barrier use channels traffic through designated access control points, where pedestrians, vessels, and vehicles can be monitored and searched for contraband, explosives, or other threats as circumstances warrant.

C23.1.3. Barriers are used within individual buildings on DoD installations for similar purposes. In addition, use of high-security doors, window glazing, and walls can provide building occupants with protection against ballistic penetrations, small arms fire, bomb fragments, and broken glass.

C23.1.4. Table C23.T1. presents a list of both natural and manmade barriers of potential interest to security program planners.

**Table C23.T1. Security Barrier Functions and Examples.**

| Barrier Function | Natural Obstacle | Manmade Obstacle |
|---|---|---|
| Establish Boundary | River, valley, forest line | Walls, fences, hedges |
| Isolate Activity or Discourage Visitors | Mountains or hills, jungle, dense growth, desert | Walls, fences berms, canals, moats |
| Aid Detection of Unauthorized Entry or Intrusion | | Electronic detection devices mounted on boundary, sand strips at boundary of areas to be isolated, electronic devices |
| Impede Pedestrian Passage | Rivers, swamps, natural terrain features | Fences and walls with or without doors or gates |

| Barrier Function | Natural Obstacle | Manmade Obstacle |
|---|---|---|
| Impede Vehicle Passage | Rivers, swamps, natural terrain features | Fences, walls, Jersey bounce barriers, specially designed vehicle barriers, aircraft arresting cable |
| Prevent External Visual Observation | Forests, natural terrain features | Berms, earthworks, walls, solid fences, masonry block screens, translucent glass blocks, polycarbonate sheets, shutters, awnings, draperies |
| Minimize Ballistic Material Penetration | | High berms, earthworks, steel-reinforced concrete or solid-fill masonry walls, blast shields fabricated from steel-ply materials, ballistic-resistant glazing |

C23.2. INSTALLATION PERIMETER BARRIERS

C23.2.1. General Guidelines.

C23.2.1.1. The first line of defense in any physical security system is usually some form of perimeter protection system. The perimeter of a facility is the outermost area that the facility owner has control. In many cases, a simple sign defining an intangible boundary is sufficient to delimit the boundary of a DoD installation. This approach is often used where the expanse of the facility makes physical demarcation impossible or economically infeasible. In other cases, elaborate structures, such as fences or walls, are used to mark the outer boundary of a DoD installation. The following discussion is intended to introduce the range of options available.

C23.2.1.2. An unobstructed area or clear zone should be maintained on both sides of and between permanent physical barriers.

C23.2.1.3. Perimeter protection systems can assume a wide range of forms, in addition to fences and walls. Waterways, forestations, ditches, berms, barricades, vehicle barriers (active and passive), difficult approaches or exit routes, and lighting systems are often used effectively in perimeter barrier systems. An IDS should be considered for the exterior perimeter to provide the earliest possible notification and identification of an intrusion.

C23.2.2. Permanent Structures.

C23.2.2.1. Several permanent structures can be used as perimeters around an entire DoD installation, around enclaves within a DoD installation, or around an isolated building used solely to house DoD activities. The following paragraphs describe some of the favored approaches.

C23.2.2.2. Generally, walls and fences provide less than 15 seconds of penetration resistance, and cannot be relied on for more than very minimal delay. Perimeter walls and fences can serve many other functions. Walls and fences are primarily used to accomplish one or more of the following.

C23.2.2.2.1. Provide a legal boundary by defining the outermost limit of a protected area.

C23.2.2.2.2. Assist in controlling and screening authorized entries into a protected area.

C23.2.2.2.3. Support detection, assessment, and other security function.

C23.2.2.2.4. Cause an intruder to make an overt action that shall demonstrate intent to penetrate the protected area.

C23.2.2.2.5. Serve as a ballistic shield against small arms fire, deny visual observation of activities being conducted within the enclosed area, and add an increased deterrence to scaling.

C23.2.2.2.6. Channel visitors through an opening providing better access control.

C23.2.2.2.7. Create a standoff distance to protect against bomb blast over-pressure effects.

C23.2.2.3. A well-constructed perimeter security wall.

C23.2.2.4. Walls of lesser construction may be worthwhile physical security system additions to DoD or U.S. Government installations at home or abroad.

C23.2.2.5. In using exterior walls to enhance security, several considerations must be addressed.

C23.2.2.5.1. Walls should be positioned far enough away from other structures—such as trees, telephone poles, antenna masts, or adjacent structures—that may be used as aids to circumvent the barrier.

C23.2.2.5.2. Walls should be built in a location such that vehicles cannot park immediately adjacent to them, thereby affording potential intruders a platform from which to mount an attack.

C23.2.2.5.3. Additional toppings on walls should be considered. These include concertina wire, picket fences, multiple-strand razor or barbed wire, and other devices to inhibit efforts to vault or go over the top of the wall.

C23.2.2.5.4. Bollards or other barricades can be used to establish permanent or temporary barriers to control vehicle access while allowing pedestrian traffic to flow freely.

C23.2.2.6. Fences are frequently used to establish boundaries between a perimeter of an installation and its surrounding area. Fences, particularly at military facilities, are typically standard metal chain-link fences. Barbed wire and field fencing are often found at major installations and overseas, as well as wood fences.

C23.2.2.7. Chain link or woven metal mesh fences can be used to establish an outer perimeter. Chain link fences are excellent platforms on which to mount surveillance systems and intrusion detection devices.

C23.2.2.8. Chain link or woven metal mesh fences can be stiffened and made somewhat more resistant to penetration by vehicles through several techniques. Vertical support posts can be installed at 4-foot intervals instead of 8- or 9-foot intervals; aircraft arresting cables can be installed parallel to the ground at 6 inches and then 30 inches above the ground. These techniques can increase the resistance to vehicle penetration offered by such fences, thereby adding to the delay in penetration.

C23.2.2.9. Chain link fences can be topped with concertina wire, razor wire, or multiple strands of barbed wire. Such toppings can be useful in adding to the psychological barrier effect of a fence, but are not likely to increase substantially the amount of delay in penetration to the facility.

C23.2.2.10. The use of picket fences, especially those made of metal, are discouraged because fence components can become a significant hazard from flying debris. Their negative blast characteristics may exceed their positive physical deterrence value.

C23.2.3. Temporary Barriers.

C23.2.3.1. Vegetation. Hedges and natural vegetation are both economical and aesthetic and blend into their surroundings. They provide a symbolic but practical delineation of the

property line. Unless hedges are thick and covered with thorns or pointed leaves, they can be easily breached. Once breached, they can provide some degree of cover from exterior observation. The main disadvantages of hedges are the time required to grow them to sufficient size, especially if a portion dies, and their continuing requirement for periodic maintenance. They are more suitable for residences than office buildings. However, hedges can be used in either situation when appropriate.

C23.2.3.2. Portable Fencing.

C23.2.3.2.1. Portable fencing can be used as a temporary perimeter to establish psychological barriers and to channel pedestrian and vehicle movement.

C23.2.3.2.2. Several portable fencing materials are available. Among the materials available on the commercial market are the following.

C23.2.3.2.2.1. Plastic netting.

C23.2.3.2.2.2. Rolled wooden slat or support wire fencing (snow fencing).

C23.2.3.2.2.3. Fixed panels of chain-link fencing materials supported by temporary posts anchored with cinder blocks or other stabilizing materials.

C23.2.3.2.2.4. Fixed panels of board-on-board wooden plank fencing or wooden stockade fencing supported by temporary posts anchored with cinder blocks or other stabilizing materials.

C23.2.3.2.3. Other materials available within the Department of Defense that can be used as portable fences include the following.

C23.2.3.2.3.1. Coils of concertina wire.

C23.2.3.2.3.2. Canvas panels supported by tent posts.

C23.2.3.2.3.3. Plastic sheeting materials supported by tent posts.

C23.2.3.3. Temporary Walls or Rigid Barriers. Several temporary devices can be employed to establish barriers against high-speed vehicle approaches to DoD installations and facilities. These structures can be installed along approaches to DoD installations or facilities within an installation's boundaries to force vehicles to make tight, slow turns before approaching gates or building entrances. These structures can also be used as temporary barriers to deny access, provided additional barriers are placed in front of areas to deny high-speed vehicle penetrations. Among the devices available are the following.

C23.2.3.3.1. Concrete vehicle barriers (Jersey barriers).

C23.2.3.3.2. Concrete or sand-filled oil drums.

C23.2.3.3.3. Concrete bollards or planters.

C23.2.3.3.4. Steel or steel-reinforced concrete posts.

C23.2.3.3.5. Sand or water-filled plastic vehicle barriers (Jersey barriers).

C23.2.4. Expedient Perimeter Devices

C23.2.4.1. Under certain circumstances, it may be necessary to establish a perimeter for psychological purposes.

C23.2.4.2. To mark a perimeter, the following materials can be used.

C23.2.4.2.1. Painted line.

C23.2.4.2.2. Rope (cloth rope, steel cable, chain, etc.).

C23.2.4.2.3. Colored plastic tape (commercially available products come in multiple colors and are without lettering, or contain warnings such as "caution," "construction area," "danger," or "police line—do not cross").

C23.2.4.2.4. A line of sandbags, one or two bags high.

C23.2.4.2.5. Saw horses, empty oil drums, construction barricades, etc.

C23.2.4.2.6. Jersey barriers or concrete vehicle barrier segments.

C23.2.4.3. The purpose of establishing such perimeters is usually to channel movement by pedestrians and vehicles as an aid to threat detection. Use of expedient perimeters can establish security zones within an installation or facility, thereby facilitating threat identification, classification, and assessment. Use of some expedient perimeter devices can add delay to movement within an installation or facility, channeling vehicles and pedestrians through choke points, slowing movement, and giving security personnel additional time to survey and assess pedestrians and vehicles as they approach and proceed through checkpoints.

C23.2.4.4. Under some circumstances, use of expedient perimeters can delay pedestrian threats by changing the configuration of an approach to a building. Erecting "trip wire" barriers in front of doors to be secured after hours or installing water-filled oil drums in a random pattern along a vehicle or pedestrian approach to a building can disorient or impede an intruder who has

been unable to make last-moment observations on changes to the approaches to the targeted DoD asset.

C23.2.4.5. Vehicles in all sizes and configurations can also be used as expedient barriers. Parked bumper-to-bumper, vehicles provide an effective barrier to personnel engaged in routine activity. Most people shall not attempt to vault a line of vehicles parked such that their bumpers touch, nor shall they usually attempt to pass underneath such a line. Large construction-type vehicles or armored vehicles can be very effective as supplemental barriers behind gates to installations or facilities. Vehicles parked randomly on open, straight expanses of road, aircraft taxiways, or runways can interfere with unauthorized use of those facilities.

C23.3. VEHICLE BARRIERS.

C23.3.1. Vehicle Barriers Systems. In recent years, all agencies and departments of the U.S. Government have taken active measures to restrict the ability of explosive-carrying vehicles to reach buildings housing Government personnel. The destruction of the Khobar Towers Complex in Dhahran, Saudi Arabia, in 1996, as well as the bombing of the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, in 1998, effectively sensitized the Department of Defense to the need for vehicle barriers to hold potential threats away from critical structures. The DOS is responsible for the approval of vehicle barriers and maintains a database of approved barriers. Vehicle barriers are available in several different systems the following are several types of systems.

C23.3.1.1. Active Barrier Systems. Barrier systems are considered active if they require action by personnel or equipment to permit entry. Systems that move solid masses, beams, gates, tire shredders, and fences, and those that create pits or ramps, are active barriers. Vehicles (trucks, bulldozers, etc.) are active barriers if used in that mode in the access control system.

C23.3.1.2. Passive Barrier Systems. Barrier systems are passive if their effectiveness relies on their bulk or mass and they have no moving parts. Such systems typically rely on weight to prevent entry into a restricted area. Sandbags, highway medians (Jersey barriers), angled posts, tires, and guardrails are examples of passive barrier systems.

C23.3.1.3. Fixed Barrier Systems. Barrier systems are fixed if they are permanently installed or if heavy equipment is required to move or dismantle the barriers. Hydraulically operated rotation or retracting systems, pits, and concrete or steel barriers are examples. Fixed barrier systems can be either active or passive.

C23.3.1.4. Movable Barrier Systems may be transferred from place to place. They may require heavy equipment or personnel to assist in the transfer. Highway medians, sandbags (large numbers), 55-gallon drums (filled), or vehicles are typical examples.

C23.3.1.5. Portable Barrier Systems are used as temporary barriers. A movable system can be used, but may take more time, money, and effort than desired. Examples of portable barriers are ropes, chains, cables, vehicles, or tire-puncture systems.

C23.3.1.6. Expedient Barrier Systems comprise one or more articles or vehicles normally used for other purposes that have been pressed into use on a temporary or interim basis. Examples of expedient barrier systems are the use of heavy earth-moving or engineering equipment, armored personnel carriers, or tanks as perimeter gates or perimeter gate barriers.

C23.3.2. Vehicle Barrier Design Considerations.

C23.3.2.1. Location. Vehicle barriers can be located in different areas: facility entrances, enclave entry points (gates), or selected interior locations (that is, entrances to restricted areas), headquarters and other primary gathering facilities. Exact locations vary among installations; however, in each case the barrier should be located as far from the critical resource as practical. When possible, gates and perimeter boundary fences should be positioned outside the blast vulnerability envelope or repositioned within the installation to a more secure area. It is more cost-effective to secure a specific critical resource than an entire facility. Consolidating critical resources into one central area may heighten security, but is also reduces the number of target areas for the aggressor to attack.

C23.3.2.2. Aesthetics. The overall appearance of a vehicle barrier plays an important role in its selection and acceptance. Many barriers are now made with aesthetics in mind so that a “fortress effect” can be avoided.

C23.3.2.3. Safety. A vehicle barrier system should be respected as a tool capable of wielding deadly force. Even when properly installed to perform its intended purpose, it can kill or seriously injure individuals as a result of accidental or inadvertent activation caused by either operator error or equipment malfunction. Proper warning signs, lights, bells, and adequate colors should be provided to identify the barrier to ensure personnel safety. Further, specific employment instructions and operator training is essential. Questions such as the following should be addressed to manufacturers and current users to identify potential safety considerations affecting the selection of a barrier system: What happens when power is lost? Is there an emergency stop switch? Is lighting adequate? What safety options are available from the

manufacturer? Once installed, vehicle barriers should be well-marked and pedestrian traffic channeled away from unsafe areas.

C23.3.2.4. Reliability. Many vehicle barrier systems have not been in production long enough to have developed a reliability history. Some systems are placed in environments not envisioned by the manufacturer, while others have developed problems not anticipated by either the manufacturer or the user. Many manufacturers indicate a remarkable willingness to resolve problems and work effectively with users. Backup generators or manual operating provisions are available. Spare parts and supplies also should be maintained on hand to facilitate rapid return of the barriers to full operation.

C23.3.2.5. Maintainability. Many manufacturers provide aesthetics, diagrams, maintenance schedules, and procedures for their systems. They should also have spare parts available to keep barriers in nearly continuous operation. Manufacturers should be asked for maintainability requirements in the form of training, operation, and maintenance manuals. If these requirements are not available, the agency that purchases the vehicle barrier must develop maintenance instructions for the user. In addition, for periods of vehicle barrier maintenance, the user should consider providing alternate traffic routes.

C23.3.2.6. Cost. Traffic in restricted or sensitive areas should be minimized and the number of entryways limited. Reducing traffic flow and the number of entryways may provide increased security and lowered costs for the vehicle barrier system. Installation costs, that may be excessive and the cost of operating the system should be addressed during the barrier selection process. Complexity and lack of standardized components can incur higher costs for maintenance and create long, costly downtime periods. Reliability, availability, and maintainability data on the system also affect costs.

C23.3.2.7. Active Barrier Operations. A barrier is active if it requires action by personnel or equipment to operate. It should allow for continuous operation with minimal maintenance and downtime, so that it may be employed during normal and emergency conditions. Emergency procedures must be available to operate the barrier in case of system breakdown or power failure. Selection of a normally open or closed option should be evaluated in light of experienced or expected traffic. Evaluate system failure modes to ensure that the barrier fails in either the open or closed position, as dictated by security and operation considerations. Barrier employment criteria should be linked to use of force and/or rules of engagement training for security personnel.

C23.3.2.8. Clear Zones. Barriers installed in clear zones must be designed so that they shall not provide terrorists with a protective hiding place or shield.

C23.3.2.9. Operating Environment. The environment of the facility must be considered when selecting vehicle barrier or barrier options. Hinges, hydraulics, or surfaces with critical tolerances may require heaters to resist freezing temperatures and ice buildup, or they may require protection from dirt and debris. If options that protect against environmental conditions are not available, the system may become inoperative.

C23.3.2.10. Installation Requirements. The vehicle barrier selected must be compatible with the location in which it is installed, the available power source and its reliability, and other security equipment. Protection of primary and alternate power sources and hydraulics must be considered.

C23.3.2.11. Operator Training. Most users recommend operator training regardless of the simplicity of the system. Operator training prevents serious injury and legal liability as well as equipment damage caused by improper system operation. Manufacturers do not always provide information on possible operator problems. The user may have to develop individual checklists for normal and emergency operating procedures to avoid experiencing serious problems.

C23.3.2.12. Manufacturer Options. Manufacturers offer additional features with their systems in the form of options or optional equipment. Some options enhance system performance while others facilitate maintenance or safety. Options increase system cost and may increase maintenance requirements. Because options vary among manufacturers, each company should be consulted to determine which options are offered and their cost.

C23.3.3. Other Vehicle Barrier Considerations. The following should also be considered when assessing vehicle barrier requirements and options.

C23.3.3.1. Avoid installing sunken (underground) barriers unless the excavation can be drained. Water collection shall cause corrosion, and freezing weather may incapacitate the system.

C23.3.3.2. Avoid providing vehicle barriers at entrance gates without providing equivalent protection along the perimeter of the protected area.

C23.3.3.3. Avoid expending large amounts of funding for soft protection of the installation perimeter. It is generally more cost-effective to provide heavy protection of individual buildings or zones within the perimeter.

C23.3.3.4. Avoid providing perimeter vehicle barriers that are not patrolled or frequently observed. Most types can be overcome quickly with simple tools or ramps.

C23.3.3.5. Avoid placing guard posts next to barriers.

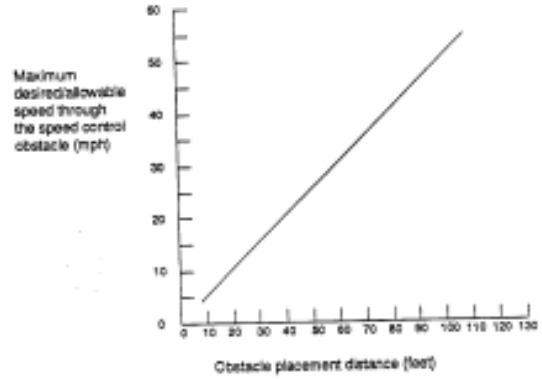
C23.3.3.6. If separate barriers are used for exits and entrances, avoid controlling only the entrance while leaving the exit barrier open. Require positive control for the exit also.

C23.3.3.7. Avoid a long, straightaway road to a crash-resistant barrier system. Where this cannot be avoided, provide a passive-type barrier maze to slow traffic prior to arrival at the vehicle barrier. Figure C23.F1. illustrates a moving vehicle, serpentine barrier system used to slow vehicle speed.

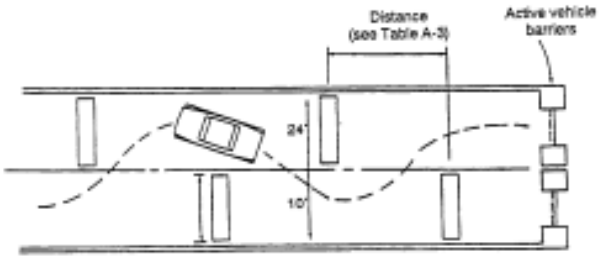
**Figure C23.F1. "Serpentine" Moving Vehicle Barrier.**

## Moving Vehicle - Speed Control Obstacles

- **"S" curves**
- **90 degree bends**
- **Traffic circles**
- **Speed bumps**
- **Serpentines**




**Ref: TM 5-853-2**




C23.4. PERIMETER BARRIER PENETRATIONS AND ACCESS CONTROL.

As previously discussed, vehicle barriers should be placed outside the installation perimeter or outside an installation interior perimeter. The following discussion addresses vehicle access to an installation or facility once the vehicle is past the vehicle barriers described above.

C23.4.1. Installation Vehicle Access Control Measures.

C23.4.1.1. Restrict installation vehicle entry/exit points to a minimum. To maximize traffic flow and economize physical security requirements, only two regularly used vehicular entry-exit points are necessary. Both should be similarly constructed and monitored. The use of the entry points should be dictated by the size of the vehicles requiring entry. This shall compliment the employment of vehicle barriers and other physical and procedural security requirements in advanced security postures. One entry point should be designed to accommodate large and/or oversized vehicles, and the other for normal sized vehicle traffic.

Where possible, a tertiary gate can be planned for contingencies. Depending on the size and nature of the facility, a gate for emergency vehicular and pedestrian egress should be installed outside the perimeter to increase the setback of the buildings. In either case, design and placement of bollards or other anti-vehicular devices should be considered in the early planning stages.

C23.4.1.2. Protect all vehicle access points against reverse entry and ramming attacks. All entry-exit points should be secured with a heavy-duty sliding steel, iron, or heavily braced chain-link gate equipped with a heavy locking device. Approaches to all vehicle exit points should be aligned such that high-speed approach from outside the perimeter is not possible. The goal of such realignment is to ensure to the maximum degree possible that intruders cannot simply enter the facility by going against the flow of exiting vehicle traffic. Passive vehicle barriers described above can be incorporated into the road and pedestrian access designs to accomplish this goal.

C23.4.1.3. All entry-exit points should be constructed with protection against a ramming vehicle attack. Passive vehicle barriers described above can be incorporated in ingress-egress designs to make ramming attacks difficult. Vehicle perimeter penetration gates can also be designed to be highly resistant to ramming attack. Additional vehicle barriers can be installed behind the gates to provide defense in depth against such attack.

C23.4.1.4. All gates not in use and under direct supervision should be locked; it should be verified that only security personnel could operate the locks. Emergency gates should be securely locked and randomly checked during each shift. Security personnel should physically lock and re-lock all gates or other penetrations secured with locks to verify that the locks in use belong to the security department and not some other activity on the installation or would-be intruders. Any lock found inoperable by the security personnel should be removed immediately and a security department lock substituted in its place. Control over keys is essential.

C23.4.1.5. Storage lanes, protected guard positions, and hard points for security guard booths should be included on plans for revised vehicle access to permit multiple vehicle inspections for explosives, weapons, or contraband outside the installation perimeter.

C23.4.1.5.1. Some of the measures implemented at DoD facilities in response to terrorist threat may result in significant traffic congestion at vehicle entry gates. Such congestion can be reduced if storage lanes can be included in installation access alignments. During periods of rigorous vehicle inspection, security personnel can inspect vehicles and their occupants in

groups. Vehicles waiting their turn for inspection can be held in storage lanes adjacent to the installation. This approach to vehicle inspection and installation access shall ease traffic congestion for those not seeking access to the DoD installation. It shall also place vehicles and their operators waiting inspection in an area where they can be monitored for indications of potentially threatening behavior.

C23.4.1.5.2. Be sure that vehicle barriers, storage lanes, security booth tie down points, and protected positions for backup security forces are considered as an integrated security package. Doing so shall ensure that vehicle barriers do not obstruct fields of vision or fields of fire for the backup security forces responsible for protecting guards conducting vehicle inspections.

C23.4.2. Vehicle Access Control Systems.

C23.4.2.1. Primary entrances to a facility should have a booth for security personnel during peak traffic periods and automated systems for remote operations during other periods. A vehicle search bay exterior to the access control gate and configured to inhibit damage from explosive laden vehicles is optimal.

C23.4.2.2. The following capabilities are recommended for vehicle access control systems.

C23.4.2.2.1. Electrically operated gates to be activated by security personnel at either the booth or security control center or by a badge reader located in a convenient place for a driver.

C23.4.2.2.2. CCTV with the capability of displaying the full-facial features of a driver and vehicle characteristics on a monitor at the security control center.

C23.4.2.2.3. An intercom system located in a convenient place for a driver to communicate with the gatehouse and security control center.

C23.4.2.2.4. Bollards or other elements to protect the security booth and gates against a car crash.

C23.4.2.2.5. Sensors to activate the gate, to detect vehicles approaching and departing the gate, to activate a CCTV monitor displaying the gate, and to sound an audio alert in the security control center.

C23.4.2.2.6. Lighting to illuminate the gate area and approaches to a higher level than surrounding areas.

C23.4.2.2.7. Signs to instruct visitors and employees.

C23.4.2.2.8. Road surfaces to enable queuing, turnaround, and parking.

C23.4.2.2.9. Vehicle bypass control (that is, gate extensions), such as low and dense shrubbery, fences, and walls.

C23.4.2.3. Vehicle perimeter access barriers and gates should be controlled by key card or remote operation by the central security office when the gatehouse is not staffed. An intercom and CCTV camera with low-light and area scan capability should be provided to facilitate communication between the central security office and personnel in vehicles seeking entry when the access point is closed. The access point should be sufficiently illuminated such that all vehicle occupants can be seen via CCTV systems.

C23.4.2.4. Overwatch. Vehicle entry control points (ECPs) with weak or non-existent barriers should be augmented at higher FPCONs with an overwatch position. The overwatch for an ECP is a manned position that provides observation and the ability to employ deadly force against vehicles that attempt to bypass, ram, or otherwise run through an ECP. The overwatch should be equipped with a weapon that can stop a vehicle by disabling it or killing the driver. This weapon should be no smaller than a 7.62mm medium machine gun. Rules of engagement, and command and control between the overwatch position and the ECP must be planned in detail.

C23.4.3. Perimeter Security Office Booth.

C23.4.3.1. At the vehicular entry-exit, a security officer booth should be constructed to control access. At facilities not having perimeter walls, the security officer booth should be installed immediately inside the facility foyer.

C23.4.3.2. The security officer booth should be completely protected with reinforced concrete walls, ballistic doors, and ballistic windows. The booth should be equipped with a security officer duress alarm and intercom system, both annunciating at the facility receptionist and security officer's office. This security officer would also be responsible for complete operation of the vehicle gate. If necessary, package inspection and visitor screening may be conducted just outside of the perimeter security officer booth by an unarmed security officer equipped with walk-through and handheld metal detectors. Provisions for environmental and personal comfort should be considered when designing the booth.

## C23.5. BUILDING PERIMETER BARRIER SELECTION AND HARDENING

### C23.5.1. Building Perimeters.

C23.5.1.1. Perimeters surrounding buildings located off DoD property vary from those with industrial-type perimeter fences to those composed of little more than aesthetically attractive landscaping.

C23.5.1.2. Exterior IDS sensors are not recommended for the perimeter protection system of most office buildings unless personnel and vehicle access is to be controlled at the perimeter entrance gate, or the building is required to be secured during non-duty hours to protect sensitive assets. Where access control is to be administered at the entrance gate, exterior sensors should be activated around the remainder of the perimeter during working hours.

C23.5.1.3. When IDS sensors are installed around the perimeter, CCTV should be utilized in support of IDS to allow remote assessment of alarm activation.

C23.5.2. Exterior Doors. Limit the number of doors to the bare minimum necessary for emergency evacuation; ideally permit normal entry and egress through only one door. Because of their functional requirements, construction, and methods of attachment, doors are less attack-resistant than adjacent walls and frequently provide a "soft spot" in an otherwise attack-resistant structure. For this reason, the number of doors to a facility or residence should be reduced to an absolute minimum and, in cases where more than one door exist, only one should be provided with outside-mounted locks and entry hardware. All others should, where practicable, present blank, flush surfaces to the outside to reduce their vulnerability to attack.

C23.5.3. Windows. Windows of various sizes and configurations are required in the walls of most structures for the passage of light, ventilation, and observation. Windows are always significant weak points in an individual facility protection system because of their low penetration resistance. Further, window glazing represents significant flying debris hazards from an explosive blast. Special precautions should be taken to harden windows from both penetration and blast.

C23.5.4. Utility Access. A careful inspection of the structure's exterior must be made to locate any utility openings. In conventional building designs, utility openings, manholes, tunnels, air-conditioning ducts, filters, or equipment access panels can provide a vulnerable entrance route with no significant delay. If such openings cannot be eliminated, their delay times must be increased. Security screens or grates can be installed over utility access openings. The

techniques described to secure a window or skylight using bars, grates, or mesh can be used to restrict access to a structure via utility penetrations.

C23.5.5. Duress Alarms. Duress alarms are devices that can be activated manually in the event of an unauthorized penetration attempt. An audible alarm can be sounded locally in an attempt to frighten off the intruder. A silent alarm can also be sent to the organization's security center or other location where the alarm would summon immediate assistance. Duress alarms can be placed in inconspicuous locations and can even be disguised as common office objects or home decorations. Duress alarms can also be incorporated into home or office furnishings.

C23.5.6. Communication Systems. Telephones are needed at all times, and secure means of communication are essential between a secured area and its dedicated response force. Telephones in many parts of the world are unavailable, unreliable, and, as in many CONUS locations, exposed and vulnerable to terrorist attacks. The security planner often has little knowledge and no control over where or how the telephone lines are routed or whether they are even minimally secured. Telephone systems required for security and safety of executive personnel must use secure dedicated lines. Where this is not possible, a secure radio communication link must be established. Portable, handheld radios can assure backup communication when other communication links are severed.

C23.5.7. IDS

As discussed earlier in this Chapter, incorporation of IDS into the overall physical security system shall help to mitigate the vulnerabilities identified above.

C23.6. INTERIOR BARRIERS.

C23.6.1. Barriers may be used within the interior of facilities to accomplish the same functions as are performed by an installation's access barriers. Interior barriers establish boundaries or lines of demarcation of different activities (and differing levels of security) within a facility. They deter and intimidate individuals from attempting unauthorized entry. As in the case of installation-level barriers, they are platforms on which intrusion detection sensors or surveillance systems can be mounted. Barriers may be used within a facility to channel pedestrian and service vehicle traffic.

C23.6.2. Barriers are used within individual buildings on DoD installations for similar purposes. In addition, use of high-security doors, window glazing, and walls can provide building occupants with protection against ballistic penetrations such as small-arms fire, bomb fragments, and broken glass.

C23.6.3. General Constraints on Facility Barrier Selection.

C23.6.3.1. A wide range of materials and construction techniques can be used within a facility to erect a barrier. The selection of materials and a construction technique is constrained by the strength and load-bearing capacity of the facility itself. The specific construction site conditions may also constrain or limit barrier construction within a facility. The requirement to access utility lines, fire-protection systems, or specific emergency ingress or egress routes may dictate use of movable barriers as opposed to fixed, anchored barriers. Perceived terrorist threat capabilities, construction costs, local building codes, and limitations on tenant construction for leased facilities also constrain or limit the selection of materials and types of barrier construction undertaken. The following discussion identifies a selection of materials and techniques that may be appropriate for enhancing the security and protection of DoD assets.

C23.6.3.2. Further information is available from the Service security engineering branch within each Service's facility engineering organization. Experts at the Defense Threat Reduction Agency can provide additional technical information and assistance to the DoD Components.

C23.6.4. Barrier Materials.

C23.6.4.1. An infinite range of materials and construction techniques is available to help security planners meet specific needs. Materials and techniques used to enhance the building exterior's resistance to penetration can also be applied within a building. The following figure illustrates some of the materials that can be used to erect barriers within a facility. Table C23.T2. illustrates that relationships exist among the materials used, the type of construction technique used, and the specific barrier function to be performed.

C23.6.4.2. Use of multiple barrier materials and construction techniques can sometimes accomplish one barrier purpose with less expensive and less disruptive construction techniques. For example, use of ballistic-resistant glass-clad polycarbonate panels accompanied by overt surveillance cameras, warning signs, and annunciator devices (such as flashing lights and buzzers) can create an intimidating picture of a high-security barrier adjacent to a high-security passageway at a cost equal to or less than the construction of a reinforced masonry wall to accomplish the same purpose.

C23.6.4.3. Given physical security system-level performance requirements, planners have considerable flexibility in choosing materials and techniques to obtain required levels of protection. Tables C23.T2. and C23.T3. are merely illustrative of the range of materials and their applications. Consultations with the security engineering departments of Service civil

engineering organizations or DTRA should be held before embarking on any detailed physical security construction to ensure that the materials and techniques selected shall in fact meet the stated security requirement.

**Table C23.T2. Selected Facility Barrier Materials.**

| Barrier Function | | | | | |
|---|---|---|---|---|---|
| Selected Permanent and Temporary Barrier Materials | Establish Boundaries | Deter Unauthorized Entry | IDS or Surveillance Sensor Platform | Prevent Visual Observation | Channel Pedestrian and Vehicle Traffic |
| 1. Reinforced masonry wall, full height | P | P | P | P | P |
| 2. Reinforced masonry wall, half height (4’ high) | P | | P | P | P |
| 3. Unreinforced masonry wall, full height | P | P | P | P | P |
| 4. Unreinforced masonry wall, half height | P | | P | P | P |
| 5. 3/4” drywall, full height, studs 16” apart | P/T | P/T | P/T | P/T | P/T |
| 6. 3/4” drywall, half height, studs 16” apart | P/T | T | P/T | P/T | P/T– |
| 7. 3/4” plywood, full height, studs 16” apart | T | T | T | T | T |
| 8. 3/4” plywood, half height, studs 16” apart | T | | T | T | T |
| 9. Safety glass panel | P/T | | | | P/T |
| 10. Ballistic-resistant glass panel | P | | | | P |
| 11. Acrylic panel | P/T | | | P | P |

| Barrier Function | | | | | |
|---|---|---|---|---|---|
| Selected Permanent and Temporary Barrier Materials | Establish Boundaries | Deter Unauthorized Entry | IDS or Surveillance Sensor Platform | Prevent Visual Observation | Channel Pedestrian and Vehicle Traffic |
| 12. Polycarbonate panel | P | | | | P |
| 13. Glass-clad polycarbonate panel | P | | | | P |
| 14. Safety glass security grid, panels less than 10” diameter each | P | P | | P | P |
| 15. Ballistic-resistant glass security grid, panels less than 10” diameter each | P | P | | P | P |
| 16. Ballistic-resistant steel-ply panels 16 gauge or better | P | P | | P | P |
| 17. Security grills | P | P | P– | | |
| 18. Security shutters, ballistic-resistant materials | | P | | P | |

P = permanent construction

T = temporary construction

A minus sign after the letter means that the material and construction techniques used in erecting a barrier for this purpose may not provide satisfactory security enhancements or may not be especially durable. Use of glass, acrylic, or polycarbonate materials to provide a visual screen requires use of translucent variants of these.

Powered vehicles used within buildings can do significant damage to all perimeter or interior barriers, especially at corners and corridor intersections.

**Table C23.T3. Selected Expedient Barrier Materials.**

| Barrier Function | | | | | |
|---|---|---|---|---|---|
| Selected Expedient Barrier Materials | Establish Boundaries | Deter Unauthorized Entry | IDS or Surveillance Sensor Platform | Prevent Visual Observation | Channel Pedestrian and Vehicle Traffic |
| 1. Plastic sheeting | • | | | • | • |
| 2. Canvas sheets, awnings | • | | | • | • |
| 3. Plywood sheets | • | • | • | • | • |
| 4. Acrylic panels | • | • | | • | • |
| 5. Polycarbonate panels | | | | | |
| 6. Safety tape | • | | | | • |
| 7. Rope | • | | | | • |
| 8. Chains | • | • | | | • |
| 9. Safety barrels or empty oil drums | | | • | | • |
| 10. Traffic cones | • | | | | • |
| 11. Safety nets | • | • | • | • | • |
| 12. Blast curtains | | | | • | |
| 13. Fire curtains | | | | • | |
| 14. Office furniture | • | • | • | • | • |
| 15. Sandbags | • | | • | | • |
| 16. Carpet rolls | | | | | • |

C23.6.4.4. New materials for increasing the penetration resistance of walls, structures, and glazing have been entering the market regularly in recent years. The materials included in this section are only examples; the state of the art is evolving rapidly. The security engineering branches of Service's civil engineering organizations and DNA have expertise available on

request. Consultations with these experts shall ensure selection of optimum materials to meet requirements for security, economy, and efficient construction.

C23.7. INSPECTION AND MAINTENANCE OF BARRIERS AND SECURITY SYSTEM COMPONENTS

C23.7.1. Barriers should be checked at least weekly for defects that would facilitate unauthorized entry, and report such defects to supervisory personnel. Inspections should look for the following maintenance problems that can have adverse implications for security.

C23.7.1.1. Damaged areas (cuts in fabric, broken posts).

C23.7.1.2. Deterioration (corrosion).

C23.7.1.3. Erosion of soil beneath the barrier.

C23.7.1.4. Loose fittings (barbed wire, outriggers, and fabric fasteners).

C23.7.1.5. Growth in the clear zones that would afford cover for possible intruders.

C23.7.1.6. Obstructions that would afford concealment or aid entry or exit for an intruder.

C23.7.1.7. Evidence of illegal or improper intrusion or attempted intrusion.

C23.7.1.8. Unauthorized construction that would facilitate access.

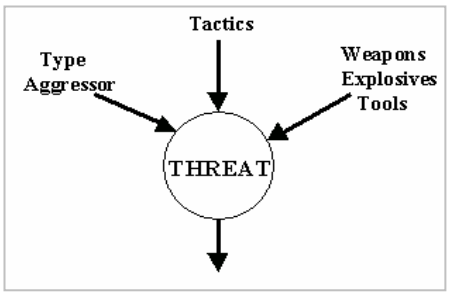
C23.7.2. Locks should be opened and closed to verify that they are in working order and that the locks can be opened and closed by the guard or security force. A lock that cannot be opened by the guard or security force should be removed immediately and replaced with a DoD lock. An investigation should be undertaken to determine whether apparent substitution of the security department lock was an error, an attempt to maintain security following loss or compromise of a lock, or an attempt to create a “trap door” through which terrorists could ingress or egress from a DoD facility. Key control procedures should be implemented to control all keys that are critical to the security of the facility.

# C24. CHAPTER 24
# MILITARY CONSTRUCTION

## C24.1. INTRODUCTION.

C24.1.1. The events of September 11, 2001 serve as a harsh reminder that terrorist attacks can impact anyone, at any time, at any location, and may take many forms. An understanding of the range of threat possibilities; especially type of aggressor, tactics, and associated weapons, tools, or explosives; is essential to design appropriate protective measures. For many reasons, DoD personnel are at increasing risk of harm from terrorism. While terrorists have many options available to them, they frequently use explosive devices when they target large numbers of DoD personnel.

**Figure C24.F1. Understanding the Range of Threat Possibilities.**




Many buildings DoD personnel utilize daily are inadequate to protect against such attacks. In order to mitigate this risk, DoD decision-makers can no longer continue to invest scarce resources in inadequate buildings that DoD personnel occupy, regardless of the threat environment. With an AT mindset, DoD personnel can determine appropriate measures for every aspect of daily operations, especially installation and building planning.

C24.1.2. Evolving Measures. In a dynamic threat environment, an ongoing review and refinement of existing protective measures is needed to successfully prevent future terrorist attacks, or substantially reduce and/or mitigate any threat. Whatever the range or likelihood of threat possibilities, a variety of practical, risk-managed short and long-term solutions are necessary.

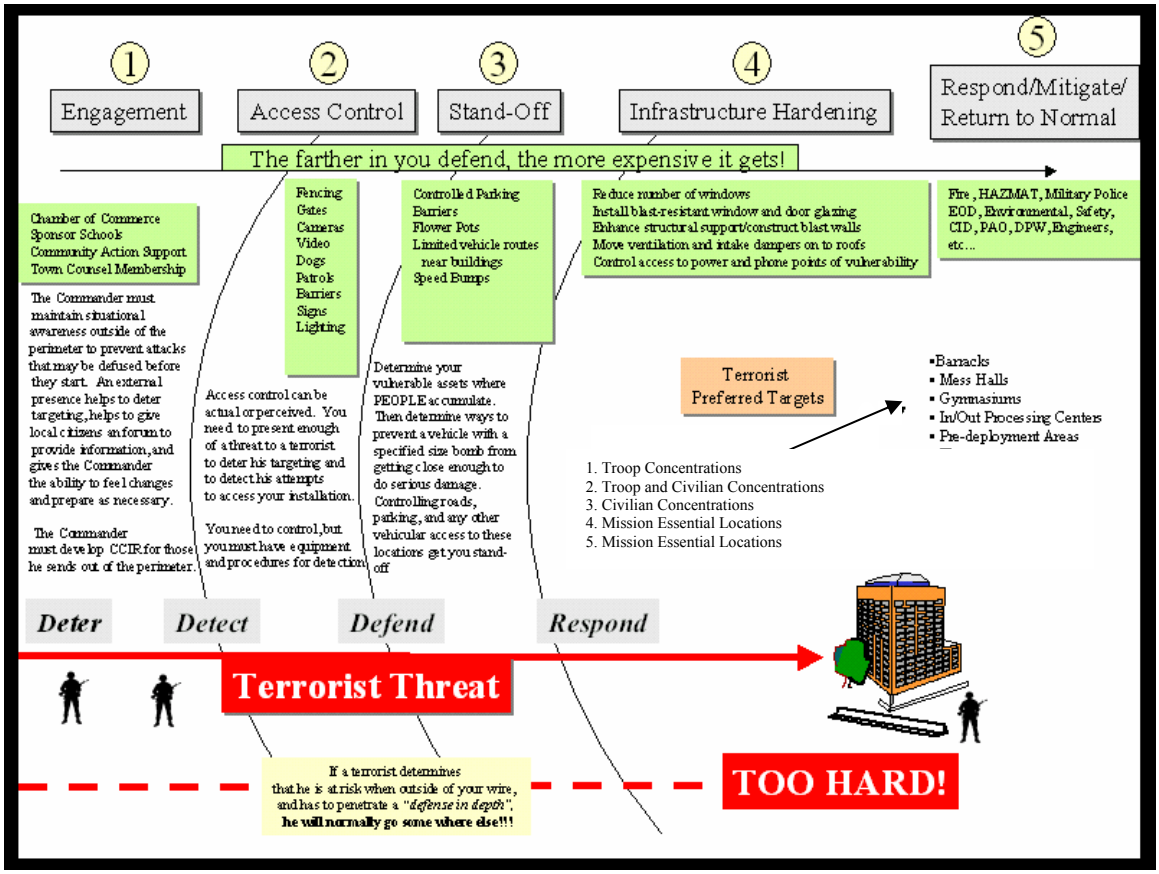
## C24.2. KEY SECURITY CONCEPTS

C24.2.1. General. Security relates to specific measures taken by the DoD Components, activities, or installations to protect themselves against all acts designed to impair its effectiveness. Whether security protective measures are to be employed before, during and/or after a terrorist incident, each one must be identified, resourced, and put in place prior to an

incident. Specific security measures provide wide-ranging capabilities such as deter, detect, assess, communicate, deny/delay, defend, mitigate, respond, and restore. Sample active and passive security measures may utilize security forces, military working dogs, barriers, surveillance, IDS, lighting, badges, and security locking systems.

C24.2.2. Physical Security. Physical security focuses on physical measures and procedures designed to safeguard assets from likely aggressors. Assets generally describe land/geography, buildings, modes of transport (ground, air, and sea), personnel, and smaller objects (packages, suitcases, equipment, etc.). Key physical security tasks DoD personnel can perform to reduce or mitigate potential harm caused by aggressors include assess (ability to identify friend/foe as far away as possible), control access (keep foe from harming assets and facilitate friendly access), move assets (disperse/centralize/combination to enhance survivability), and provide protection (personal protective equipment, hardened buildings/vehicles, weapons and forces). For example, access control involves key operational concepts including defense in depth, as shown in figure C24.F2 desired degree of control, inspection/search procedures, enforcement, restricted area identification and RAM.

**Figure C24.F2. Defense in depth.**



C24.2.3. Security Engineering. Security engineering integrates the assets to be protected, the threat to those assets, the desired level of protection, and an examination of existing constraints and available opportunities to establish a design criteria as the basis to develop specific protective measures. Security engineering works with all security concepts, including those described herein, to identify effective solutions that integrate many factors, especially procedures, resources, and construction to enhance protection of all DoD personnel and associated critical assets within acceptable risk levels to address the range of threat possibilities. As a part of security engineering, antiterrorism protective construction measures and practices focus on facilitating all other protective measures while incorporating greater resistance to terrorist attack into all installation and building design.

**Figure C24.F3. Key inputs to security engineering design**

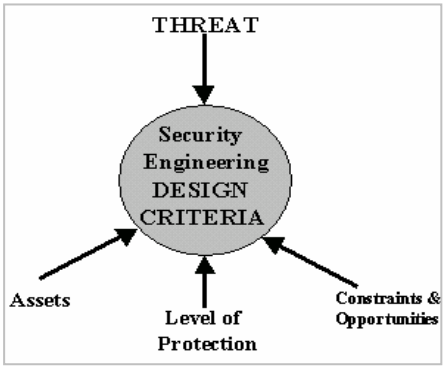
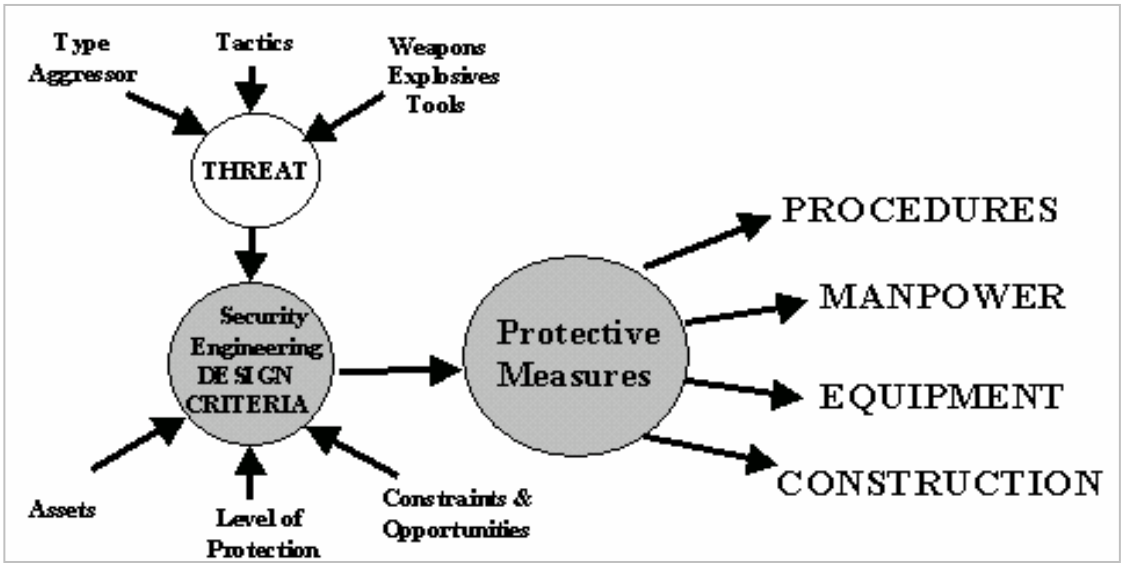



**Figure C24.F4. Protective measure development.**



C24.2.4. Construction Planning. Although predicting specific threats is a difficult task, proper planning and integration of force protection considerations into installation plans provide a solid foundation for anticipating, preventing and if necessary, reacting when terrorist incidents or other emergencies unfold. Leadership guidance and support undergirds all force protection efforts to address the terrorist threat. Strong relationships are needed amongst all key installation decision-makers and advisors, including every separate organization and specialized functional area. Examples of such entities includes fire fighting, communications, engineering and public works, emergency medical services, public health, environmental and HAZMAT, resource support, emergency management, security and law enforcement, explosive ordnance disposal, and master planning.

C24.2.4.1. Planning Teams. Effective planning teams possess the following qualities:

C24.2.4.1.1. Obtain the Right Information. Know how and where to obtain the right information to facilitate planning.

C24.2.4.1.2. Involve Others. Ensure the right people are involved in the planning process and clarify all roles and responsibilities.

C24.2.4.1.3. Focus Time and Energy. Focus the planning effort and related activities. Identifies key strategies, assumptions and information needs while identifying existing and emerging requirements.

C24.2.4.1.4. Formalize Decisions. Facilitate the development and execution of supporting operational plans, procedures and reports. Trains and exercises all aspects of the plan.

C24.2.4.1.5. Obtain Support. Identify, obtain and sustain necessary resources.

C24.2.4.1.6. Coordinate, Integrate, and Synchronize all Related Efforts. Leverage ongoing efforts to optimize effectiveness and efficiency.

C24.2.4.2. Local Antiterrorism Program and Planning Overall Objectives.

C24.2.4.2.1. Deterring terrorist incidents.

C24.2.4.2.2. Employing countermeasures against terrorists.

C24.2.4.2.3. Mitigating the effects of terrorist attacks.

C24.2.4.2.4. Responding and recovering from terrorist incidents should they occur.

C24.2.5. Building Design Strategies. The philosophy of AT building standards is to build greater resistance to terrorist attack into all inhabited buildings. In general, the majority of terrorist incident deaths result from building collapse (progressive failure) and severe injuries occur because of flying debris, especially glass. Building design has traditionally emphasized aesthetics and openness (the more glass the better), protecting occupants from standard loads (people, equipment, building walls and floors) during normal operations, anticipated naturally occurring events (snow, cold, heat, hurricanes and earthquakes), and limited criminal activity (theft). Available construction methods and materials to appropriately mitigate terrorist threats are only starting to influence current construction practices. Accordingly, the primary methods to achieve this outcome are to maximize standoff distance, to construct superstructures to avoid progressive collapse, and to reduce flying debris hazards. The design strategies identified below work together to help focus, synchronize, and integrate available personnel and resources so that effective measures can be identified, implemented and refined for each installation and activity.

C24.2.5.1. Maximize Standoff Distance (Site Planning). The best way to reduce the risk of harm from explosive effects due to terrorist attack is to keep terrorists as far away from inhabited buildings as possible. However, even with adequate space, standoff must be coupled with appropriate operational security procedures in order to be effective. Allowances for standoff distance also provide opportunities to upgrade buildings in the future to meet increased threats or to accommodate higher levels of protection.

C24.2.5.2. Prevent Building Collapse (Structural Design). Even when a large explosion causes extensive damage to structural elements of a building, proper selection of building systems and careful design and detailing can help minimize the extent of major damage. Provisions relating to preventing building collapse and building component failure for taller structures go farthest to protect the lives of building occupants. In addition, structural systems that provide greater continuity and redundancy among structural components shall help limit collapse in the event of severe structural damage from unpredictable terrorist acts.

C24.2.5.3. Minimize Hazardous Flying Debris (Architectural Design). In past explosive events where there was no building collapse, a high number of injuries resulted from flying glass fragments and debris from walls, ceilings, and fixtures (non-structural features.) The glass used in most windows breaks at very low blast pressures resulting in hazardous, dagger-like shards. Minimizing those hazards has a major effect on limiting mass casualties and increasing the chance that building occupants can immediately evacuate after the initial shock. In addition to limiting the size and number of windows of individual buildings where possible, window and

door designs must treat glazing, frames, connections, and the structural components to which they are attached as an integrated system. Laminated glass and other glass technology advancements can be designed to reduce flying glass injuries. Hazardous fragments may also include secondary debris such as those from concrete barriers and site furnishings.

C24.2.5.4. Provide Effective Building Layout (Architectural Design). Effective design of building layout and orientation can significantly reduce opportunities for terrorists to target building occupants or injure large numbers of people in the event of an attack.

C24.2.5.5. Limit Airborne Contamination (Electrical and Mechanical Design). Effective design of heating, ventilation, and air conditioning systems can significantly reduce the potential for chemical, biological, and radiological agents being distributed throughout buildings should they be used. Only a fully functioning collective-protection shelter can provide total protection. Systems should be turned off to reduce or eliminate contaminants from spreading if detected.

C24.2.5.6. Provide Mass Notification (General Design). Providing a timely means to notify building occupants of threats and what should be done in response to those threats reduces the risk of mass casualties. This strategy can be implemented using fairly low-tech, well-practiced procedures. However, in practice this strategy is extremely difficult for most installations and buildings to achieve.

C24.2.5.7. Facilitate Future Upgrades (General Design). Many of the provisions of these standards facilitate opportunities to upgrade building protective measures in the future if the threat environment changes.

C24.2.6. Assumptions. All plans are based on key assumptions that must be identified, made explicit, and understood if the personnel required to execute them are to recognize when the changing threat environment or realities at a particular location differ. Emerging information that challenges the baseline assumptions upon which protective measures are based must be reviewed to ensure updated information is appropriately addressed. Several general assumption categories are listed below:

C24.2.6.1. Threat. As shown in figure C24.F1. the likely type of aggressor, tactics, and associated weapons (direct and indirect fire), tools, or explosives must be known and updated as necessary. Terrorist activities may cross the entire spectrum of aggressors, tactics and weapons, that security engineering routinely considers.

C24.2.6.1.1. Aggressors. Terrorists (domestic, foreign including paramilitary), saboteurs, spies, extremist protestors, and criminals (unsophisticated, sophisticated, organized criminal groups and vandals).

C24.2.6.1.2. Tactics. Vehicle Bomb (stationary or moving), bomb delivery (mail, supplies), contamination (airborne, waterborne), entry (forced, covert), weapons (standoff, ballistic), exterior, surveillance (visual, acoustic eavesdropping), insider compromise.

C24.2.6.1.3. Weapons/Tools/Explosives. CBRNE.

C24.2.6.2. Levels of Protection. Situations vary, but the degree to which an asset is protected against injury or damage from an attack must be decided. UFC 4-010-01 (reference (aw)) prescribes levels of protection for new, existing and expeditionary/temporary construction. For example, the DoD standards provide a Low level of protection for billeting and primary gathering buildings and a Very Low level of protection for other inhabited buildings. Greater protection is desired for primary gathering buildings and billeting because of the higher concentration of personnel and the more attractive nature of the target.

C24.2.6.3. Controlled Perimeter. Installation and building AT plans and related protective measures are based on assumptions as to whether procedures are implemented that would limit the likelihood that a vehicle (or other mode of transport) carrying specific quantities of explosives could penetrate a controlled perimeter undetected. Similarly, provisions to reject vehicles at entry control points without penetrating the controlled perimeter must also be reviewed.

C24.2.6.4. Building Categories. An assessment of installation assets shall determine which buildings may require a higher level of protection or which may be adequately protected. Individual buildings are constructed of a variety of materials that influence appropriate protective measures. Expeditionary and temporary structures are commonly built in combinations of metal frames and fabric or wood frames and rigid walls. All DoD minimum AT building standards that are unique to expeditionary and temporary structures pertain to site planning. Operational, logistic, and security requirements must be integrated in the overall configuration of structures, equipment, landscaping, parking, roads, and other features. The most cost-effective solution to mitigating explosive effects on any structure is to keep explosives as far away as possible. Most expeditionary and temporary structures cannot be retrofitted or hardened sufficiently for higher threats; therefore, unless adequate planning is done to obtain the needed space to achieve

appropriate standoff, DoD personnel shall be highly vulnerable to terrorist attack. Further definitions of DoD building categories can be found in reference (aw).

C24.2.6.5. Adequate Standoff Distances. The ability to maintain an adequate distance between a potential location for an explosive detonation and the closest point on the exterior of any inhabited building is a key measure designed to safeguard personnel inside the buildings from terrorist attacks. Specific minimum standoff distances were developed to provide survivable structures for a wide range of conventional buildings and expeditionary/temporary structures. These buildings range from tents and wood framed buildings to reinforced concrete buildings. Reference (aw) illustrates specific AT construction standard standoff requirements within a controlled perimeter, in the absence of a controlled perimeter, and for expeditionary and temporary structures. UFC 4-010-02 (reference (ax)) contains minimum standoff distances.

C24.2.7. Policies and Procedures. Policies and procedures are a critical adjunct to any construction standard. Unless indicated otherwise, it is usually assumed that there are means to control access to controlled perimeters, underground parking, and other locations where vehicle access should to be limited. It may be further assumed that unusual packages or containers or improperly parked vehicles shall be recognized as potential terrorist threats and appropriate reactive measures shall be implemented to reduce the potential for casualties. Finally, it may be assumed that policies and procedures shall be developed to support these and other related issues and that those policies and procedures shall be incorporated into antiterrorism plans, training, and exercises.

C24.2.8. Training. Although key to success, it may not be safe to assume that key security and facility personnel shall receive training in security engineering, antiterrorism, and related areas. There are many sources for training, such as the Security Engineering Working Group website, www.sewg.nwo.usace.army.mil, or this Handbook. Several assumptions related to training include: that all DoD personnel have been trained in basic antiterrorism awareness in according to reference (e), that they are able to recognize potential threats, and that they know the proper courses of action should they detect a potential threat.

C24.2.9. Design Codes. While it is not easy to deconflict every requirement that exists, a key assumption is that any provision in DoD or local AT construction standards shall be coordinated with all other applicable building and design codes and Federal building policies. Nothing in those standards should be interpreted to supercede the provisions of any other applicable building or design code. Where other codes mandate more stringent requirements it is assumed that the provisions of those codes shall be followed. Depending on the age, existing

buildings do not likely meet all current design codes, but must do so when being renovated. Design code standards work in tandem with force protection standards to greatly enhance protection of building occupants.

C24.2.10. DoD AT Construction Standard Development. Refer to reference (aw), for detailed information. Also, refer to Combatant Commander, Service and local command guidance for unique, site-specific standards.

C24.2.11. Intent. DoD Minimum AT Building Standards were developed to identify appropriate and enforceable measures that would minimize the possibility of mass casualties resulting from possible terrorist attacks targeting buildings or portions of buildings owned, leased, privatized, or otherwise occupied, managed, or controlled by or for the Department of Defense. These standards provide a baseline level of protection in buildings much like a sturdier car frame and safety glass enhances protection in a moving car, and are generally least costly to incorporate before construction. While complete protection against all potential threats for every inhabited building and occupant may be cost prohibitive, a level of protection can be provided for all DoD personnel at a reasonable cost.

C24.2.12. Execution. The intent of these standards can be achieved through prudent, master planning, real estate acquisition, and refined construction practices. The master planning implications of these standards are not intended to be resolved overnight. They should be considered to be a blueprint for facilities and installations that shall be implemented over decades as those facilities and installations evolve. With adequate standoff, it is generally possible to utilize conventional building construction, supplemented with other minimum requirements (such as laminated glass). Where site specific issues and constraints or mitigation requires protective measures required beyond the DoD standards, those standards shall be incorporated according to their implementing directives, but not to the exclusion of the DoD standards. While many standard provisions facilitate opportunities to upgrade building protective measures in a higher threat environment, they must be in place prior to the initiation of a terrorist attack. These standards assume no specified terrorist threat, but provide limited protection against all threats.

C24.2.13. Specific Construction Protective Measures. While there are many ways to organize the variety of possible construction protective measures available to specific installations, one way to do so generally aligns with the seven previously discussed construction design strategies. The specific measures and other construction considerations described in Appendix 17 generally fall within the four groupings of site planning, structural design, architectural design, and electrical and mechanical design. Other construction terms such as

landscape design, parking security, interior design, fire protection engineering, and electronic security are generally addressed within these same four groupings. Also refer to Appendix 18, to highlight specific structural and infrastructure engineer considerations and questions to help direct installation leaders to implement options or actions.

# AP1. APPENDIX 1
# AT CHECKLIST FOR COMMANDERS AND AT OFFICERS

## AP1.1. INTRODUCTION

Protection of DoD assets is an inherent obligation of management and military commanders. The following checklist is a self-assessment, management tool that can be used by the commanders, agency manager, and/or unit AT Officer to assess the status of his/her AT program. This checklist is structured around the AT Standards outlined in reference (e). Not all the standards are applicable to all levels of command; therefore, Combatant Commander and Service AT guidance should be used where applicable.

AP1.1.1. Questions for commanders/managers to evaluate AT program adequacy:

**Table AP1.T1. Antiterrorism Checklist - Commanders**

| DoD Std | AT METRIC |
|---|---|
| 4, 6, 14, 22 | **Assuming Command:**<br>❑ Does unit have an AT program and security posture appropriate for mission and potential threat?<br>• AT Officer appointed?<br>• AT Working Group (ATWG) designated?<br>• DIA and/or FBI Threat Assessment current?<br>• Vulnerability assessment current?<br>• AT Plan complete?<br>• Program review within past 12 months?<br>• AT Plan exercised within past 12 months?<br>• AT Level I training current?<br>❑ Have you reviewed DoDI 2000.16 and appropriate Combatant Commander/Service AT guidance?<br>• Is Combatant Commander/Service AT guidance implemented? |
| 4, 5, 14, 24 | **Organize for AT:**<br>❑ Does unit have adequate focus on AT?<br>• Is unit ATO school trained?<br>• Are right functions represented in ATWG?<br>• Is ATWG active? Meeting minutes? Accomplishments?<br>• Next meeting? Next action? |
| 4, 7, 8, 9, 10, 15 | **Threat Assessment:**<br>❑ Do Threat Assessments provided by DIA and/or FBI and/or the local threat assessment process?<br>• Identify specific terrorist capabilities, weapons, and tactics (to include WMD).<br>• Provide the necessary information for the commander to help tailor Force Protection Conditions.<br>• Have a review mechanism to provide up to date information.<br>❑ Is unit aware of current and potential threats (conventional and WMD)?<br>• DIA and/or FBI (CONUS) assessed threat level for area?<br>• Combatant Commander-assigned higher local threat level?<br>• Formal Intel assessment on hand & current? |

| DoD Std | AT METRIC |
|---|---|
| | • Relationship with supporting Intel activity?<br>• Is Counter-Intelligence or law enforcement support needed?<br>• Local information considered?<br>• Local information network established?<br>• Aggressive list of threat options identified? |
| 26, 27 | **Vulnerability Assessment (VA):**<br>❑ Do Vulnerability Assessments & the vulnerability process include?<br>• The range of terrorist threat identified in the Threat Assessment.<br>• Recommendations for procedural enhancements and resource requirements.<br>• Provided complete inventory of assets & areas?<br>• Prioritization of assets/areas on criticality?<br>• Catalog of known vulnerabilities?<br>• Provide for annual revisions.<br>❑ Has unit evaluated the vulnerability of all assets to potential threats to support risk management decisions?<br>• When was the last Vulnerability Assessment?<br>• Did last VA reveal significant vulnerabilities?<br>• What is status of remedial actions?<br>• Next scheduled VA? |
| 11, 12, 13, 14, 15, 16, 17, 18 | **Antiterrorism Plan (see AP4 for AT Plan sample):**<br>❑ Does my unit have a suitable AT plan?<br>• How is this plan documented? (Five par. order, or annexes to other orders?)<br>• Does the plan specify the AT mission and concept of operation?<br>• Does the plan layout the task organization and Mission Essential or Vulnerable Areas (MEVAs)?<br>• Does the plan include the Risk Management process, to include annual AT Threat Assessment with WMD coverage?<br>• Is there a process, based on local terrorism threat information to raise FPCONs?<br>• Does plan provide actions at each FPCON?<br>• Does plan provide a baseline for normal ops?<br>• What FPCON measures have been adopted due to local threat?<br>• Does plan provide diagram for Random Antiterrorism Measures (RAMs)?<br>• Does the plan include Security Force operations (including augmentation forces) and post priorities?<br>• Has plan been reviewed within past year to remediate procedural and resource shortfalls?<br>• Has plan been approved by higher HQ?<br>• Received/approved AT plans from lower HQ?<br>• Is the plan executable?<br>• Is the plan resourced?<br>• Does plan mitigate vulnerabilities with policy and procedural solutions?<br>• Does plan address response to incident and mass casualties?<br>❑ Does the AT plan contain, as a minimum, site specific procedures for?<br>• Terrorism Threat Assessments.<br>• AT Physical Security Measures.<br>• Mass notification procedures.<br>• Incident Response Measures.<br>• Consequence Management Measures.<br>• AT considerations for plans/orders for temporary operations or exercises.<br>❑ Does the command have an adequate “Baseline” security posture to include?<br>• General AT and physical security awareness.<br>• Adequately equipped and trained First Response Forces. |

| DoD Std | AT METRIC |
|---|---|
| | • A security posture, capable of sustained operations and commensurate to the local threat that adequately protects personnel and assets.<br>• Plans and procedures to transition from Normal Operations to and Elevated state of readiness/execution.<br>❑ Is there a process for you to evaluate subordinate units and/or tenant commands knowledge and status of their AT responsibilities? |
| 19 | **AT Exercises:**<br>❑ Has AT plan been validated by exercises and is unit ready to execute it?<br>• Has AT plan been exercised within one year?<br>• Have key organizations exercised their roles?<br>• Unit response to increasing threat levels been exercised?<br>• Unit response to incident/mass casualties been exercised?<br>• AT plan been exercised in a manner to heighten awareness? Incorporated RAMs?<br>• Has exercise identified discrepancies? Plan to correct them? |
| 28, 29, 30, 31 | **Antiterrorism Resources:**<br>❑ Does AT resource program support the required long-term security posture?<br>• Defined resource requirements to mitigate security deficiencies?<br>• Requirements justified with risk analysis?<br>• Alternative plans, policy, and procedural solutions considered or implemented?<br>• Does the command have a formal process to track, document, and justify resource requirements and identify resource shortfalls to Higher Headquarters?<br>• Higher HQ approved these requirements?<br>• Does the command request Combating Terrorism Readiness Initiative Funds for emergent and or emergency Combatant Commander AT requirements?<br>• Emergent (OCONUS) needs submitted for immediate support by Combating Terrorism Readiness Initiative Fund (CbT-RIF)?<br>• Does the command incorporate AT requirements into the Program Change Proposal process?<br>• Are Program Change Proposal requirements submitted for out year support of CbT-RIF funded investments?<br>• Status of CbT-RIF and Program Change Proposal requirements in the program/budget process?<br>• AT and security factors adequately weighed in acquisition and use of facilities (both temporary and permanent)?<br>• Current facilities conform to DoD and Component AT MILCON standards?<br>• Do structural engineers and security personnel work together to incorporate AT consideration in building design and review?<br>• Are DoD AT Standards for buildings incorporated into new constructions?<br>• How is technology being used to enhance security and human performance?<br>• What technologies have been identified as recommended/required for higher threat levels/FPCONs?<br>❑ Is the AT Officer a member of the Resource Management Committee? |
| 19, 21, 22, 23, 24, 25 | **AT Training:**<br>❑ Are personnel receiving the appropriate levels of AT training to include?<br>• Level I-IV training.<br>• High Risk Personnel.<br>• AOR specific training prior to deployment.<br>• A system to track and document training.<br>❑ Is individual awareness of terrorism threat sufficient for threat environment/mission?<br>• Annual Level I training current?<br>• AOR updates current and briefed?<br>• Special local individual protective measures briefed and used? |

| DoD Std | AT METRIC |
|---|---|
| 5, 14, 20 | **Program Review:**<br>❑ Is AT program comprehensive, current, and effective?<br>• Can unit do mission under FPCONs in use?<br>• Are critical FPCONs compromised for unit morale or convenience?<br>• Is AT a routine element of daily mission planning and execution?<br>• Are operational patterns varied?<br>• Is OPSEC included in mission planning?<br>• Does unit continually monitor threat and corresponding security posture?<br>• Does unit monitor and control access of visitors and employees in sensitive areas?<br>• Has threat level changed since last VA?<br>• Is threat assessment current and valid?<br>• Are RAMs having desired effect on unit awareness, readiness, and deterrence? |
| 4 | **MOU/MOA:**<br>❑ Is unit conforming to and employing MOU/MOA for local support?<br>• Does unit or any detached personnel fall under State Department for force protection?<br>• Are State Department's force protection instructions on hand for those individuals?<br>• Identified organizations with jurisdiction for law enforcement, health, safety, and welfare of assigned service members on and off duty?<br>• Unit conforming to jurisdictional agreements in these areas (SOFA, inter-agency)?<br>• Identified local community organizations with shared security interests (police, federal law enforcement, hospitals, and public health)?<br>• Mutual aid agreements in place with local community to leverage shared interests?<br>• Mutual aid agreements been reviewed by higher HQ?<br>• Mutual aid agreements executable (liability, jurisdiction, capabilities)? |
| 10, 17, 18 | **Mitigate WMD Effects:**<br>• Has unit prepared for WMD attack?<br>• Does AT plan consider terrorist use of WMD (CBRNE)?<br>• What are AT plan assumptions concerning the worst case threat options?<br>• Procedures for detection of unconventional CBRNE attacks?<br>• Unit training include awareness of indicators of unconventional attacks?<br>• Do all personnel have individual protective equipment available?<br>• Are collective protective systems available?<br>• What NBC detection equipment is available?<br>• What decontamination equipment is available? |
| 28, 29, 30 | **Off-installation Housing:**<br>• Are troops housed off-installation adequately secured?<br>• Service members in Moderate, Significant, and High threat areas receive instruction and supervision in residential security measures?<br>• In such areas, do unit AT response plans include current residence location information for all unit members residing off installation?<br>• In such areas, do units coordinate with local law enforcement authorities for protection of unit members residing off-installation (MOUs/MOAs/SOFs)?<br>• Incident response plans include measures for off-installation personnel (personnel warning system)? |
| 16, 23 | **Rules of Engagement (ROE)/Rules of Force (RUF):**<br>• Does unit have correct ROE/RUF guidance for the mission and environment?<br>• Do plan/current procedures provide enough "stand-off" to determine hostile intent and make proper decision to use force?<br>• Are troops trained for making ROE/RUF decisions in realistic situations?<br>• ROE/threat scenarios adequate & rigorous? |

| DoD Std | AT METRIC |
|---|---|
| | • Is unit prepared to apply ROE/RUF for threat scenarios? |

AP1.1.2. Questions for facilities ATOs.

**Table AP1.T2. Antiterrorism Checklist – ATOs**

| DoD Std | AT METRIC |
|---|---|
| 1 | **DoD AT Policy**: This standard does not apply. |
| 2 | **Development of AT Standards**<br>- Do you have a copy of the applicable DoD, Combatant Commander, Service, and Agency AT regulations, standards, and other guidance?<br>- Combatant Commander/Service and/or DoD Agency Standards should address:<br>- Procedures to collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks.<br>- Terrorism threat assessment, Vulnerability Assessment, Terrorism Incident Response Measures, and Terrorist Consequence Management measures.<br>- AT Plans and procedures to enhance AT protection.<br>- Procedures to identify AT requirements and to program for resources necessary to meet security requirements.<br>- DoD Military AT constructions considerations. |
| 3 | **Assignment of AT Operational Responsibility**<br>❑ Does facility understand which Combatant Commander, Service or DoD Agency has AT Tactical Control (TACON) for operational responsibility? |
| 4 | **AT Coordination in Overseas Locations**: This standard does not apply to facility AT Plans. |
| 5 | **Comprehensive AT Development, Implementation, and Assessment**<br>❑ Does the installation AT Program contain, as a minimum, the following elements:<br>• Threat Assessments (Standard 15).<br>• Planning (Standards 14-20)<br>• Exercises (Standard 19)<br>• Program Review (Standard 20)<br>• Training (Standards 19, 21-25)<br>• Vulnerability Assessments (Standards 26-27) |
| 6 | **Antiterrorism Officers (ATO) Assigned in Writing**<br>❑ Has the commander designated a Level II qualified/trained commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO?<br>❑ For deploying organizations (e.g. battalion, squadron, ship) have at least one Level II qualified individual designated in writing?<br>❑ Has the ATO attended a Service approved Level II AT Training course? |
| 7 | **Application of Department of Defense Terrorism Threat Analysis Methodology**<br>❑ Does the unit use the DoD threat level methodology (*Low, Moderate, Significant, High*) in their local threat assessments? |
| 8 | **Threat Information Collection and Analysis**<br>❑ Has the commander tasked the appropriate organization under their command to gather, analyze, and disseminate terrorism threat information?<br>❑ Are personnel in the command encouraged and trained to report information on individuals, events, or situations that could pose a threat to the security of DoD personnel, families, facilities, and resources?<br>❑ Does the command have procedures to receive and process Defense Terrorism Warning Reports and/or higher headquarters threat message? |
| 9 | **Threat Information Flow** |

| DoD Std | AT METRIC |
|---|---|
| | ❑ Does the command forward all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD personnel or assets for which they have AT responsibility up and down the chain of command?<br>❑ Does the command ensure there is intelligence sharing between all organizations?<br>❑ Does the command provide tailored threat information for transiting units? |
| 10 | **Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD)**<br>❑ Does the command have the procedures to process immediately through the chain of command reports of significant information obtained identifying organizations with WMD capability in their AOR?<br>❑ Is an estimate of terrorist potential use of WMD indicated in the local threat assessment? |
| 11 | **Adjustment of Force Protection Conditions**<br>❑ Does the command have a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower FPCONs? |
| 12 | **FPCON Measures Implementation:** This standard does not apply to facility AT Plans. |
| 13 | **FPCON Measures**<br>❑ Has the command developed site-specific measures or actions for each FPCON which supplement measures/actions enumerated for each FPCON as listed within Appendix A of DoD 2000.12-H (reference (b)?<br>❑ Does the command have procedures to set and transition between FPCONs?<br>❑ Does the command have procedures to establish a LOWER FPCON than Higher Headquarters?<br>❑ Are site-specific AT measures, linked to FPCONs classified as a minimum, CONFIDENTIAL?<br>❑ Site-specific AT measures separated from the AT plan can remain FOR OFFICIAL USE ONLY.<br>❑ Do FPCONs permit sufficient time and space to determine hostile intent IAW standing ROE? |
| 14 | **Comprehensive AT plan**<br>❑ Does the command have a signed AT Plan?<br>❑ Is the plan site-specific and address the following key elements?<br>• Terrorism Threat Assessment (including WMD).<br>• Vulnerability Assessment (see Standard 26).<br>• Risk Assessment<br>• AT Physical Security measures.<br>• Terrorism Incident Response measures.<br>• Terrorism Consequence Management measures.<br>• Does the installation incorporate AT planning into operations orders for temporary operations or exercises? |
| 15 | **Terrorism Threat Assessment**<br>❑ Does the command have an annually updated terrorism threat assessment?<br>❑ Does the threat assessment consider the following during the assessment process:<br>• Capabilities of the terrorist threat.<br>• Vulnerability of the facilities.<br>• Criticality of the facilities.<br>❑ Is the threat assessment used as the basis and justification for recommendations on AT enhancements, program/budget requests and establishment of FPCONs?<br>❑ Does the command use a risk assessment to integrate threat and vulnerability assessment information in order to make an informed decision to commit resources and/or enact policies and procedures to mitigate the threat or define the risk?<br>❑ Does the risk assessment analyze the following elements?<br>• Terrorist Threat.<br>• Criticality of the Assets.<br>• Vulnerability of facilities, programs, and systems to terrorist threats.<br>• The ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident. |

| DoD Std | AT METRIC |
|---|---|
| 16 | **AT Physical Security Measures**<br>❑ Does the Installation Commander coordinate and integrate subordinate unit physical security plans and measures into the AT plan?<br>❑ Are physical security measures considered, do they support, and are they referenced in the AT plan to ensure an integrated approach to terrorist threats?<br>❑ Do AT physical security measures include provisions for the use of:<br>• Physical Structures.<br>• Physical Security Equipment.<br>• Chemical, Biological, Radiological detection & protection equipment.<br>• Security Procedures.<br>• Random Antiterrorism Measures (RAM)<br>• Response Forces<br>• Emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to terrorist attack.<br>❑ Are RAMs used for both in-place and transiting forces? |
| 17 | **Terrorist Incident Response Measures (first response)**<br>❑ Has the command prepared installation-wide and/or shipboard terrorist incident response measures which include:<br>• Procedures for determining the nature and scope of the terrorist incident and required response.<br>• Procedures for coordinating security, fire, and medical First Responders.<br>• Steps to reconstitute the installation's ability to perform AT measures<br>• In Moderate, Significant, or High terrorist threat level areas, has the command included residential location information for all DoD personnel and their dependents in their Incident Response Measures? |
| 18 | **Terrorist Consequence Management Measures**<br>❑ Do CM measures provide for appropriate emergency response and disaster planning and/or preparedness to respond to a terrorist attack for the installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support?<br>❑ Do CM measures include guidelines for pre-deployment and garrison operations, pre-attack procedures, actions during attack, and post-attack actions? |
| 19 | **Training and Exercises**<br>❑ Has the command conducted field and staff training (annually) to exercise AT plans to include?<br>• AT Physical Security measures.<br>• Terrorist Incident Response measures.<br>• Terrorist Consequence Management measures.<br>❑ Does the command maintain exercise AARs/Lessons Learned and document actions taken to remediate identified shortfalls for at least a year?<br>❑ Does command pre-deployment training include?<br>• Credible deterrence/response.<br>• Deterrence-specific tactics, techniques, and procedures.<br>• Terrorist scenarios and hostile intent decision-making. |
| 20 | **Comprehensive AT Review**<br>❑ Does the command review own and subordinate AT programs and plans at least annually to facilitate AT program enhancement?<br>❑ Does the command review the AT program when the terrorist threat level changes? |
| 21 | **General Requirements for AT Training**<br>❑ Does the command ensure all personnel records are updated to reflect AT training IAW DoD Component policy? |
| 22 | **Level I AT Awareness Training** |

| DoD Std | AT METRIC |
|---|---|
| | ❑ Does the command conduct Level I training IAW DoD and Combatant Commander/Service/Agency standards?<br>❑ Does the installation ensure Military Service family members traveling beyond CONUS on official business receive Level I training (i.e., PCS move)? |
| 23 | **AOR-Specific Training Requirements for all Department of Defense Personnel**<br>❑ Does the command ensure all individuals traveling outside CONUS for either permanent or temporary duty complete Level I AT Awareness Training?<br>❑ Has he command provided Combatant Commander approved AOR specific AT protection information to individuals traveling outside CONUS within three months prior to travel?<br>❑ Does the command ensure intra- theater transiting units receive detailed threat information covering travel routes and sites that will be visited by the unit? |
| 24 | **Level II Antiterrorism Officer (ATO) Training**<br>❑ Does the installation and/or each deployed unit have at least one Level II trained ATO assigned?<br>❑ Have 0-5/0-6 commanders received Level III training prior to assumption of command? |
| 25 | **Training for High-Risk Personnel and High-Risk Billets**<br>❑ Has the command identified high-risk billets and high-risk personnel to higher headquarters annually?<br>❑ Have personnel designated as " Personnel at High-Risk to Terrorist Attack" and "Personnel Assigned to High-Risk Billets" received appropriate AT training? |
| 26 | **Vulnerability Assessments of Installations**<br>❑ Has a local vulnerability assessment been conducted within the past year?<br>❑ Did the vulnerability assessment identify vulnerabilities and means to eliminate or mitigation them?<br>❑ Did the vulnerability assessment identify options for enhanced protection of DoD personnel and assets?<br>❑ Does the AT vulnerability assessment assess the following functional areas at a minimum:<br>• AT Plans and Programs.<br>• Counterintelligence, Law Enforcement, Liaison, and Intelligence Support.<br>• AT Physical Security Measures.<br>• Vulnerability to a Threat and Terrorist Incident Response Measures.<br>• Vulnerability Assessment for Terrorist Use of WMD.<br>• Availability of resources to support plans as written.<br>• Frequency and extent to which plans have been exercised.<br>• Level and adequacy of support from the host nation, local community, and where appropriate, inter-Service and tenant organizations to enhance force protection measures or respond to a terrorist incident.<br>• Status of formal and informal agreements to support AT functions.<br>• Does the vulnerability assessment team contain expertise in order to meet the intent of providing comprehensive assessments?<br>❑ Is there a process to track and identify vulnerabilities through the chain of command? |
| 27 | **Pre-Deployment AT Vulnerability Assessment**<br>❑ Has a pre-deployment AT vulnerability assessment been conducted for units prior to deployment?<br>❑ Have appropriate AT measures been implemented to reduce risk and vulnerability?<br>❑ Has the command received onboard and/or advance-site assessments prior to and during visits to higher-threat areas of Significant or High Threat Levels or where a geographically specific Terrorism Threat Warning Report is in effect?<br>❑ Has the command requested funds from CbT RIF for emergent AT requirements prior to movement of forces?<br>❑ Has the command explored the use of Commercial-off-the-shelf or Government-off-the-shelf products to meet near-term AT protection requirements? |
| 28 | **Construction Considerations**<br>❑ Do DoD Components adopt and adhere to common criteria and minimum construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate AT vulnerabilities and terrorist attacks? |
| 29 | **Facility and Site Evaluation and/or Selection Criteria** |

| DoD Std | AT METRIC |
|---|---|
| | ❑ Has the command developed a prioritized list of AT factors for site selection for facilities, either currently occupied or under consideration for occupancy by DoD personnel? AT factors should include, but not limited to, screening from direct fire weapons, building separation, perimeter standoff, window treatments, protection of entrances and exits, parking lots and roadways, standoff zone delineation, security lighting, external storage areas, mechanical and utility systems.<br>❑ Has the command used these factors to determine if facilities can adequately protect occupants against terrorism attack? |
| 30 | **AT Guidance for Off-Installation Housing**<br>❑ Does the command have procedures to ensure DoD personnel assigned to Moderate, Significant, and High Terrorism Threat Level areas, who are not provided on-installation or other Government quarters, are furnished guidance on the selection of private residence to mitigate risk of terrorist attack?<br>❑ Does the command have procedures to conduct physical security reviews of off-installation residences for permanently and temporary-duty DoD personnel in Significant or High Threat Level areas?<br>❑ Based on these physical security reviews, does the command have procedures to provide AT recommendations to residents and facility owners?<br>❑ As appropriate, does the command have procedures to recommend to appropriate authorities the construction or lease of housing on an installation or safer area?<br>❑ Does the command have procedures to complete residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing in Significant or High Threat areas?<br>❑ Does the command have procedures to include coverage of private residential housing in AT plans where private residential housing must be used in Moderate, Significant, or High Threat Level areas?<br>❑ In Moderate, Significant, or High Threat areas, does the command incorporate family members and dependent vulnerabilities into antiterrorism assessment, mitigation, and reporting tools for:<br>• Facilities used by DoD employees and their dependents.<br>• Transportation services and routes used by DoD employees and their dependents. |
| 31 | **Executive Protection and High Risk Personnel Security**<br>❑ Has the command annually reviewed and revalidated the protective services for executives?<br>❑ Has the command taken necessary measures to provide appropriate protective services for designated individuals in high-risk billets and high-risk personnel?<br>❑ Does the command review needs for supplemental security within 30 days of a change in the Terrorism Threat Level? |
| | **Miscellaneous Issues**<br>❑ Does the command have technology to access critical terrorism intelligence e.g., SIPRNET?<br>❑ Has the 0-6 through 0-8 commander been to Level IV training? |

# AP2. APPENDIX 2
# SUGGESTED VA METHODOLOGIES

## AP2.1. INTRODUCTION

Facility Commanders are encouraged to use a RA tool that is simple yet has some quantifiable logic to help in decision making. Assessment teams shall use the methodology to determine terrorist options against specific targets and use them as examples of protection strategies discussed in this Handbook. The suggested tools offered below have their strengths and their weaknesses -- as with all tools, there is a right tool for the job at hand. As an example, CARVER is not specifically tailored for AT assessments, although it can be used. Likewise, MSHARPP is a targeting analysis tool geared more closely to assessing personnel vulnerabilities. Assessment team members should be cognizant of potential gaps when choosing one methodology over another. The use of the Joint Staff CVAMP shall assist commanders and ATOs in managing their command's vulnerabilities and associated funding requirements.

## AP2.2. MSHARPP.

AP2.2.1. The purpose of the MSHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., "attractiveness" to enemy, potential psychological effect on community, etc.) of potential targets. This document provides an example of how to use MSHARPP.

AP2.2.2. After developing a list of potential targets, use the MSHARPP selection factors to assist in further refining your assessment by associating a weapon/tactic to a potential target to determine the efficiency, effectiveness and plausibility of the method of attack and to identify vulnerabilities related to the target. After the MSHARPP values for each target or component are assigned, the sum of the values indicate the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

AP2.2.3. Mission. Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation's mission.

AP2.2.3.1. When assessing points in this area, determine whether or not an attack on mission components shall cause degradation by assessing the Component's:

AP2.2.3.1.1. Importance. Importance measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

AP2.2.3.1.2. Effect. Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

AP2.2.3.1.3. Recuperability. Recuperability measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

AP2.2.3.2. Mission Criteria Scale. Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist.

AP2.2.3.2.1. ONE. Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

AP2.2.3.2.2. TWO. The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

AP2.2.3.2.3. THREE. Half of the mission capability remains if the asset were successfully attacked.

AP2.2.3.2.4. FOUR. Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

AP2.2.3.2.5. FIVE. Installation cannot continue to carry out its mission until the attacked asset is restored.

AP2.2.4. Symbolism. Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of U.S. military, Christianity, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy.

AP2.2.4.1. Symbolism criteria scale.

AP2.2.4.1.1. High profile, direct symbol of target group or ideology, asset is perceived to be vital to the mission of the installation.

AP2.2.4.1.2. Low profile, direct symbol of target group or ideology.

AP2.2.4.1.3. Low profile and/or obscure symbol of target group or ideology.

AP2.2.5. History. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities.

AP2.2.5.1. Symbolism criteria scale.

AP2.2.5.1.1. Strong history of attacking this type of target.

AP2.2.5.1.2. History of attacking this type of target, but none in the immediate past.

AP2.2.5.1.3. Little to no history of attacking this type of target.

AP2.2.6. Accessibility. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an extended period.

AP2.2.6.1. The four basic stages to consider, when assessing accessibility are:

AP2.2.6.1.1. Infiltration from the staging base to the target area.

AP2.2.6.1.2. Movement from the point of entry to the target or objective.

AP2.2.6.1.3. Movement to the target's critical element.

AP2.2.6.1.4. Exfiltration.

AP2.2.6.2. Accessibility criteria scale.

AP2.2.6.2.1. Easily accessible, standoff weapons can be employed.

AP2.2.6.2.2. Inside Perimeter fence, climbing or lowering required.

AP2.2.6.2.3. Not accessible or inaccessible without extreme difficulty.

AP2.2.7. Recognizability. A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (yours and the enemy's). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy.

AP2.2.7.1. Recognizability criteria scale.

AP2.2.7.1.1. Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition.

AP2.2.7.1.2. Target is easily recognizable at small-arms range and requires a small amount of training for recognition.

AP2.2.7.1.3. Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition.

AP2.2.7.1.4. Target cannot be recognized under any conditions—except by experts.

AP2.2.8. Population. Population addressed two factors, quantity of personnel and their demography. Demography asks the question "who are the targets?" Depending on the ideology of the terrorist group (s), being a member of a particular demographic group can make someone (or some group) a more likely target.

AP2.2.8.1. When assessing points in this area, determine whether or not the group (s) have a history of, or are predicted to target:

AP2.2.8.1.1. Military personnel.

AP2.2.8.1.2. Family members (U.S. citizens in general).

AP2.2.8.1.3. Civilian employees of the U.S. Government (include local nationals).

AP2.2.8.1.4. Senior officers or other high-risk personnel.

AP2.2.8.1.5. Member of an ethnicity (racial, religious, or regionally defined).

AP2.2.8.2. Quantity addresses the number of people that would become victims if a particular target were attacked. Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

AP2.2.8.3. Population criteria scale.

AP2.2.8.3.1. Densely populated; prone to frequent crowds, facility routinely contains substantial numbers of personnel known to be targeted by the enemy and/or the population is comprised of personnel deemed vital to the accomplishment of the installation's mission.

AP2.2.8.3.2. Relatively large numbers of people, but not in close proximity (i.e., spread out and hard to reach in a single attack), contains known target group, but rarely in large concentrations, population has no special segment necessary for mission accomplishment.

AP2.2.8.3.3. Sparsely populated; prone to having small groups or individuals, little target value based on demographics of occupants

AP2.2.9. Proximity. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (e.g., near national monuments, protected/religious symbols, etc., that the enemy holds in high regard).

AP2.2.9.1. It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack; a "target-rich" environment may increase the chances of attack.

AP2.2.9.2. Proximity criteria scale.

AP2.2.9.2.1. Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.

AP2.2.9.2.2. Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.

AP2.2.9.2.3. Target is in close proximity; serious injury/ damage or death/total destruction of protected personnel/facilities likely.

AP2.2.10. Figure AP2F1 is an example MSHARPP worksheet. Values from 1 to 5 are assigned to each factor based on the associated data for each target. Five represents the highest vulnerability or likelihood of attack and 1 the lowest. Accordingly, the higher the total score, the more vulnerable the target. Because this analysis is highly subjective, some analysts prefer simple "stoplight" charts with red, yellow and green markers representing descending degrees of vulnerability. The MSHARPP analysis must consider both the present force protection posture and enhanced postures proposed for escalating FPCONs. Specific target vulnerabilities must be combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not deemed exploitable an otherwise vulnerable building becomes a less likely target.

**Figure AP2.F1. Example MSHARPP matrix.**

| TARGET | M | S | H | A | R | P | P | TOTAL | WEAPON |
|---|---|---|---|---|---|---|---|---|---|
| HQ BLDG | 5 | 4 | 5 | 1 | 3 | 4 | 1 | 23 | 4,000 Truck IED |
| Barracks B | 2 | 4 | 5 | 4 | 4 | 4 | 2 | 25 | 220 lb Car IED |
| Comm Center | 5 | 4 | 2 | 3 | 5 | 3 | 1 | 23 | 4,000 Truck IED |
| SF Ops Center | 3 | 3 | 2 | 4 | 4 | 4 | 2 | 22 | 7.62 (Sniper) |
| Fuel Storage | 4 | 3 | 1 | 5 | 5 | 1 | 3 | 22 | 50 lb Satchel Charge |
| Hanger A | 5 | 5 | 3 | 2 | 5 | 5 | 4 | 29 | Mortar |
| Wpns Storage | 5 | 5 | 1 | 1 | 5 | 3 | 1 | 21 | RPG |
| Elec Transformer | 5 | 2 | 3 | 5 | 5 | 0 | 4 | 24 | Grenade |

AP2.3. CARVER.

AP2.3.1. The CARVER matrix is used by Special Forces and commandos to target enemy infrastructure including public works facilities such as bridges and power plants. It is believed that our enemies – overt and covert – employ a similar method to target our facilities. They all, though, seek soft, unprotected targets.

AP2.3.2. CARVER is a very useful tool for determining that your critical assets might indeed offer an enemy a good or soft target. If you employ the very same CARVER analysis to every asset, it shall yield a good estimate as to the attractiveness of those assets to an enemy. Specifically Commanders shall then know which "targets" require hardening or otherwise increased protection.

AP2.3.3. CARVER is an acronym, with each letter representing the following:

AP2.3.3.1. Criticality. The importance of a system, subsystem, complex, or component. A target is critical when its destruction or damage has a significant impact on the output of the targeted system, subsystem, or complex, and at the highest level, on the unit's ability to make war or perform essential functions. Criticality depends on several factors:

AP2.3.3.1.1. How rapidly shall the impact of asset destruction affect the unit's essential functions.

AP2.3.3.1.2. What percentage of output and essential functions is curtailed by asset damage.

AP2.3.3.1.3. Is there an existence of substitutes for the output product or service

AP2.3.3.1.4. What is the number of assets and their position in the system or complex flow diagram

AP2.3.3.1.5. Criticality asks the question: How critical is the facility to your mission accomplishment?

AP2.3.3.2. Accessibility. The ease that an asset can be reached, either physically or by standoff weapons. An asset is accessible when a terrorist element can physically infiltrate the asset, or the asset can be hit by direct or indirect fire. As a reminder, assets can be people, places, or things. The use of standoff weapons should always be considered when evaluating accessibility. Survivability of the attacker is usually most related to a target's accessibility. Accessibility asks the question: How easily can an enemy get access to, or have their weapons reach the asset?

AP2.3.3.3. Recuperability. A measure of time required to replace, repair or bypass, the destruction or damage inflicted on the target. Recuperability varies with the sources and ages of targeted components and with the availability of spare parts. The existence of economic embargoes and the technical resources of the installation shall influence recuperability. Recuperability asks the question: How long would it take you to repair or replace the asset?

AP2.3.3.4. Vulnerability. A measure of the ability of the terrorist to damage the target using available assets (people and material). A target (asset) is vulnerable if the terrorist has the means and expertise to successfully attack it. Vulnerability depends on:

AP2.3.3.4.1. The nature of the construction of the target.

AP2.3.3.4.2. The assets available (manpower, transportation, weapons, explosives, and equipment) to defend the facility.

AP2.3.3.4.3. Vulnerability asks the question: Is the asset literally hardened or guarded? Are measures in place to mitigate any threat?

AP2.3.3.5. Effect on the population. The positive or negative influence on the population as a result of the action taken. Effect considers public relation in the vicinity of the target, but also considers the domestic and international reaction as well. Shall reprisals against friendlies result? Shall national PSYOP themes be contradicted or reinforced? Shall exfiltration and evasion be helped or hurt? Shall the enemy population be alienated from its government, or shall it become supportive of the government. Effect is often neutral at the tactical level. Effect

asks the question: What is the effect on the local population, be it terror or demoralization, and associated mission degradation?

AP2.3.3.6. Recognizability. The degree that a target can be recognized under varying weather, light, and seasonal conditions without confusion with other targets or components.

AP2.3.3.6.1. Factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, and the technical sophistication and training of the terrorists.

AP2.3.3.6.2. Recognizability asks the question: Can the enemy recognize the target for what it truly is and its importance?

AP2.3.4. Target selection requires detailed intelligence and thorough planning, and is based on the CARVER factors identified above. The CARVER Matrix, as shown in Table AP2.T1, is a decision tool for rating the relative desirability of potential targets and for wisely allocating attack resources. Two rules of thumb apply for completing the matrix:

AP2.3.4.1. For strategic level analysis, list systems and subsystems.

AP2.3.4.2. For tactical level analysis list complexes or components of subsystems and complexes. Keep in mind that the scale can be adjusted, such as one to ten or 10 to 100, provided that consistency is observed.

**Table AP2.T1. Example CARVER Matrix.**

| Potential Targets | C | A | R | V | E | R | TOTAL |
|---|---|---|---|---|---|---|---|
| Commissary | 5 | 7 | 10 | 7 | 8 | 10 | 47 |

CARVER CRITERIA

| Criticality: | Rating |
|---|---|
| Immediate Output halt or 100% curtailment | 10 |
| Output halt less than one day or 75% curtailment | 6 |
| Output halt less than one week or 50% curtailment | 4 |
| Output halt in over one week and less than 25% curtailment | 1 |
| Accessibility: | |
| Standoff weapons can be deployed | 10 |
| Inside perimeter fence, but outdoors | 8 |
| Inside of a building, but ground floor | 6 |
| Inside of a building, but second floor | 4 |
| Inside of a building, climbing required | 1 |
| Recuperability: | |
| 1 month or more | 10 |
| Up to 1 month | 8 |
| Up to 1 week | 6 |
| Up to 1 day | 4 |
| 4 hours or less | 1 |

| | |
|---|---|
| Vulnerability: | |
| To small arms fire or charges 5 pounds or less | 10 |
| To anti-tank weapons or charges of 5 to 10 pounds | 7 |
| To charges of 10 to 30 pounds | 5 |
| To charges of 30 to 50 pounds | 3 |
| More drastic measures must be employed. | 1 |
| Effect on the Population: | |
| National PSYOP objectives fostered; no reprisals against friendlies likely. | 10 |
| No effect, or neutral | 5 |
| Very negative public reaction, reprisals against friendlies likely, or high domestic uprising potential. | 1 |
| Note: On the tactical level, effect on population is often neutral. That is, the effect is the same for all components within a complex. There are conspicuous exceptions, such as reactor components in nuclear sites. If all components within a complex are neutral, the entire "E" column can be removed from the matrix. | |
| Recognizability: | |
| The complex or component is recognizable day or night, rain or shine, without confusion with other complexes or components. | 10 |
| The complex or component may be difficult to recognize at night or in bad weather or might be confused with other complexes and components. | 5 |
| The complex or component is difficult to recognize under any condition and is easily confused with other complexes and components. | 1 |

AP2.3.5. After completing the matrix for all assets, total the scores in the right hand column and then rank order those totals to prioritize vulnerabilities.

AP2.3.6. The following are basic mitigation tips to address four of the six CARVER Components.

AP2.3.6.1. Reduce criticality. As practicable have a back-up device, system or tested plan to afford mission accomplishment without the asset; create redundancy either physically or operationally; have a tested and viable Continuity Of Operations Plan; and have a fall-back site for conducting the same mission from another location.

AP2.3.6.2. Reduce accessibility. Reduce access both, physical and cyber, as applicable; use barriers, other barricades, carefully controlled pedestrian and vehicle movement and/or access and parking; and use fences, remote motion sensors, and remote video surveillance.

AP2.3.6.3. Reduce vulnerability. Harden the structure and/or immediate environment to include window treatment to prevent glass shards, structural reinforcement, and shatterproof and fireproof building materials. Move vehicle parking and access sufficiently away from personnel-massing facilities.

AP2.3.6.4. Reduce recognizability. Delete location and purpose of facility from all base maps and remove building signs that describe function or give title of unit in facility. Instruct telephone operators to not give out number or existence of facility. Use plant cover, including trees and bushes, to partially conceal facility, particularly from roads.

AP2.3. CORE VULNERABILITY ASSESSMENT MANAGEMENT PROGRAM.

AP2.3.1. CVAMP is an automated and web-based means of managing a command's vulnerabilities and associated funding requirements. CVAMP key capabilities include:

AP2.3.1.1. Provide a means to database vulnerability assessment findings in accordance with reference (e), for both higher headquarters and local assessments.

AP2.3.1.2 . Provide capability of receiving observations directly from the JSIVA Information System.

AP2.3.1.3 . Document a commander's risk assessment decision for each vulnerability.

AP2.3.1.4 . Track the status of known vulnerabilities until mitigated.

AP2.3.1.5 . Provide a tool to assist in prioritizing vulnerabilities via a weighted scale based on user input.

AP2.3.1.6 . Provide commanders a vehicle to identify requirements to the responsible chain of command.

AP2.3.1.7 . Provide the ability to roll vulnerability data into a resource requirement. This includes UFR submissions as well as emergent and emergency CbT RIF requests. Use of CVAMP is mandatory for submission to the Joint Staff of CbT RIF requests.

AP2.3.1.8 . Provide ability to control release of vulnerabilities and associated funding requests through the chain of command – access is limited to a "need to know" basis as determined by system administrators at each command level.

AP2.3.1.9 . Allow for prioritization of emergent CbT RIF requests and UFRs as well as provide a tool to assist in this process based on user input.

AP2.3.1.10. Provides a ready reference to track the status of installations and activities by FPCON and/or Terrorism Threat Level.

AP2.3.2. Registration for CVAMP is embedded within the Joint Staff's Antiterrorism Enterprise Portal (ATEP) via the SIPRNET. Once registered on ATEP, system administrators identified at each level of command shall assign CVAMP roles and functions to users based on their needs/requirements. To allow for flexibility, administrators can assign multiple roles to a user. Each role sets specific user permissions within the system. Besides SIPRNET access, minimal additional equipment or training is required to use CVAMP. The system operates in a user-friendly format with drop down menus and no complex computer skills are required to create, review, modify or manage the program. Initial CVAMP-related roles and their permissions are:

AP2.3.2.1. Commander. Capability to read and/or write with comment and retains sole release authority to higher headquarters on all vulnerability assessments, vulnerabilities, and funding requests.

AP2.3.2.2. ATO. Capability to create vulnerability assessments, vulnerabilities and funding requests.

AP2.3.2.3. Resource Manager. Capability to read and/or write to all funding requests.

AP2.3.2.4. Assessor. Capability to create observations associated with a vulnerability assessment.

AP2.3.2.5. System Administrator. Capability to assign and manage roles within immediate organization and one level down.

AP2.3.2.6. Users should contact their local/and or next higher headquarters CVAMP administrators to establish their roles within CVAMP.

# AP3. APPENDIX 3
# DoD FPCON SYSTEM

## AP3.1 Basic FPCON Procedures

### AP3.1.1. General

AP3.1.1.1. The FPCONs outlined below describe the progressive level of countermeasures in response to a terrorist threat to U.S. military facilities and personnel as directed by reference (a). These security measures are approved by the Joint Chiefs of Staff and are designed to facilitate inter-Service coordination and support of U.S. Military antiterrorism activities. When installations adapt these measures for their site-specific circumstances, they should account for, as a minimum, Combatant Commander/Service requirements, local laws, and SOFA. Per reference (e), FPCONs measures are FOR OFFICIAL USE ONLY. An AT Plan with a complete listing of site-specific AT measures, linked to a FPCON, shall be classified, as a minimum, CONFIDENTIAL. When separated from the AT Plan, specific measures and FPCON measures remain FOR OFFICIAL USE ONLY.

AP3.1.1.2. Once a FPCON is declared, all listed security measures are implemented immediately unless waived by competent authority as described in Chapter 10. The declared FPCON should also be supplemented by a system of RAMs in order to complicate a terrorist group's operational planning and targeting.

AP3.1.1.2.1. Airfield specific measures are for installations and facilities with a permanently functioning airfield. Installations and facilities with an emergency helicopter pad should review and implement any applicable airfield specific measures when they anticipate air operations.

AP3.1.1.2.2. Due to their specific security requirements, DoD ship's measures are listed separately in section AP3.2. Those measures applying solely to USN combatant ships are further identified throughout the paragraph. Shipboard guidelines are specially tailored to assist commanding officers and ship masters in reducing the effect of terrorist and other security threats to DoD combatant and non-combatant vessels, to include U.S. Army and Military Sealift ships worldwide. They provide direction to maximize security for the ship based on current threat conditions consistent with performance of assigned missions and routine functions.

AP3.1.1.3. Specific countermeasures were determined taking into consideration the following factors:

AP3.1.1.3.1. Ability to maintain highest state of operational readiness.

AP3.1.1.3.2. Measures to improve physical security through the use of duty and guard force personnel limit access to the exposed perimeter areas and interior of the unit/facility by hostile persons, and barriers to physically protect the unit/facility.

AP3.1.1.3.3. Availability of effective command, control, and communication systems with emphasis on supporting duty/watch officers, security forces, and key personnel.

AP3.1.1.3.4. An AT awareness program for all personnel.

AP3.1.1.3.5. Protection of high-risk assets and personnel.

AP3.1.1.3.6. Measures necessary to limit activities, and visitor/social engagements.

AP3.1.1.4. FPCON NORMAL and all FPCON levels should include site specific measures a facility commander deems necessary when establishing a baseline posture.

AP3.1.2. FPCON NORMAL

AP3.1.2.1. Measure NORMAL 1. Secure and randomly inspect buildings, rooms, and storage areas not in regular use.

AP3.1.2.2. Measure NORMAL 2. Conduct random security spot checks of vehicles and persons entering facilities under the jurisdiction of the United States.

AP3.1.2.3. Measure NORMAL 3. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

AP3.1.3. FPCON ALPHA Measures.

AP3.1.3.1. Measure ALPHA 1. Continue, or introduce, all measures in previous FPCON.

AP3.1.3.2. Measure ALPHA 2. At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.

AP3.1.3.3. Measure ALPHA 3. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

AP3.1.3.4. Measure ALPHA 4. Increase security spot checks of vehicles and persons entering installations under the jurisdiction of the United States.

AP3.1.3.5. Measure ALPHA 5. Initiate food and water Operational Risk Management (ORM) procedures, brief personnel on food and water security procedures, and report any unusual activities.

AP3.1.3.6. Measure ALPHA 6. Test mass notification system.

AP3.1.3.7. Measure ALPHA 7. Review all plans, identify resource requirements, and be prepared to implement higher FPCONs.

AP3.1.3.8. Measure ALPHA 8. Review and, if necessary, implement security measures for high-risk personnel.

AP3.1.3.9. Measure ALPHA 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

AP3.1.3.10. Measure ALPHA 10. Review intelligence, counter intelligence, and operations dissemination procedures.

AP3.1.4. FPCON BRAVO Measures.

AP3.1.4.1. Measure BRAVO 1. Continue, or introduce, all measures in previous FPCONs.

AP3.1.4.2. Measure BRAVO 2. Enforce control of entry onto U.S. infrastructure critical to mission accomplishment, lucrative targets, and high profile locations; and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large IED (cargo vans, delivery vehicles) sufficient to cause catastrophic damage or loss of life.

AP3.1.4.3. Measure BRAVO 3. Identify critical and high occupancy buildings. Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality; the protection level provided by structure, IED/Vehicle Borne IED threat; and available security measures. Consider centralized parking.

AP3.1.4.4. Measure BRAVO 4. Secure and inspect all buildings, rooms, and storage areas not in regular use.

AP3.1.4.5. Measure BRAVO 5. At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

AP3.1.4.6. Measure BRAVO 6. Implement mail-screening procedures to identify suspicious letters and parcels.

AP3.1.4.7. Measure BRAVO 7. Randomly inspect commercial deliveries. Advise family members to check home deliveries.

AP3.1.4.8. Measure BRAVO 8. Randomly inspect food and water for evidence of tampering/contamination before use by DoD personnel. Inspections should include delivery vehicles and storage area/containers.

AP3.1.4.9. Measure BRAVO 9. Increase security/guard presence or patrol/surveillance of DoD housing areas, schools, messes, on-base clubs, and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

AP3.1.4.10. Measure BRAVO 10. Implement plans to enhance off-installation security of DoD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and family members.

AP3.1.4.11. Measure BRAVO 11. Inform local security committees of actions being taken.

AP3.1.4.12. Measure BRAVO 12. Verify identity of visitors and randomly inspect their suitcases, parcels, and other containers.

AP3.1.4.13. Measure BRAVO 13. Conduct random patrols to check vehicles, people, and buildings.

AP3.1.4.14. Measure BRAVO 14. As necessary, implement additional security measures for high-risk personnel.

AP3.1.4.15. Measure BRAVO 15. Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

AP3.1.4.16. Measure BRAVO 16. Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

AP3.1.4.17. Measure BRAVO 17. As deemed appropriate, verify identity of personnel entering buildings.

AP3.1.4.18. Measure BRAVO 18. Review status and adjust as appropriate OPSEC, COMSEC, and INFOSEC procedures.

AP3.1.4.19. Measure BRAVO 19. (airfield specific) As appropriate, erect barriers and man and establish checkpoints at entrances to airfields. Ensure identity of all individuals entering the airfield (flightline and support facilities) -- no exceptions. Randomly inspect vehicles, briefcases and packages entering the airfield.

AP3.1.4.20. Measure BRAVO 20. (airfield specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate threat of surface-to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

AP3.1.5. FPCON CHARLIE Measures.

AP3.1.5.1. Measure CHARLIE 1. Continue, or introduce, all measures in previous FPCON.

AP3.1.5.2. Measure CHARLIE 2. Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and SOFAs. Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapons capabilities.

AP3.1.5.3. Measure CHARLIE 3. Be prepared to react to requests for assistance, from both local authorities and other installations in the region.

AP3.1.5.4. Measure CHARLIE 4. Limit access points to strictly enforce entry. Randomly search vehicles.

AP3.1.5.5. Measure CHARLIE 5. Ensure or verify identity of all individuals entering food and water storage and distribution centers, use sign in/out logs at access control/entry points, and limit and/or inspect all personal items.

AP3.1.5.6. Measure CHARLIE 6. Initiate contingency monitoring for biological and chemical agents as required. Suspend contractors/off-facility users from tapping into facility water system (alternate locally developed measure should be executed when contractors are

responsible for DoD water supplies or when water is provided by local (non-DoD) sources or agencies).

AP3.1.5.7. Measure CHARLIE 7. Increase standoff from sensitive buildings based on threat. Implement barrier plan to hinder vehicle borne attack.

AP3.1.5.8. Measure CHARLIE 8. Increase patrolling of the facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions/persons outside the facility perimeter. For airfields, patrol or provide observation of approach and departure flight corridors as appropriate to the threat (coordinate with TSA, Marine Patrol, U.S.C.G., and local law enforcement as required to cover off-facility approach and departure flight corridors).

AP3.1.5.9. Measure CHARLIE 9. Protect all designated infrastructure critical to mission accomplishment. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

AP3.1.5.1.10. Measure CHARLIE 10. To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

AP3.1.5.11. Measure CHARLIE 11. Consider searching suitcases, briefcases, packages, etc., being brought onto the installation through access control points and consider randomly searching suitcases, briefcases, packages, etc., leaving.

AP3.1.5.12. Measure CHARLIE 12. Review personnel policy procedures to determine course of action for family members.

AP3.1.5.13. Measure CHARLIE 13. Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flightline and support facilities.

AP3.1.5.14. Measure CHARLIE 14. Consider escorting children to and from DoD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.).

AP3.1.5.15. Measure CHARLIE 15. (airfield specific) Reduce flying to essential operational flights only. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or TSA (civilian aircraft). Consider relief landing ground

actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

AP3.1.6. FPCON DELTA Measures.

AP3.1.6.1. Measure DELTA 1. Continue, or introduce, all measures in previous FPCON.

AP3.1.6.2. Measure DELTA 2. Augment guards as necessary.

AP3.1.6.3. Measure DELTA 3. Identify all vehicles within operational or mission support areas.

AP3.1.6.4. Measure DELTA 4. Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted very important personnel are exempted.

AP.4.1.6.5. Measure DELTA 5. Control facility access and implement positive identification of all personnel--no exceptions.

AP3.1.6.6. Measure DELTA 6. Search all suitcases, briefcases, packages, etc., brought into the installation.

AP3.1.6.7. Measure DELTA 7. Close DoD schools and/or escort children to/from DoD schools as required.

AP3.1.6.8. Measure DELTA 8. Make frequent checks of the exterior of buildings and of parking areas.

AP3.1.6.9. Measure DELTA 9. Restrict all non-essential movement.

AP3.1.6.10. Measure DELTA 10. (airfield specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

AP3.1.6.11. Measure DELTA 11. (airfield specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

AP3.1.6.12. Measure DELTA 12. If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

## AP3.2. SHIPBOARD FPCON MEASURES

### AP3.2.1. General

AP3.2.1.1. The measures outlined below do not account for local conditions, regulations, special evolutions, or current threat intelligence. The command must maintain flexibility. As threat levels or assessments change, the ship's crew must be prepared to take actions to counter the threat. When necessary, additional measures must be taken immediately. While the simple solution to FPCON CHARLIE or DELTA is to get underway, this option may not always be available.

AP3.2.1.2. Prior to a ship pulling into any port outside of its homeport, the ship shall have an in-port force protection plan approved by the appropriate Commander. Measures to be taken shall be consistent with local rules, regulations, SOFA and the approved in-port force protection plan.

AP3.2.1.3. The duty of the security watch is to safeguard the ship and the ship's company from sabotage, terrorism, civil disturbance, danger, or compromise. The Officer of the Deck (OOD) or equivalent is directly responsible to the Command Duty Officer (CDO) or equivalent, for posting all security watches/sentries and shall ascertain that personnel on watch are familiar with and proficient in their duties. All watch standers bearing arms shall be properly qualified.

AP3.2.1.4. Shipboard FPCON measures are designed to protect vessels in port or at anchorage.

AP3.2.1.5. General Physical Security Procedures for afloat units:

AP3.2.1.5.1. Anyone with reason to believe the ship is in danger of sabotage or terrorist attack shall immediately notify the Officer of the Day.

AP3.2.1.5.2. All hands shall be alert for attempts to board the ship at locations other than the brows, sea ladders, or normal access areas.

AP3.2.1.5.3. Where hostile or subversive elements exist, all hands shall be alert for floating mines or attempts to attach limpet mines to the ship.

AP3.2.1.5.4. Any person who desires to visit the ship shall be denied access until cleared by the OOD.

AP3.2.1.5.5. Material brought aboard shall be randomly inspected by watch-standers, designated members of the Master-at-Arms force, or other petty officers trained in proper inspection procedures. When practical, these inspections shall be conducted prior to bringing material aboard. Contract tools/materials or ship's stores/equipment and like items are to be inspected as soon as practical on weather decks or hangar decks before being struck below.

AP3.2.1.6. Pre-Port procedures. High levels of activity (aboard ship and on the pier when a vessel arrives in port) must not be allowed to degrade security. Security must be integrated into pre-arrival procedures and should include the following actions:

AP3.2.1.6.1. Obtain a current threat assessment from the local NCIS representative.

AP3.2.1.6.2. The appropriate senior commander shall issue security requirements for all ships.

AP3.2.1.6.3. Brief crew on threat, security precautions, recall procedures, and ship's Self Defense Force (SDF) duties.

AP3.2.1.6.4. Muster security forces, brief threat specifics, review rules of engagement or use of force policies, security assignments, and responsibilities.

AP3.2.1.6.5. Brief beach guards and shore patrols on threats and review special procedures applicable to the specific port visit including pier and/or fleet landing security and access control procedures.

AP3.2.1.6.6. When operating under FPCON BRAVO, in non-Navy ports, or a threat to a specific ship is received use, a Military Working Dog and divers to conduct a search of the pier prior to the ship's arrival when available.

AP3.2.1.6.7. If a suspicious item is found, notify the appropriate Explosive Ordnance Disposal unit. Once cleared, shore security elements shall maintain security until relieved by ship's personnel.

AP3.2.1.7. FPCON NORMAL should include ship specific measures a Commander deems necessary when establishing a baseline posture.

AP3.2.2. FPCON NORMAL.

AP3.2.2.1. Measure NORMAL 1. Brief crew on the port specific threat, the security/AT plan, and security precautions to be taken while ashore. Ensure all hands are knowledgeable of various FPCON requirements and that they understand their role in implementation of measures.

AP3.2.2.2. Measure NORMAL 2. Remind all personnel to be suspicious and inquisitive of strangers, be alert for abandoned parcels or suitcases and for unattended vehicles in the vicinity. Report unusual activities to the OOD, Master or Mate on watch, as applicable.

AP3.2.2.3. Measure NORMAL 3. Secure and periodically inspect spaces not in use.

AP3.2.2.4. Measure NORMAL 4. Review security plans and keep them available.

AP3.2.2.5. Measure NORMAL 5. Review pier and shipboard access control procedures including land and water barriers.

AP3.2.2.6. Measure NORMAL 6. Ensure sentries/Mate on Watch, roving patrols and the quarterdeck/gangway watch have the ability to communicate with one another.

AP3.2.2.7. Measure NORMAL 7. Coordinate pier/fleet landing security requirements with SOPA, collocated forces, and/or husbanding agent. Identify anticipated needs for mutual support and define methods of implementation and communication.

AP3.2.3. FPCON ALPHA Measures.

AP3.2.3.1. Measure ALPHA 1. Muster, arm, and brief security personnel on the threat and rules of engagement. Keep key personnel who may be needed to implement security measures on call.

AP3.2.3.2. Measure ALPHA 2. USN combatant ships when in a non-U.S. Navy controlled port, deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside U.S. (minimum standoff distances). DoD non-combatants in a non-U.S. Government controlled port, request husband agent arrange and deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside U.S. (minimum standoff distances).

AP3.2.3.3. Measure ALPHA 3. (USN combatant ship specific) Randomly inspect vehicles entering pier.

AP3.2.3.4. Measure ALPHA 4. Randomly inspect hand carried items and packages before they are brought aboard.

AP3.2.3.5. Measure ALPHA 5. Regulate shipboard lighting to best meet the threat environment.

AP3.2.3.6. Measure ALPHA 6. When in a non-U.S. Government controlled port, rig hawsepipe covers and rat guards on lines, cables and hoses. Consider using an anchor collar.

AP3.2.3.7. Measure ALPHA 7. When in a non-U.S. Government controlled port, raise accommodation ladders, stern gates, ladders, etc when not in use.

AP3.2.3.8. Measure ALPHA 8. Increase frequency of security drills.

AP3.2.3.9. Measure ALPHA 9. Establish internal and external communications; including connectivity checks with local operational commander/agencies/authorities that shall be expected to provide support, if required.

AP3.2.4. FPCON BRAVO Measures.

AP3.2.4.1. Measure BRAVO 1. Continue or introduce all measures in previous FPCON.

AP3.2.4.2. Measure BRAVO 2. Set Material Condition YOKE (secure all watertight door and hatches), main deck and below.

AP3.2.4.3. Measure BRAVO 3. Consistent with local rules, regulations, and/or the SOFA: USN combatant ships post armed pier sentries as necessary; and non-combatant ships post pier sentries (armed at the Master's discretion) as necessary.

AP3.2.4.4. Measure BRAVO 4. Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or the SOFA, establish unloading zones and move all containers as far away from the ship as possible (recommend 100 feet in the United States, 400 feet outside the United States as the minimum stand-off distance).

AP3.2.4.5. Measure BRAVO 5. Consistent with the local rules, regulations, and/or the SOFA: USN combatant ships post additional armed watches as necessary; and non-combatant ships post additional watches (armed at the Master's discretion) as necessary. Local threat, environment and fields of fire should be considered when selecting weapons.

AP3.2.4.6. Measure BRAVO 6. Post signs in local language specifying visiting and loitering restrictions clearly.

AP3.2.4.7. Measure BRAVO 7. When in a non-U.S. Government controlled port, identify and randomly inspect authorized watercraft, such as workboats, ferries and commercially rented liberty launches, daily.

AP3.2.4.8. Measure BRAVO 8. When in a non-U.S. Government controlled port, direct liberty boats to make a security tour around the ship upon departing from and arriving at the ship, with particular focus on the waterline and under pilings when berthed at a pier.

AP3.2.4.9. Measure BRAVO 9. Inspect all visitors' hand carried items, and packages before allowing them aboard. Where available, use baggage scanners and walk through or hand held metal detectors to screen visitors and their packages prior to boarding the ship.

AP3.2.4.10. Measure BRAVO 10. Implement measures to keep unauthorized craft away from the ship. Authorized craft should be carefully controlled. Coordinate with host nation's husbanding agent/local port authority, as necessary, and request their assistance in controlling unauthorized craft.

AP3.2.4.11. Measure BRAVO 11. Raise accommodation ladders, etc, when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

AP3.2.4.12. Measure BRAVO 12. Review liberty policy in light of the threat and revise it, as necessary to maintain safety and security of ship and crew.

AP3.2.4.13. Measure BRAVO 13. USN combatant ships conduct division quarters at foul weather parade. All DoD ships avoid conducting activities that shall gather large number of crewmembers at the weatherdecks. Where possible, relocate such activities inside the skin of the ship.

AP3.2.4.14. Measure BRAVO 14. Ensure an up-to-date list of bilingual personnel for area of operations is readily available. Maintain warning tape, in both the local language and English, is in bridge/pilot house/quarterdeck, for use on the ship's announcing system to warn small craft to remain clear.

AP3.2.4.15. Measure BRAVO 15. If not already armed, arm the quarterdeck/gangway or mate on watch.

AP3.2.4.16. Measure BRAVO 16. If not already armed, consider arming the sounding and security patrol.

AP3.2.4.17. Measure BRAVO 17. Review procedures for expedient issue of firearms and ammunition to the shipboard self-defense force (SSDF)/reaction force and other members of the crew, as deemed necessary by the commanding officer/master.

AP3.2.4.18. Measure BRAVO 18. Instruct watches to conduct frequent, random searches of pier to include pilings and access points.

AP3.2.4.19. Measure BRAVO 19. Conduct visual inspections of the ship's hull and ship's boats at intermittent intervals and immediately before it is put to sea using both landside personnel and waterside patrols.

AP3.2.4.20. Measure BRAVO 20. Hoist ships boats aboard when not in use.

AP3.2.4.21. Measure BRAVO 21. Terminate all public visits. In U.S. Government controlled ports, host visits (family, friends, small groups sponsored by the ship) may continue at the commanding officer's/master's discretion.

AP3.2.4.22. Measure BRAVO 22. After working hours, reduce entry points to ship's interior by securing infrequently used entrances. Safety requirements must be considered.

AP3.2.4.23. Measure BRAVO 23. In non-U.S. Government controlled ports, use only one brow/gangway to access ship (remove any excess brows/gangways). CV(N)s and other large decks may use two as required, when included in an approved AT Plan specific to that port visit.

AP3.2.4.24. Measure BRAVO 24. In non-U.S. Government controlled ports, maintain capability to get underway on short notice or as specified by standard operating procedures.

AP3.2.4.25. Measure BRAVO 25. In non-U.S. Government controlled ports, consider layout of fire hoses. Brief designated crew personnel on procedures for repelling boards, small boats and ultra-light aircraft.

AP3.2.4.26. Measure BRAVO 26. Where applicable obstruct possible helicopter landing areas.

AP3.2.4.27. Measure BRAVO 27. Where possible, monitor local communications (ship to ship, TV, radio, police scanners, etc).

AP3.2.4.28. Measure BRAVO 28. As appropriate, inform local authorities of actions being taken as FPCON increases.

AP3.2.4.29. Measure BRAVO 29. (USN combatant ship specific) If the threat situation warrants, deploy picket boats to conduct patrols in the immediate vicinity of the ship. Brief boat crews and arm with appropriate weapons considering threat, the local environment, and fields of fire.

AP3.2.5. FPCON CHARLIE Measures.

AP3.2.5.1. Measure CHARLIE 1. Continue or introduce all measures in previous FPCON.

AP3.2.5.2. Measure CHARLIE 2. Consider setting Material Condition Zebra (secure all access doors and hatches), main deck and below.

AP3.2.5.3. Measure CHARLIE 3. Cancel liberty. Execute emergency recall.

AP3.2.5.4. Measure CHARLIE 4. Prepare to get underway on short notice. If conditions warrant, request permission to sortie/get underway.

AP3.2.5.5. Measure CHARLIE 5. Block unnecessary vehicle access to the pier.

AP3.2.5.6. Measure CHARLIE 6. Coordinate with host nation husbanding agent and/or local port authorities to establish small boat exclusion zone around ship.

AP3.2.5.7. Measure CHARLIE 7. (USN combatant ship specific) Deploy the SSDF to protect command structure and augment posted watches. Station the SSDF in positions that provide 360 degrees coverage of the ship.

AP3.2.5.8. Measure CHARLIE 8. Energize radar and or sonar, rotate screws and cycle ruder(s) at frequent and irregular intervals, as needed to assist in deterring, detecting or thwarting attacks.

AP3.2.5.9. Measure CHARLIE 9. Consider manning repair locker(s). Be prepared to man one repair locker on short notice. Ensure adequate lines of communications are established with damage control central.

AP3.2.5.10. Measure CHARLIE 10. (USN combatant ship specific) If available and feasible, consider use of airborne assets as an observation/force protection platform.

AP3.2.5.11. Measure CHARLIE 11. If a threat of swimmer attack exists, activate an anti-swimmer watch.

AP3.2.5.12. Measure CHARLIE 12. In non-U.S. Government controlled ports and if unable to get underway, consider requesting armed security augmentation from area Combatant Commander.

AP3.2.6. FPCON DELTA Measures.

AP3.2.6.1. Measure DELTA 1. Continue or introduce all measures in previous FPCON.

AP3.2.6.2. Measure DELTA 2. Permit only necessary personnel topside.

AP3.2.6.3. Measure DELTA 3. If possible, cancel port visit and get underway.

AP3.2.6.4. Measure DELTA 4. Employ all necessary weaponry to defend against attack.

# AP4. APPENDIX 4
# SAMPLE INSTALLATION ANTITERRORISM PLAN FORMAT

## AP4.1. OVERVIEW

AP4.1.1. The format outlined below is offered as one means of developing an AT plan. It is optimized for a base or installation, but can be adapted for other facilities and deployed units. It is meant to help the AT officer structure the AT plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military operations order (Situation-Mission-Execution-Administration and Logistics-Command and Signal).

AP4.1.2. This format enables the synchronization of existing programs such as Law Enforcement, Physical Security, AT, OPSEC, INFOSEC, High-Risk Personnel protection and other installation efforts. AT Plans should be integrated into all plans and separate annexes. Remember that staff interaction is a crucial element of developing a realistic, executable plan.

AP4.1.3. Although this sample is patterned after the military operations order, it is applicable to managers of OSD Agencies as they develop plans to protect personnel, activities, and material under their control.

AP4.1.4. This sample uses supporting Annexes, Appendices, Tabs, and Enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

Copy no. ____of_____ Copies

Installation/Operation Name
Location
Date/Time Group

INSTALLATION/OPERATION NAME ANTITERRORISM PLAN 2002 (AT-04)

Task Organization. [Include all agencies/personnel (base and civilian) responsible to implement the plan. Include as a separate Annex. See Annex A (Task Organization).]

Maps/Charts: [List all applicable maps or charts. Include enough data to ensure personnel are using the correct year/edition/version of the subject material.]

Time Zone: [Enter the time zone of the installation. Indicate the number of hours to calculate (plus/minus) ZULU time.]

Ref: [Enter the compilation of pertinent publications, references, MOU/MOA/MAA. This list may be included in a separate Annex. See Annex Q (References).]

1. SITUATION

a. General. [This plan applies to all personnel assigned or attached to the installation. [Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.]

b. Enemy. [The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. [ENTER the general threat of terrorism to this installation including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See paragraph 1f, Intelligence, on identifying specific threats.] This information may be included as a separate Annex. See Annex B (Intelligence).]

c. Friendly. [ENTER the forces available (both military and civilian) to respond to a terrorist WMD attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units/organizations may include Host Nation (HN) and US military police forces, fire and emergency services, medical, and federal/state and local agencies, special operations forces, engineers, detection (radiological, nuclear, biological, and chemical) decontamination or smoke units, and explosive ordnance disposal (EOD). Include MOAs/MOUs and any other special arrangements that will improve forces available to support the plan. If in the U.S. and its territories, the Department of Justice, Federal Bureau of Investigation (FBI) is responsible for coordinating all Federal agencies and DoD forces assisting in the resolution of a terrorist incident. If outside the U.S. and its territories, the Department of State (DOS) is the lead agency. This information can be included in a separate Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).]

d. Attachments/Detachments. [ENTER installation/civilian agencies NOT normally assigned to the installation that are needed to support this plan. Explain interagency relationships and interoperability issues. This can be listed in other Annexes. See Annex A (Task Organization) and Annex J (Command Relationships).]

e. Assumptions. (List planning/execution assumptions) [ENTER all critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT plan and that must addressed in order to continue to plan. They can range from the installation's troop strength to addressing the local political/social environment. Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats. The installation is also vulnerable to a WMD attack.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources; therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to WMD attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, non-military response forces will arrive within [time] of notification.

(7) Units specializing in WMD response will arrive on-site within [number of hours based on installation location] of notification.

(8) The HN is supportive of U.S. policies, and will fulfill surge requirements needed to respond to a WMD incident IAW MOAs/MOUs.]

f. Intelligence. [ENTER the person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence. This can be included in Annex B (Intelligence).] [National-level agencies, Combatant Commanders, and intelligence systems provide theater or country threat levels and threat assessments. In the U.S. and its territories, local installations must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other federal agencies.]Obtain these assessments, as they will serve as a baseline for the installation's tailored assessment. The installation should have a process in place for developing the installation's tailored threat assessment or "local threat picture." The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation commander. The commander should determine the frequency and the means of dissemination of the installation's tailored AT product. Note: Commanders cannot change the threat level, which is developed at the national-level although they can declare higher FPCONs than the baseline.

2. MISSION. [ENTER a clear, concise statement of the command's mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat, enhance security and AT awareness, and to assign AT responsibilities for installation personnel.]

3. EXECUTION

a. Commander's Intent. (Commander's vision on how he/she sees the execution of the unit's AT program. Refer to Service planning doctrine for assistance.)

b. Concept of Operations. [ENTER how the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.

(1) The installation's AT Concept of Operations should be phased in relation to pre-incident actions and post-incident actions. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The

AT mission, and the unpredictability of its execution, requires very specific "how to" implementation instructions of DoD FPCON Measures and in what manner these actions must be coordinated. This "how to" element is not normally included in the Concept of Operations paragraph; however the necessity to provide "how to" guidance in the AT plan requires a different manner of data presentation to ensure brevity and clarity. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix (Pre-Incident Action Set Matrix).

(2) In Post-Incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation's organic capabilities. National-level responders (Federal Emergency Management Agency (FEMA), Red Cross, and Federal Bureau of Investigation (FBI)) may not be immediately accessible or available to respond to an installation's needs. Therefore each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation not only conduct the initial response but also sustained response operations. Many installations do not have onboard WMD officers or response elements. This paragraph will include specific implementation instructions for all functional areas of responsibility and the manner in which these actions must be coordinated. The implementation instructions can be put in the form of actions sets and displayed in the form of a synchronization matrix (Post-Incident Action Set Synchronization Matrix). The synchronization matrix format clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a terrorist incident.

c. Tasks. [ENTER the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT and/or WMD specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. While the tasks and responsibilities for each AT planning and response Element will be delineated in the Pre- and Post-incident Action Set Matrices, it is recommended that the installation commander identify/designate the primary lead for each element and enter that information in this paragraph.]

(1) First Subordinate Unit/Element/Tenant

(a) Task listing.

d. Coordinating Instructions. [This paragraph should include AT specific coordinating instructions and subparagraphs, as the commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the purposes of this plan, there are five basic coordinating instructions: 1) AT planning and response elements; 2) Procedural; 3) Security Posture; 4) Threat Specific Responsibilities; and 5) Special Installation Areas. The reader will be directed to specific Annexes that will provide amplifying instructions on these topics. The sections listed below are representative, and may not be all-inclusive.

(1) AT Planning and Response. For instructional purposes, this template outlines AT planning and response elements on the installation required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort between the many AT planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/State/ Federal agencies (U.S. and its territories) or HN (outside the U.S. and its territories). For the purposes of this plan, an installation's capability is divided into AT planning and response elements. These tailored, installation-level elements parallel the national-level FEMA ESFs and the JSIVA evaluation criteria to the greatest degree possible.

AT Planning & Response Elements

| | | |
|---|---|---|
| Information & Planning | * | |
| Communications | * | + |
| HAZMAT | | * |
| Security | * | + |
| Explosive Ordnance Disposal (EOD) | | + |
| Firefighting | * | + |
| Health & Medical Services | * | + |
| Resource Support | * | |
| Mass Care | | * |
| Public Works | | * |
| Intelligence Process | | + |
| Installation AT Plans/Programs | | + |
| Installation Perimeter Access | | + |
| Security System technology | | + |
| Executive Protection | | + |
| Response & Recovery | | + |
| Mail Handling | | + |

* Derived from FEMA ESFs
\+ Derived from JSIVA assessment criteria

(2) Procedural

(a) Alert Notification Procedures. See Appendix 14 to Annex C (Operations).

(b) Use of Force/Rules of Engagement. See Annex H (Legal).

(c) Installation Training & Exercises. See Annex N (AT Program Review, Training & Exercises).

(d) Incident Response. See Appendix 1 to Annex C (Operations).

(e) Consequence Management. See Appendix 1 to Annex C (Operations).

(f) High-Risk Personnel Protection Procedures. See Appendix 9 to Annex C (Operations).

(g) AT Program Review (See Annex N (AT Program Review, Training & Exercises).

(h) Higher Headquarters Vulnerability Assessments. See Annex N (AT Program Review, Training & Exercises).

(3) Security Posture Responsibilities

(a) Law Enforcement. See Appendix 7 to Annex C (Operations).

(b) Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C Operations).

(c) Other On-site Security Elements. See Appendix 8 to Annex C (Operations).

(d) Operations Security. See Appendix 10 to Annex C (Operations).

(e) Technology. See Appendix 15 to Annex C (Operations).

(f) EOC Operations. See Appendix 12 to Annex C (Operations)

(g) Critical Systems Continuity of Operations (optional). See Appendix 13 to Annex C (Operations).

(h) Other

(4) Threat Specific Responsibilities

(a) Antiterrorism. See Appendix 2 to Annex C (Operations).

(b) Weapons of Mass Destruction. See Appendix 5 to Annex C (Operations).

(c) Special Threat Situations. See Appendix 3 to Annex C (Operations).

(d) Information Security. See Appendix 11 to Annex C (Operations).

(e) Natural/Man-made Hazards (Optional). See Appendix 16 to Annex C (Operations).

(f) Other

(5) Special Security Areas

(a) Airfield Security. See Appendix 4 to Annex C (Operations).

(b) Port Security. See Appendix 4 to Annex C (Operations).

(c) Embarkation/Arrival Areas. See Appendix 4 to Annex C (Operations).

(d) Buildings. See Appendix 4 to Annex C (Operations).

(e) Other

4. ADMINISTRATION AND LOGISTICS. [ENTER the administrative and logistics requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for both pre- and post-incident measures addressing the following: locations of consolidated WMD defense equipment; expedient decontamination supplies; Individual Protective Equipment exchange points; special contamination control requirements; retrograde contamination monitoring sites; WMD equipment/supply controlled supply rates and pre-stockage points; and procedures for chemical defense equipment "push" packages. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the Concept of Operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Finally, include fiscal instructions on how to support AT operations.

a. Administration. See Annex O (Personnel Services).

b. Logistics. See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. [ENTER instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and emergency operations center. Enter the installation's chain of command. Highlight any deviation from that chain of command that must occur as a result of a WMD incident. The chain of command may change based on the deployment of a Joint Task Force or a National Command Authority-directed mission. Identify the location of any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. Recommend the installation

coordinate with higher headquarters to establish procedures to allow for parallel coordination to report a terrorist WMD incident. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to the incident.]

a. Command. See Annex A (Task Organization) and Annex J (Command Relationships).

b. Signal. See Annex K (Communications).

c. Command Post Locations

(1) Primary: [ENTER location]

(2) Alternate: [ENTER Location]

d. Succession of Command

(1) First alternate: [ENTER POSITION/TITLE]

(2) Second alternate: [ENTER POSITION/TITLE]

//SIGNATURE//
Commanding General/Officer
Signature Block

ANNEXES: (Should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be sub-divided into APPENDICES, TABS, and ENCLOSURES as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures, and referenced as required.)

ANNEX A - Task Organization [ENTER key AT organization composition i.e., AT Working Group, Crisis Management Team, Emergency Operations Center, First Response Elements, etc.]

Appendix 1 – Table of Organization

Appendix 2 – Post Prioritization Chart

ANNEX B – Intelligence [ENTER the agency(s) responsible for intelligence and specific instructions. In the U.S. and its territories, commanders must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement or other federal agencies]

Appendix 1 – Local Threat Assessment

Appendix 2 – Local WMD Assessment

Appendix 3 – Local Criticality/Vulnerability Assessment

Appendix 4 – Risk Assessment

Appendix 5 – Pre-deployment AT Vulnerability Assessment

ANNEX C – Operations [This is the most IMPORTANT part of the plan]. Annex C and supporting Appendices will provide specific instructions for all the various AT operations. All other Annexes/Appendices support the implementation of Annex C.

Appendix 1 – Incident Planning and Response [ENTER how the various agencies (military/civilian) and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the operational spectrum. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure.]

Tab A – Incident Command and Control Procedures
Tab B – Incident Response Procedures
Tab C – Consequence Management Procedures

Appendix 2 – Antiterrorism

Tab A - Mission Essential Vulnerable Assets (MEVA)
Tab B - Potential Terrorist Targets
Tab C – FPCON
Enclosure 1 - FPCON Action Sets [Who/What/When/Where/How]
Tab D - Random Antiterrorism Measures (RAM) Procedures

Appendix 3 - Special Threat Situations

Tab A - Bomb Threats
Enclosure 1 – Bomb Threat Mitigation
Enclosure 2 – Evacuation Procedures
Enclosure 3 – Search Procedures
Tab B - Hostage Barricaded Suspect
Tab C – Mail Handling Procedures

Appendix 4 – Special Security Areas

Tab A – Airfield Security
Tab B – Port Security
Tab C – Embarkation/Arrival Areas.
Tab D – Buildings

Appendix 5 – Weapons of Mass Destruction (CBRNE) & HAZMAT [ENTER the specific procedures planning, training, and response to WMD (CBRNE) incidents. Care should be taken to integrate existing plans for response to HAZMAT incidents to avoid duplication. Include "baseline" preparedness.]

Tab A - WMD Action Set Synchronization Matrix [Who/What/Where/When/How]
Tab B – CBRNE Emergency Responder Procedures

Appendix 6 – Physical Security

Tab A – Installation Barrier Plan [ENTER procedures and pictorial representation of barrier plan.]
Tab B – Installation Curtailment Plan
Tab C – Construction Considerations
Tab D – Facility and Site Evaluation and/or Selection
Tab E – AT Guidance for Off-Installation Housing

Appendix 7 – Law Enforcement

Tab A – Organization, training, equipping of augmentation security forces
Tab B – Alternate Dispatch Location
Tab C – Alternate Arming Point

Appendix 8 – Other On-Site Security Forces

Appendix 9 – High Risk Personnel

Tab A – List of High Risk Billets

Appendix 10 – Operations Security

Appendix 11 – Information Security

Appendix 12 – Emergency Operations Center (EOC) Operations [ENTER procedure for the activation & operations of the EOC.]

Tab A – EOC Staffing (Partial/Full)
Tab B – EOC Layout
Tab C – EOC Messages & Message Flow
Tab D – EOC Briefing Procedures
Tab E – EOC Situation Boards
Tab F – EOC Security and Access Procedures

Appendix 13 – Critical Systems Continuity of Operations Plans (Optional) [ENTER those systems that are essential to mission execution and infrastructure support of the installation i.e., utilities systems, computer networks, etc. This document outlines how the installation will continue to operate if one or more critical systems are disrupted or fails and how the systems will be restored.]

Tab A – List of installation critical systems
Tab B – Execution checklist for each critical system

Appendix 14 - Emergency Mass Notification Procedures [ENTER the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.

Tab A – Situation Based Notification
Tab B – Matrix List of Phone Numbers/Email Accounts

Appendix 15 – Exploit Technology Advances [ENTER the process and procedures for developing and employing new technology. Identify who is responsible and what should be accomplished.]

Appendix 16 – Higher Headquarters Vulnerability Assessments [ENTER procedures for conducting higher headquarters vulnerability assessments.

Appendix 17 – Natural/Man-made Hazards (Optional) [Hurricanes, Flooding, Chemical Plants etc.]

Tab A - Locality specific natural and man-made hazards)

ANNEX D – Logistics (Specific logistics instructions on how to support AT operations)

Appendix 1 – Priority of Work [ENTER the priority of employing scarce logistical resource.]

Appendix 2 – Emergency Supply Services

Appendix 3 – Weapons and Ammunition Supply Services

Appendix 4 – Emergency Equipment Services

Appendix 5 – Evacuation Shelters

Appendix 6 – Generator Refueling Matrix

ANNEX E – Fiscal (Specific fiscal instructions on how to support AT operations from pre-incident through post-incident)

Appendix 1 – AT Program of Memorandum Budget Submission Instruction

Appendix 2 – Combating Terrorism Readiness Submission Instructions

Appendix 3 – Fiscal Management during Exigent Operations

ANNEX F – Tenant Commanders (Specific instructions on how tenant commands/agencies support AT operations)

Appendix 1 – Areas of Responsibility (Pictorial)

ANNEX G – Air Operations (Specific air instructions on how to support AT operations)

Appendix 1 – List of Landing Zones (Used for emergency medical evacuations or equipment/personnel staging areas.)

Appendix 2 – LZ Preparation Procedures

ANNEX H – Legal [ENTER the jurisdictional limits of the installation's commander and key staff. Although the Department of Justice, Federal Bureau of Investigation (FBI), has primary law enforcement responsibility for terrorist incidents in the United States, the installation commander is responsible for maintaining law and order on the installation. For OCONUS incidents, the installation commander must notify the HN and the geographic combatant commander; the geographic combatant commander will notify the Department of State (DOS). Once a task force or other than installation support arrives on the installation, the agencies fall under the direct supervision of the local Incident Commander. In all cases, command of military elements remains within military channels. The installation should establish HN agreements to address the use of installation security forces, other military forces, and host-nation resources that clearly delineate jurisdictional limits. The agreements will likely evolve into the installation having responsibility "inside the wire or installation perimeter" and the HN having responsibility "outside the wire or installation perimeter". There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms that may require the installation to be responsible for certain areas outside of the installation perimeter.]

Appendix 1 – Jurisdictional Issues

Appendix 2 – Use of Force and/or Rules of Engagement Instructions

Appendix 3 – Pictorial Representation of Installation Jurisdiction

ANNEX I – Public Affairs (Specific PAO instructions on how to support AT operations)

Appendix 1 – Command Information Bureau Organization & Operation

Appendix 2 – Local/Regional Media Contact Information

annex J – Command Relationships (Provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control).

Appendix 1 – AT Organizational Charts [Crisis Management Team, AT Working Group, First Responder Elements, Incident Command Organization (include civilian and other external agencies).]

ANNEX K – Communications (Specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means.)

Appendix 1 – Installation AT Communication Architecture

Appendix 2 – Incident Command Communication Architecture

Appendix 3 – EOC Communication Architecture

Appendix 4 – Security Force Communication Architecture

Appendix 5 – Fire Department Communication Architecture

Appendix 6 – Medical Communication Architecture

Appendix 7 – Other Agencies

ANNEX L - Health Services (Specific medical instructions on how to support AT operations)

Appendix 1 - Mass Casualty Plan

Appendix 2 - Procedures for Operating with Civilian Emergency Medical Service and Hospitals

ANNEX M – Safety (Specific safety instructions on how to support AT operations)

ANNEX N – AT Program Review, Training, & Exercises

Appendix 1 – AT Program Review

Tab A – Local Assessments
Tab B – Higher Headquarters Assessments

Appendix 2 – AT Required Training

Appendix 3 – Exercises

ANNEX O – Personnel Services [ENTER administrative and personnel procedures required to support the plan i.e., civilian overtime, post-traumatic stress syndrome counseling.]

Appendix 1 – Operating Emergency Evacuation Shelters

ANNEX P – Reports [ENTER all the procedures for report submissions & report format.]

Appendix 1 – Reporting Matrix

ANNEX Q – References [ENTER all supporting reference materials, publication, regulations etc.]

ANNEX R – Distribution [ENTER the list of agencies to receive this plan. Cover plan classification, handling and declassification procedures.]

# AP5. APPENDIX 5
# TERRORIST INCIDENT RESPONSE MEASURES CHECKLIST

## AP5.1. INTRODUCTION

The antiterrorism success of each unit operating within a Combatant Command shall depend on the degree and seriousness of the crisis management planning. The following checklist identifies items that should be considered for inclusion into the crisis management plan prepared for each unit, activity, installation, or organization as appropriate.

**Table AP5.T1. Terrorist Incident Response Checklist**

| | |
|---|---|
| Intelligence | |
| | Does the plan allow for the intelligence-gathering process (e.g., collection, evaluation, and dissemination of information) to aid in the identification of the local threat? |
| | Does the plan consider restrictions placed on the collection and storage of information? |
| | Does the plan indicate an awareness of sources of information for the intelligence-gathering effort (e.g., military intelligence, federal agencies, state/local authorities)? |
| | Does the plan allow for liaison and coordination of information (e.g., establishing a threat committee)? |
| Threat Analysis | |
| | Does the plan identify the local threat (immediate and long-term)? |
| | Does the plan identify other threats (e.g., national and international groups who have targeted or might target US installations)? |
| | Does the installation incorporate factors of the installation vulnerability determining system when assessing the threat? Does it address: |
| | Geography of the area concerned. |
| | Law enforcement resources. |
| | Population factors. |
| | Communications capabilities. |
| | Does the plan establish a priority of identified weaknesses and vulnerabilities? |
| Security Countermeasures | |
| | Does the plan have specified FPCONs and recommended actions/measures? |
| | Do security countermeasures include a combination of physical operations and sound-blanketing security measures? |

| | |
|---|---|
| Operations Security | |
| | Have procedures been established that prevent terrorists from readily obtaining information about plans and operations (e.g., not publishing the commanding general's itinerary, safeguarding classified material, etc.)? |
| | Does the plan allow for in-depth coordination with the installation's OPSEC program? |
| | Has an OPSEC annex been included in the contingency plan? |
| Personnel Security | |
| | Has an education process been started that identifies threats to vulnerable personnel? |
| | Has the threat analysis identified individuals vulnerable to terrorist attack? |
| | Has a school trained AT Officer been designated in writing. |
| Physical Security | |
| | Are special threat plans and physical security plans mutually supportive? |
| | Do security measures establish obstacles to terrorist activity (e.g., guards, host nation forces, lighting, fencing)? |
| | Does the special threat plan include the threats identified in the threat statements of higher headquarters? |
| | Does the physical security officer assist in the threat analysis and corrective action? |
| | Is there obvious command interest in physical security? |
| | Does the installation have and maintain detection systems and an appropriate assessment capability? |
| Security Structure | |
| | Does the plan indicate that the FBI has primary domestic investigative and operational responsibility? |
| | Has coordination with the staff judge advocate been established? |
| | Does the plan allow for close cooperation between principal agents of the military, civilian, and host nation communities and federal agencies? |
| | Does the plan clearly indicate parameters for use of force, including the briefing of any elements augmenting military police assets? |
| | Is there a mutual understanding between all local agencies (e.g., military, local FBI resident or senior agent-in-charge, host nation forces and local law enforcement) that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction? |
| | Has the staff judge advocate considered ramifications of closing the post (e.g., possible civilian union problems)? |
| Emergency Operations Center (EOC) Training | |
| | Has the EOC been established and exercised? |
| | Is the EOC based on the needs of the installation while recognizing manpower limitations, resource availability, equipment, and command? |
| | Does the plan include a location for the EOC? |
| | Does the plan designate alternate locations for the EOC? |

| | |
|---|---|
| Emergency Operations Center (EOC) Training (cont.) | |
| | Does the plan allow for the use of visual aids (e.g., chalkboards, maps with overlays, etc.) to provide situation status reports and countermeasures? |
| | Does the plan create and designate a location for a media center? |
| | Have the EOC and media center been activated together within the last quarter? If not provide date of the last activation. |
| | Does the EOC have SOPs covering communications and reports to higher headquarters? |
| Reaction Force Training | |
| | Has the reaction force been formed, equipped (including CBRNE equipment) and mission-specific trained (e.g., building entry and search techniques, vehicle assault operations, anti-sniper techniques, equipment)? |
| | Has the force been briefed on laws and policies governing the use of force and the use of deadly force in the protection of DoD personnel, facilities, and materiel? |
| | Has the force been trained and exercised under realistic conditions? |
| | Has corrective action been applied to shortcomings/deficiencies? |
| | Has the reaction force been tested quarterly (alert procedures, response time, overall preparedness)? |
| | Has responsibility been fixed for the negotiation team? Has the negotiation team been trained and exercised under realistic conditions? |
| General Observations | |
| | Was the plan developed as a coordinated staff effort? |
| | Does the plan outline reporting requirements (e.g., logs, journals, after-action report)? |
| | Does the plan address controlled presence of the media? |
| | Does the plan include communications procedures and communications nets? |
| | Does the plan consider the possible need for interpreters? |
| | Does the plan consider the need for a list of personnel with various foreign backgrounds to provide cultural intelligence on foreign subjects and victims, as well as to assist with any negotiation efforts? |
| | Does the plan provide for and identify units that shall augment military police assets? |
| | Does the plan delineate specific tasking(s) for each member of the operations center? |
| | Does the plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)? |
| | Does the plan designate service support requirements (e.g., engineer, aviation, medical, communications, etc.)? |
| | Does the plan make provisions for notification of nuclear assessment teams and the nuclear accident/incident control officer? |
| | Does the plan provide for explosive ordnance disposal (EOD) support? |

| General Observations (cont.) | |
|---|---|
| | Does the plan take into consideration the movement from various locations, including commercial airports, of civilian and military advisory personnel with military transportation assets? |
| | Does the plan allow for the purchase and/or use of civilian vehicles, supplies, food, etc., if needed (including use to satisfy a hostage demand)? Does the plan make provisions for paying civilian employees overtime if they are involved in a special threat situation? |
| | Does the plan take into consideration the messing, billeting, and transportation of civilian personnel? |

# AP6. APPENDIX 6
# AT MEASURES FOR IN-TRANSIT FORCES

## AP6.1. INTRODUCTION

Numerous DoD elements, personnel and assets constantly transit, or are deployed outside of U.S. controlled areas. These elements, commonly referred to as in-transit forces, confront unique vulnerabilities due to their "in-transit" status. This appendix provides guidance for Commanders and ATOs to enhance the AT posture of in-transit forces transiting, or deployed to/from their AOR.

## AP6.2. AT ASSESSMENTS

AP6.2.1. Reference (e) requires Commanders with AT responsibility for a transiting force complete a pre-deployment AT VA. The VA should include movement routes that may be used by transiting DoD forces, ships and aircraft. Transiting forces include all DoD ships, aircraft, units and elements that could present lucrative and/or vulnerable terrorist targets.

AP6.2.1.1. AT Assessments should be conducted sufficiently in advance of deployments to allow and facilitate the development of security procedures, acquisition of necessary materials, obtaining tailored and focused intelligence, organize necessary security support augmentation, and to conduct required host nation coordination.

AP6.2.1.2. The AT Assessment should also be within a timeframe that provides the Commander with current situational information. Previous and periodic assessments of many locations shall be available to Commanders. These assessments may satisfy many pre-deployment requirements and provide data that can be updated and/or validated to alleviate the need for an additional assessment, or reduce the scope of the assessment if warranted.

AP6.2.2. The AT Assessment should provide deploying Commanders a baseline to implement appropriate AT measures to reduce risk and vulnerability.

AP6.2.2.1. If warranted, Commanders faced with emergent AT requirements prior to movement of forces should submit CbT RIF requests through established channels (see chapter 16) to procure necessary materials or equipment for required AT measures.

AP6.2.2.2. Equipment and technology can significantly enhance AT posture for all DoD forces (see chapter 17), and in particular the security posture of transiting units against terrorist threats. The Component Commanders should research and identify AT equipment and/or

technology requirements to their chain of command. The use of COTS or government-of-the-shelf (GOTS) products should be stressed to meet near-term requirements.

AP6.3. SECURITY PLANS

AP6.3.1. A security document should be prepared for each deployment. This document can be in various formats (Plan, SOP, or LOI) according to the existing AT threat, the deployment size and/or its complexity. While not to the detail of an installation AT Plan, it should address the following areas as applicable.

**Table AP6.T1. AT Security Document**

| AT Security Document (Plan, SOP, or LOI) |
|---|
| • Task Organization |
| • Threat Assessment Process (see Chapter 5) |
| • Request and Review of Tailored Threat Information |
| • Process and Equipment to Transmit and Receive Intelligence |
| • Vulnerability Assessment Process (see Chapter 7) |
| • Concept of Operations |
| • Risk Assessment Process (see Chapter 8) |
| • Implementation of Force Protection Condition Measures (see Chapter 10) |
| • Security Measures Tailored to Local Conditions |
| • Security for In-transit Aircraft |
| • Coordinated Transient Aircraft Security Requirements |
| • Message Guidance for Requesting Additional Security |
| • Rules of Engagement/Use of Force |
| • Threat Working Group |
| • Airfield Responsibility Matrix |
| • Airfield Assessment Checklist |
| • Security for In-transit Ships |

| AT Security Document (Plan, SOP, or LOI) |
|---|
| • Example of Inport Security Plan<br>• Example of LOGREQ Security Supplement<br>• Example of Inport Security Plan Approval<br>• Security Assessment Survey Form and Checklist for Non-U.S. Ports<br>• Security for In-transit Ground Forces<br>• Assessment Checklist for In-transit Ground Forces<br>• Transitioning to Higher Force Protection Conditions (see Chapter 10)<br>• RAM (see Chapter 10)<br>• Access Control Procedures<br>• Physical Security Measures<br>• Incident Response and Consequence Management (see Chapters 11 and 12)<br>• Billeting Security<br>• Vetting of Contract Services (see Chapter 16)<br>• Local/Host Nation Support and Coordination |

AP6.3.2. AT Planning Requirements. The following matrix displays AT planning requirements to consider when developing in-transit forces security plans.

**Table AP6.T2. AT Planning Requirements Matrix**

| CATEGORY | THREAT | FPCON | PLANNING PROCESS | REMARKS |
|---|---|---|---|---|
| | | | | |
| **Combatant Command Level** | | | AT OPORD | AT factored into OPORD/DEPORDs |
| | | | | |
| | | | | |
| **Component Level** | | | OPORD/Regulation/Instruction | AT factored into OPORD/DEPORDs |
| | | | | |
| | | | | |
| **Intermediate Command (NAF, CORPS, etc.)** | | | AT factored into OPORDs and DEPORDs | |
| | | | | |
| **Installation/site** | | | Comprehensive, executable AT Plan/OPORD | |
| | | | | |
| | | | | |

| CATEGORY | THREAT | FPCON | PLANNING PROCESS | REMARKS |
|---|---|---|---|---|
| **Significant Military Exercises (SME)** | | | AT factored into EXORD, Exercise Directive, SMEB, and/or AT Plan/OPORD | |
| | | | | |
| **CTF, JTF, TF, Deployed Operational Force** | | | Comprehensive, tailored AT Plan/OPORD | As specified in OPORD/DEPORD |
| | | | | |
| **Transiting Ships** | | | For each Port Visit: | |
| | All Levels | All Levels | Port Vulnerability Assessment (PVA) | |
| | All Levels | All Levels | Threat Assessment | |
| | All Levels | All Levels | Inport Security Plan (ISP) | |
| | All Levels | BRAVO or higher | AT LOGREQ Supplement | |
| | | | | |
| **Transiting Aircraft** | | | | |
| Category "A" Airfield | | | Based on Threat/Vulnerability Assessments and TWG review, Security Planning Package for aircrew | More stringent security required at CAT "B" locations |
| Category "B" Airfield | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Unit Ground Movement** | | | | |
| More than 50 | All Levels | | Movement Security Plan | |
| More than 50 | Significant or High | | Movement Security Plan Approved by General Officer | Vulnerability Assessment required for Significant/High threat level or Terrorist Warning Report |
| *** Less than 50 | | | At discretion of Commander | |
| | | | | |
| **TDY Groups/Individuals** | | | | |
| General/Flag Officer | | | Engage in planning process as defined in OPORD | HRP itineraries FOUO or classified |
| | | | | |
| 06 and below | | | Follow FCG procedures, and Combatant Command Travel Policy - Review Threat Information & conduct Risk Assessment | |
| *** Less than 50 | | | | |
| | | | | |
| | | | | |
| | | | | |
| Event (50 +) | | | Follow FCG procedures, and Combatant Command Travel Policy - Review Threat Information & conduct Risk Assessment | If threat is significant or high, General/ Flag Officer must approve |
| *** Event (25 - 50) | | | | |
| *** Event (Less than 25) | | | | |
| | | | | |
| *** See AP6.3.3. | | | | |

AP6.3.3. For events, activities or travel involving less than 50 personnel, a detailed written AT plan is usually inappropriate. Factoring AT into each phase of planning is still required, but the documented results may be as simple as a 5 Para OPORD, or just a wallet-sized card listing key POCs and contact numbers at the visited location. Table AP6.T3. provides a Planning Guide

for Small Groups designed to help the Commander prepare a plan for individual and/or small group travels.

**Table AP6.T3. AT Planning Process for Individual & Small Group Travel (less than 50)**

| AT Planning Process for Individual & Small Group Travel (less than 50) |
|---|
| PART I. OBJECTIVE: DETERMINE THE THREAT<br><br>1. Determine if any DOS Travel Warnings are in effect.<br><br>2. Determine if Combatant Commander has issued any warnings.<br><br>3. Determine if Combatant Commander has placed any restrictions on DOD travel to the area.<br><br>4. Determine the country's existing Threat Levels for the Foreign Intelligence Threat, Terrorism Threat, Political Violence, Crime, and Health Protection/Risk.<br><br>5. Obtain any additional threat information about a given country from the Combatant Commander's intelligence organization (i.e. graphic picture of potential threats). |
| PART II. OBJECTIVE: DETERMINE MISSION CRITICALITY AND VULNERABILITIES<br><br>6. Determine importance/priority of MISSION:<br><br>ADMINISTRATIVE: _____<br>OPERATIONAL: _____<br>ESSENTIAL/CRITICAL: _____<br><br>7. Determine Foreign Clearance Guide (FCG) requirements/constraints. The following key elements of information for planning purposes can be extracted:<br><br>COUNTRY CLEARANCE REQUIRED: _____<br>THEATER CLEARANCE REQUIRED: _____<br>SPECIAL AREA CLEARANCE REQUIRED: _____<br>COORDINATION ONLY: _____<br>APPROVAL ASSUMED: _____<br>CLEARANCE GRANTING AUTHORITIES _____<br>LEAD TIME REQUIRED: _____<br>MESSAGE REQUEST FORMAT _____<br>KEY CONTACT NUMBERS (DATT, POST 1, ETC,) _____<br><br>8. Develop Mission Plan in coordination with POC at the TDY location:<br><br>Determine Modes of Travel and Routes _____<br>If arriving by Air:<br>Rental car required _____<br>Taxi service available _____<br>Expeditor provided _____<br>* Review local maps _____<br>Identify Billeting location _____ |

**AT Planning Process for Individual & Small Group Travel (less than 50)**

** Review Vulnerability Assessments _____
Determine Visibility of Mission (publicity) _____
*** Determine Operating Environment _____
Determine Policy for Wear of Uniform _____

* To find local maps, there are a variety of tools on the NIPRNET. For example, go to <MAPQUEST.COM> and select <MAPS>; then the appropriate country. On the SIPRNET, go to <Geography & Maps> and select one of search engines available, such as Raster Roam.

** To find previous Vulnerability Assessments, query the POC at the TDY location.

*** The Operating Environment is one factor in the Terrorist Threat methodology and should be contained in the DIA/JAC Threat Assessments. See PART I, above. Also query the POC at the TDY location.

PART III. OBJECTIVE: CONDUCT MISSION RISK ASSESSMENT AND MITIGATING MEASURES TO REDUCE THE RISK

9. Contrast the results of Threat and Vulnerability Assessment data. Make a reasonable, subjective judgment of the level of Risk associated with the mission, AND based on the criticality of the mission, determine if the level of Risk is acceptable.

LOW _____ MEDIUM _____ HIGH _____

10. Consider introducing the following mitigating measures to reduce the level of Risk:

Prior to and during Travel Phase:

Adjust itineraries to avoid High/Potential Physical Threat Countries _____
Use of MILAIR in lieu of commercial air transportation _____
Obtain and use Regular-fee passports _____
Use name-only credit cards with no USG identifiers _____
Remove all USG identifiers from luggage, carryon baggage & clothing _____
Wear conservative, low profile civilian clothing _____
Upon arrival at airports, enter a secure/protected area ASAP _____
Handle all detailed itineraries as FOUO (or classify if appropriate) _____
Have worldwide capable cell phone available _____
Follow recognized procedures to minimize impact of hijacking scenario _____
Arrange for expeditor support upon arrival at TDY location _____

At TDY Location:

Upon arrival, immediately establish communications with local POC _____
Confirm accuracy of all local contact numbers _____
Ensure "home office" has local contact numbers and itinerary _____
Have communications capability with home office and local POC at all times _____
Obtain local threat update briefing as soon as practical _____
Review all Welcoming packet information to increase awareness _____
Avoid ground floor billeting and rooms with exteriors facing streets _____
Identify all fire exits and escape routes from the billeting location _____
When in hotel room, keep curtains closed and jam entrance doors _____
When exiting hotel room, always check for unusual activity _____

| AT Planning Process for Individual & Small Group Travel (less than 50) | |
|---|---|
| Turn off lights in hotel room, before opening the door to exit | _____ |
| Keep room neat and orderly to detect any surreptitious activity | _____ |
| When entering and exiting facilities, vary use of stairwells and elevators | _____ |
| Wear civilian clothing in public areas outside of military facilities | _____ |
| Maximize use of "buddy" system during all travel | _____ |
| Vary daily departure/arrival times, routes and modes of travel | _____ |
| If at TDY location for extended period, consider switching hotel locations | _____ |
| * Use non-tactical armored car support | _____ |
| * Travel with armed escort | _____ |
| * Arrange for local counter surveillance support | _____ |
| ** Have available firearms for personal protection | _____ |
| ** Issue and carry firearms for personal protection | _____ |

* These measures normally are only associated with High Risk Personnel who warrant protective services support.

** These measures would only be authorized for critical missions in extremely hazardous locations with the approval of both Combatant Commander and the COM.

PART IV. OBJECTIVE: FINALIZE ARRANGEMENTS FOR TDY AND BUILD A PLAN BASED ON THE FOLLOWING KEY ELEMENTS. Documentation could amount to nothing more than wallets size cards with contact numbers if a clear understanding of procedures is established.

11. Make final Risk assessment and "Go" – "No Go" decision based on introduction of mitigating measures in PART III.

12. Confirm that all travelers have documented evidence of Level I AT training within the time limits prescribed.

13. Increase the situational awareness of all travelers by reviewing results of PARTS I, II and III, above, prior to mission execution.

14. Ensure all travelers have key contact numbers and understand all ground rules and AT procedures for the mission. Wallet size cards may suffice.

15. If appropriate, identify divert locations for the mission and alternate local POC information. Ensure communications capability exists to notify home office and primary POC if mission must be diverted.

16. Initiate notifications/requests IAW the FCG. Message request must follow exact format specified, and include a request for Country/Theater Clearance granting authority to identify precisely and explicitly who (Combatant Commander or COM) has responsibility and TACON for force protection of all travelers. Include as the last paragraphs in the message any additional AT measures instituted and results of risk assessment if required or appropriate. Explicitly state that Level I AT training has or shall be completed prior to mission execution.

17. Once all travel clearances have been obtained, continue to update itineraries with local AT POCs and clearance granting authorities. Conduct ongoing mission analysis and risk assessment until execution and completion of mission.

NOTE: Mitigating measures to reduce Risk are not limited to those listed in PART III, above, and application of additional innovative measures to enhance security are encouraged. Authority to grant travel clearance to some areas is severely restricted and may require forwarding the travel proposal to the appropriate Combatant Commander for review/approval.

AP6.3.4. A detailed and complete example of an AT security plan in OPORD format can be found in the Force Protection section of EUCOM's secure SIPRNET web site.

AP6.4. COORDINATING INSTRUCTIONS

AP6.4.1. Every deployment should be provided with a focused, tailored AT Threat Assessment (see chapter 5) that reflects the most up to date threat information and the impact on the threat environment of raising the profile of U.S. personnel due to the deployment. A generic threat assessment may change once the increased presence of U.S. forces on the ground is factored in. This AT TA is a stand-alone product that should include information similar to that gathered for the Risk Management Process.

AP6.4.2. The supporting intelligence center/element must coordinate for additional collection emphasis for certain deployments. This shall ensure additional collection is dedicated to meeting the AT needs of deploying and in transit forces.

AP6.4.3. As applicable, the Commanders also shall ensure compliance with AT Pre-Deployment and AT Training and Equipment Requirements established in reference (e).

# AP7. APPENDIX 7
# TERRORIST SURVEILLANCE DETECTION

## AP7.1. INTRODUCTION

AP7.1.1. This appendix provides guidance for Commanders and ATOs to stress the importance of overt terrorist surveillance detection efforts by military police forces to deter terrorist surveillance activities.

AP7.1.2. The recent increase in reporting of suspicious individuals conducting surveillance of U.S. military and civilian sites in the United States and overseas indicates possible pre-operational targeting by terrorists and merits attention by Commanders at all levels. The persistent stream of reports necessitates Commanders and security planners to understand the purpose of terrorist surveillance, know what terrorists look for, and know how they conduct surveillance operations. With this basic knowledge, Commanders can then implement protective countermeasures, comply with DoD standardized reporting procedures, and in the end deter, detect, disrupt, and defend against future terrorist attacks.

## AP7.2. TERRORIST SURVEILLANCE

AP7.2.1. Vulnerability Assessment. Terrorists conduct surveillance to determine a target's suitability for attack by assessing the capabilities of existing security systems and discerning weaknesses for potential exploitation. Terrorists closely examine security procedures, such as shift changes, access control, and roving patrols; citizenship of security guards; models and types of locks; presence of closed-circuit cameras; and guard dogs. After identifying weaknesses, terrorists plan their attack options at the point or points of greatest vulnerability.

AP7.2.2. Terrorist Surveillance Techniques. The basic methods of surveillance are "mobile" and "fixed" (or static).

AP7.2.2.1. Mobile surveillance entails active participation by the terrorists or operatives conducting surveillance, usually following as the target moves. Terrorists conduct mobile surveillance on foot, in a vehicle, or by combining the two. Mobile surveillance usually progresses in phases from a stakeout, to a pick up and then through a follow phase until the target stops. At this point operatives are positioned to cover logical routes to enable the surveillance to continue when the target moves again.

AP7.2.2.2. Terrorists conduct fixed or static surveillance from one location to observe a target, whether a person, building, facility, or installation. Fixed surveillance often requires the use of an observation point to maintain constant, discreet observation of a specific location. Terrorists establish observation posts in houses, apartments, offices, stores, or on the street. A mobile surveillance unit, such as a parked car or van, can also serve as an observation post. Terrorists often park outside a building, facility, or installation to observe routines of security and personnel coming and going. Terrorists also use various modes of transportation to include buses, trains or boats or move by foot to approach and observe installations.

AP7.2.3. Protective Countermeasures.

AP7.2.3.1. The incorporation of visible security cameras, motion sensors, working dog teams, random roving security patrols (varying size, timing, and routes), irregular guard changes, and active searches (including x-ray machines and explosive detection devices) of vehicles and persons at entry points shall improve a facilities' situational awareness and present a robust force protection posture that dramatically inhibits terrorist surveillance efforts.

AP7.2.3.2. The emplacement of barriers, roadblocks, and entry mazes that are covered by alert security forces shall provide additional deterrence as these measures increase standoff and improve security force reaction time in the event of an attack.

AP7.2.3.3. The implementation of unannounced random security measures such as 100 percent identification of all personnel entering the facility or installation, conducting inspections and searches of personnel and vehicles, and visible displays of vehicles mounted with crew served weapons shall increase uncertainty and thus the risk of failure in the minds of terrorists.

AP7.2.4. Surveillance Detection. Because terrorists must conduct surveillance - often over a period of weeks, months, or years – detection of their activities is possible. Regardless of the level of expertise, terrorists invariably commit mistakes. Knowing what to look for and being able to distinguish the ordinary from the extraordinary are keys to successful surveillance detection. For these reasons, overt surveillance detection in its most basic form is simply watching for persons observing personnel, facilities, and installations.

AP7.2.4.1. The objectives of overt surveillance detection measures are to record the activities of persons behaving in a suspicious manner and to provide this information in a format useable by the appropriate law enforcement or intelligence officials. It is important to note that overt surveillance detection emphasizes the avoidance of interpersonal confrontations with suspicious individuals unless exigent situations necessitate otherwise. Depending upon the

circumstances or trends, Commanders and senior law enforcement officials in coordination with intelligence experts through installation threat working groups may determine the need for more specialized covert countersurveillance measures to assure installation protection.

AP7.2.4.2. For surveillance detection efforts to achieve positive results, military police/security forces should immediately report incidents of surveillance and suspicious activities by providing detailed descriptions of the people, the times of day, the locations, the vehicles involved, and the circumstances of the sightings to their respective criminal investigative services or counterintelligence elements for incorporation into reports such as U.S.A.F. TALON or the NCIS Suspicious Incident Report. The incident reports are important pieces of information that over time combined with other similar sightings allow investigators to assess the level of threat against a specific facility, installation, or geographic region.

AP7.2.4.3. The emphasis of surveillance detection is on indicators and warnings of terrorist surveillance activities. Surveillance detection efforts should focus on recording, then reporting incidents similar to the following:

AP7.2.4.3.1. Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction.

AP7.2.4.3.2. Possible locations for observation post use.

AP7.2.4.3.3. Individuals who stay at bus and/or train stops for extended periods while buses/trains come and go.

AP7.2.4.3.4. Individuals who carry on long conversations on pay or cellular telephones.

AP7.2.4.3.5. Individuals who order food at a restaurant and leave before the food arrives or who order without eating.

AP7.2.4.3.6. Joggers who stand and stretch for an inordinate amount of time.

AP7.2.4.3.7. Individuals sitting in a parked car for an extended period of time.

AP7.2.4.3.8. Individuals who don’t fit into the surrounding environment by wearing improper attire for the location (or season).

AP7.2.4.3.9. Individuals drawing pictures and/or taking notes in an area not normally of interest to a standard tourist or showing interest in or photographing security cameras, guard locations, or noticeably watching security reaction drills and procedures.

AP7.2.4.3.10. Individuals who exhibit unusual behavior such as staring or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas.

AP7.2.4.3.11. Terrorists may also employ aggressive surveillance by false phone threats, approaching security checkpoints to ask for directions or "innocently" attempting to smuggle non-lethal contraband through checkpoints. Clearly the terrorists intend to determine firsthand the effectiveness of search procedures and to gauge the alertness and reaction of security personnel.

AP7.2.4.4. It is important to highlight that the above surveillance indicators are recorded overtly and while performing normal military police/security forces activities. The intent is to raise the awareness of our military police/security forces to record and report the unusual during the course of routine law enforcement and security duties.

AP7.2.5. Reporting Terrorist Surveillance Indicators. Implementing effective security countermeasures and employing overt surveillance detection principles shall deter terrorist surveillance. However, regardless of the capabilities of a facility or installation to resource antiterrorism protective measures, good working relationships with local, State, and Federal law enforcement agencies are essential to establishing cohesive, timely and effective responses to the indicators of terrorist activity.

AP7.2.5.1 Installation Commanders and senior law enforcement officials should coordinate and establish partnerships with local authorities (i.e. installation threat working groups) to develop intelligence and information sharing relationships to improve security for the installation and the military community at large.

AP7.2.5.2. For those occasions when the indicators of terrorist surveillance continue despite well executed overt security countermeasures the objectives should be to provide detailed reports of the indicators of surveillance to the appropriate law enforcement agency or intelligence activity. As reports of suspicious activity increase and the trends clearly indicate pre-operational terrorist surveillance, it may be necessary for installation Commanders in coordination with senior law enforcement and intelligence officials to implement more sophisticated, uniquely tailored countersurveillance solutions and assets to investigate the circumstances.

AP7.2.5.3. Specialized countersurveillance assets should be coordinated and vetted by forwarding requests through the chain of command via pre-determined service or combatant command request procedures.

# AP8. APPENDIX 8
# ANTITERRORISM (AT) SECURITY CONSIDERATIONS FOR THE CONTRACTING PROCESS

## AP8.1. INTRODUCTION

AP8.1.1. Contracting for support services is a normal, ever expanding function of providing essential logistical services within the Department of Defense. Contracting for services present AT security challenges (which if not addressed) could create seams and gaps in a unit's overall security profile. The Federal Acquisition Regulations (FAR) (reference (ay)) is the principle guidance used to establish Federal Government contracts and provides explicit directions for contract requirements, award, execution, and evaluation. At OCONUS locations, SOFA, MOA, and other documents shall prescribe guidance for the contracting process with regard to host nation service providers. ATOs should work closely with the contracting officer and the legal officer to ensure AT security considerations are properly and legally incorporated into the contracting process. Each Combatant Commander should consider developing AOR and/or country specific, AT security guidance for the contract process based on their individual threat concerns and agreements with host nations.

AP8.1.2. Reference (aw) does not specifically prohibit or prescribe AT security considerations for contracts. It is the responsibility of the commander to incorporate AT security considerations into the contracting process. This appendix shall offer an AT process that can be used to incorporate AT security considerations into the contracting process. It also suggests specific AT security measures that can be employed.

## AP8.2. INCORPORATING AT SECURITY CONSIDERATIONS INTO THE CONTRACTING PROCESS

AP8.2.1. Commanders are responsible for ensuring AT security measures are included into the contracting process. Each commander should develop area specific, AT security guidance and incorporate the same into their AT program. This Commander's guidance forms the core AT security criteria that shall be applied to all contracts as a baseline. Contract AT security considerations should be considered during the commander's AT risk assessment process. This process results in the acceptance of a level of AT risk and parameters; or in the investment of additional AT security costs.

AP8.2.2. The ATO and the contracting officer are responsible for ensuring the application of the Commander's guidance. This ensures AT security measures are included into the statement of work (SOW) and if applicable, the DD Form 254, }Contract Security Classification Specification." It is the contracting officer's responsibility to ensure the contract is prepared IAW appropriate contracting regulations/guidance. It is important to include the AT working group and host nation representatives as required throughout this process. Listed below is a step-by-step process for considering AT security into contracts. Table AP8.T1 also outlines the process for incorporating AT security considerations into the logistics contract process.

AP8.2.2.1. Determine the Contract Requirement. The unit requiring the contract service is responsible for identifying the specific contract requirement. The unit shall work with the contracting officer to ensure the framework of the contract/scope of work is properly constructed. This is done within the Department of Defense, Service, Combatant Commander, FAR, and contracting guidance. It is at this step that the unit should determine how essential this contract service is to mission accomplishment. Are there alternative means to providing the contract service without mission degradation? It is important to determine the scope of the contract, who shall execute the contract, what unit (s) shall be affected by it, when it shall be executed (timeframe), where it shall be executed, and what the area/building access requirements are. The concern during this step is to determine the specific logistics requirement (s), not determining AT security considerations.

AP8.2.2.2. Conduct AT RA. The unit shall conduct an AT risk management process using locally prepared AT assessments (Threat, Criticality, Vulnerability, and Risk). The use of these products shall help the unit in assessing and identifying the potential AT risks associated with the contract and the incorporation of specific AT security countermeasures. Part of this process is to consider alternative means of fulfilling the contract requirement as a means to mitigate or eliminate risks. The ATO shall assist in the AT risk management process; ensuring local security measures are leveraged and/or modified against risks/vulnerabilities associated with the contract.

AP8.2.2.3. Determine AT Security Requirements. During this step, the ATO shall assist the unit in the development of specific AT security measures. AT security measures should be based on an AT RA and reflect the Commander's overall AT risk management strategy. There should be a balance between effective security measures and cost-benefit. The unit and the ATO should apply the Commander's AT security considerations during this step. The ATO should craft AT security strategies that complement the existing security profile of the location from a normal security posture through advanced readiness postures. Flexibility should be incorporated into the contract to allow for random schedules, access and/or search requirements, and changes in the local threat. For example, contractor personnel may be directed to enter the location through certain access points where they can best be identified and searched. Contractor personnel may be prohibited from certain portions of the location and during advanced readiness postures. Contract services may be curtailed or more closely supervised.

**Table AP8.T1 Process for Considering AT Security Measures into Contracts**

| Step | Major Tasks | OPR |
|---|---|---|
| Determine Contract Requirements | - Determine contract support requirement.<br>- Comply with applicable DoD and Service FAR guidance and Combatant Commander contracting guidance.<br>- Determine scope of contract. | Unit and Contracting Officers |
| Perform AT Risk Analysis | - Conduct AT risk analysis.<br>- Leverage local risk analysis information.<br>- Determine risks associated with contract.<br>- Develop logistics alternatives…balanced with mission accomplishment. | Unit and AT Officer |
| Determine AT Security Measures | - Develop specific AT security measures.<br>- Leverage and/or modify security measures.<br>- Develop range of security measures…normal through advanced readiness postures.<br>- Include AT security requirements in SOW and DD Form 254.<br>- Consider linkage with local FPCON system.<br>- Balance between security and cost-benefit. | AT Officer and Unit |
| Build Contract | - Incorporate contract requirement(s) and security measures into written contract.<br>- Staff contract.<br>- Commander endorsement of security measures and acceptance of risk. | Unit and Contracting Officer |

| Step | Major Tasks | OPR |
|---|---|---|
| Award/Execute Contract | - Select and screen contractors.<br>- Incorporate contract security requirements into unit AT/FP plan.<br>- Notify ATO contract is activated.<br>- Ensure all AT security measures are in place before execution. | Unit and Contracting Officer/AT Officer |
| Contract Review | - Periodically inspect AT security measures.<br>- Review AT security measures should local threat change.<br>- Annual, formal review upon contract renewal. | Unit and Contracting Officer |

Table AP8.T2 below identifies some of the specific AT security measures that should be considered for the logistics contract process.

AP8.2.2.4. Build Contract. This step involves combining the logistics requirement (s) with the AT security measure (s) into a written contract. As a minimum, the contract should be staffed through the AT Working Group, the legal officer, and the Commander. This is the Commander's formal endorsement that the AT security measures are satisfactory and he or she has accepted the AT risk.

AP8.2.2.5. Award/Execute Contract. The unit should consider including contract security requirements as part of their unit's AT Plan to ensure proper coordination and synchronization with other AT activities. Once the contract is awarded, those security requirements become binding and should be in place. Any contractor personnel screening requirements should be met prior to starting the contract. The contracting officer and the unit should notify the ATO prior to the contract services starting so he can ensure all required AT security measures are in place.

AP8.2.2.6. Contract Review. The unit should establish procedures to periodically review the effectiveness of the contract, both in terms of services rendered and AT security measures in place. Contract reviews should all be the day-to-day inspection/evaluation of services rendered, periodic inspection of access controls to ensure control procedures are not being abused, and a formal annual review process to renew or cancel the contract. A contract review should also be done if the local threat changes and/or there is a requirement to modify and renegotiate the terms of the contract.

**Table AP8.T2 AT Security Measures for Logistics Contracts**

| AT Security Area | AT Security Measure |
|---|---|
| Contractor Screening | - Pre-approved, reputable companies vetted through contracting office, Chief of Mission, DoD.<br>- Consider limiting the announcement for contractors to trusted sources based on sensitivity of the mission.<br>- Background Check (Law Enforcement, Host Nation).<br>- Screen company and prospective workers. |
| Access Control | - Defined process for replacement of workers.<br>- Establish a central contractor database that is accessible to security forces and contains contractor ID with picture.<br>- Limit work area. Clearly identify restricted/exclusion areas where contractor personnel are not authorized without specific permission or an escort.<br>- Access control roster (personnel and vehicles). Names/vehicles verified by the company and received background screening, and/or host nation certification. Substitutes receive same vetting process prior to work.<br>- Badge systems.<br>- Exchange badge system.<br>- Personal identification systems i.e., work uniform, vehicle marking.<br>- Biometrics systems i.e., fingerprint, retinal, facial feature reading device.<br>- Have large vehicles arrive empty before entering location i.e., trash trucks.<br>- Arranging vehicle loads to facilitate searching.<br>- Verify contents of large vehicles at distribution point and/or using an electronic vehicle-screening device.<br>- Consider an alternate access control point for screening/search contractor personnel and vehicle. Especially oversize vehicles.<br>- Consider an unloading zone away from protected assets. |

| AT Security Area | AT Security Measure |
|---|---|
| | - Ensure host nation language translation support.<br>- Coordinate host nation security requirements. |
| Circulation Control | - Designate authorized work areas and travel routes.<br>- Provide easily identifiable coding for badges and vehicle.<br>- Assign a unit escort (armed as required) to the contractor.<br>- Deny access during increased readiness conditions. |
| Special Security Concerns | - Include contract services as part of the local risk analysis/management process.<br>- Ensure AT security measures already in place are leveraged/complemented.<br>- Consider all possible alternatives to fulfilling the required service. Is the service really required to accomplish the mission?<br>- Consider time and space factors to allow determination of hostile intent into AT security measures.<br>- Consider incorporating contractor security measures into the local FPCON system.<br>- Monitor contractor (s) at the work-site as required by security environment.<br>- Review contracts annually or when the local threat changes.<br>- Establish food and/or water testing protocols.<br>- Identify and monitor food, water, and petroleum distribution points (on and off location).<br>- Ensure delivery schedules are random and unpredictable.<br>- Consider periodic interviews of contractors by security force personnel.<br>- Provide contractor training and procedures for reporting suspicious activity and/or stolen equipment.<br>- Determine what risks still remain after all AT security measures are applied...acceptance of risk. |

| AT Security Area | AT Security Measure |
|---|---|
| | - Conduct frequent, random patrols, inspections, and spot-checks.<br>- Establish a security response force.<br>- Ensure host nation agreements allow for adequate AT security considerations during the logistics contracting process. |

# AP9. APPENDIX 9
# IMPORTANT INTERNET LINKS

The far-reaching capability of the Internet, or World-Wide-Web, makes it an invaluable source for additional information. Table AP9.T1. below provides suggested links for unclassified (NIPRNET) platforms.

**Table AP9.T1. NIPRNET (Non-secure Internet Protocol Relay Network**

| MILITARY | |
|---|---|
| DefenseLINK | http://www.defenselink.mil/ |
| Defense Threat Reduction Agency (DTRA) | http://www.dtra.mil/ |
| Office of the Inspector General of the Department of Defense (OIG DoD) | http://www.dodig.osd.mil |
| OIG Defense Criminal Investigative Service (DCIS) | http://www.dodig.osd.mil/INV/DCIS/index.html |
| Joint Center for Lessons Learned | http://deploymentlink.osd.mil/lessons_learned/jc_ll.shtml / |
| Joint Electronic Library | http://www.dtic.mil/doctrine/index.html/ |
| Joint Chiefs of Staff | http://www.dtic.mil/jcs/ |
| DD AT/HD | http://www.dtic.mil/jcs/force_protection/main.html |
| National Guard Bureau | http://www.ngb.army.mil/ |
| Washington Headquarters Services, Directives and Records Branch | http://www.dtic.mil/whs/directives/ |
| Unified Commands | |
| U.S. Central Command (CENTCOM) | http://www.centcom.mil/ |
| U.S. European Command (EUCOM) | http://www.eucom.mil/ |
| U.S. Joint Forces Command (JFCOM) | http://www.jfcom.mil/ |
| U.S. Northern Command (NORTHCOM) | http://www.northcom.mil/ |
| U.S. Pacific Command (PACOM) | http://www.pacom.mil/ |
| U.S. Special Operations Command (SOCOM) | http://www.socom.mil/ |
| U.S. Southern Command (SOUTHCOM) | http://www.southcom.mil/home/index.cfm/ |
| U.S. Strategic Command (STRATCOM) | http://www.stratcom.af.mil/ |
| U.S. Transportation Command (TRANSCOM) | http://www.transcom.mil/ |
| **Services** | |
| Army | http://www.army.mil/ |
| Center for Army Lessons Learned | http://call.army.mil/ |
| U.S. Army Soldier and Biological Chemical Command (SBCCOM) | http://www.sbccom.army.mil/ |
| U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) Publications | http://www.usamriid.army.mil/publications/ |
| U.S. Army Center for Health Promotion & Preventive Medicine, Biological Threats | http://chppm-www.apgea.army.mil/BiologicalThreats/ |
| U.S. Army Center for Health Promotion & Preventive Medicine, Checking Suspicious Mail | http://chppm-www.apgea.army.mil/homelandsecurity/suspiciousmail.pdf/ |
| Air Force | http://www.af.mil/ |
| Air Force Center for Lessons Learned | https://afknowledge.langley.af.mil/afcks/default.asp/ |
| Air Force Office of Special Investigations (AFOSI) | http://www.dtic.mil/afosi/ |
| USAF Battlelabs | http://www.xo.hq.af.mil/afbattlelab/ |
| USAF Security Forces | http://afsf.lackland.af.mil/ |

| MILITARY | |
|---|---|
| Navy | http://www.navy.mil/ |
| Naval Criminal Investigative Service (NCIS) | http://www.ncis.navy.mil/ |
| Navy Lessons Learned System | http://www.nwdc.navy.mil/nlls/default.asp/ |
| Navy FP/PSE | https://dodpse.spawar.navy.mil |
| Marine Corps | http://www.usmc.mil/ |
| Marine Corps Lessons Learned System | http://www.doctrine.quantico.usmc.mil/ |
| Coast Guard | http://www.uscg.mil/ |
| Coast Guard Office of Law Enforcement | http://www.uscg.mil/hq/g-o/g-opl/mle/welcome.htm/ |

| GOVERNMENT | |
|---|---|
| CDC -- Center for Disease Control, Public Health Emergency Preparedness and Response | http://www.bt.cdc.gov/ |
| CIA -- Central Intelligence Agency | http://www.odci.gov/ |
| DHS – Department of Homeland Security | http://www.dhs.gov/ |
| DHS Emergencies and Disasters | http://www.dhs.gov/dhspublic/theme_home2.jsp/ |
| DOJ -- Department of Justice | http://www.usdoj.gov/ |
| Federal Bureau of Investigation | http://www.fbi.gov/ |
| DOS -- Department of State | http://www.state.gov/ |
| Office of the Coordinator for Counterterrorism | http://www.state.gov/s/ct/ |
| Bureau of Diplomatic Security | http://www.ds.state.gov/index.htm/ |
| Travel Warnings and Consular Information Sheets | http://travel.state.gov/travel_warnings.html/ |
| Response to Terrorism | http://usinfo.state.gov/topical/pol/terror/ |
| EPA -- Environmental Protection Agency | http://www.epa.gov/ |
| Chemical Emergency Preparedness Office | http://www.epa.gov/ceppo/ |
| FEMA -- Federal Emergency Management Agency | http://www.fema.gov/ |
| Federal Response Plan | http://www.fema.gov/rrr/frp/ |
| Disaster Preparedness (Fact Sheets) | http://www.fema.gov/library/factshts.shtm/ |
| Treasury Department | http://www.treas.gov/ |
| Office of Foreign Assets Control | http://www.treas.gov/offices/enforcement/ofac/ |
| Abbreviations and Acronyms of the U.S. Government | http://www.ulib.iupui.edu/subjectareas/gov/docs_abbrev.html/ |

| REFERENCES | |
|---|---|
| Acronym Finder | http://www.acronymfinder.com/ |
| Army Acronyms | http://www.army.mil/aps/97/acro.htm/ |
| CIA Factbook | http://www.odci.gov/cia/publications/factbook/index.html/ |
| CIA Maps | http://www.odci.gov/cia/publications/factbook/docs/refmaps.html/ |
| Dictionary.com | http://dictionary.com/ |
| DoD Dictionary of Military Terms | http://www.dtic.mil/doctrine/jel/doddict/index.html/ |
| FirstGov | http://firstgov.gov/ |
| GovSpot | http://www.govspot.com/ |
| Joint Acronyms and Abbreviations | http://www.dtic.mil/doctrine/jel/doddict/acronym_index.html/ |
| US Armed Forces Abbreviations | http://www.globemaster.de/html/dictionary.html/ |

| REFERENCES | |
|---|---|
| Navy Acronyms and Abbreviations | https://www.cnet.navy.mil/netpdtc/acronyms.htm/ |
| The Reference Desk | http://www.refdesk.com/ |
| Thesaurus.com | http://thesaurus.com/ |
| The Weather Channel | http://www.weather.com/ |

| TECHNOLOGY | |
|---|---|
| Military | |
| Defense Technical Information Center | http://www.dtic.mil/ |
| DoD Joint Non-Lethal Program Office | http://www.jnlwd.usmc.mil/ |
| U.S. Air Force, Electronic System Center, Force Protection | http://esc.hanscom.af.mil/default.asp/ |
| U.S. Army Corps of Engineers – Protective Design Center | https://pdmcx.pecp1.now.usace.army.mil/index2.html/ |
| U.S. Army Program Manager, Physical Security Equipment | http://www.pmpse.org/ |
| SPAWAR Charleston | http://sscc.spawar.navy.mil/ |
| Government | |
| Extranet for Security Professionals | http://isp.hpc.org/ |
| National Institute of Standards and Technology | http://www.nist.gov/ |
| National Institute of Standards and Technology - Computer Resource | http://csrc.nist.gov/ |
| National Institute of Standards and Technology Rainbow Series | http://csrc.ncsl.nist.gov/secpubs/rainbow/ |
| Technical Support Working Group | http://www.tswg.gov/ |
| Commercial | |
| American Society for Industrial Security | http://www.asisonline.org/ |
| CardTech/SecurTech | http://www.ct-ctst.com/ |
| Delta Scientific | http://www.deltascientific.com/ |
| National Institute of Justice | http://www.nlectc.org/ |
| Security Products Magazine | http://www.secprodonline.com/ |
| Terrorism Research Center | http://www.terrorism.com/ |

# AP10. APPENDIX 10
# FAMILY SECURITY QUESTIONS

## AP10.1. INTRODUCTION

The following are questions that can be asked to help identify practices that may increase the likelihood that a DoD person or dependent shall become a victim of a kidnapping or other terrorist act.

## AP10.2. HEAD OF HOUSEHOLD

AP10.2.1. Is your telephone number and address in local directories?

AP10.2.2. Do you, your family members, or your domestic employees answer your telephone with your name and rank?

AP10.2.3. Have you had a security check run on all domestic employees? If overseas, did you check with the MILGROUP and/or Embassy Regional Security Officer to see if they have any program to help screen prospective employees' records? If not, contact the local military police/counterintelligence office or local police to obtain pre-employment screening assistance.

AP10.2.4. Have you maintained a file on each household employee including the full name, address, description, date and place of birth, current photograph and a full set of fingerprints (if allowed, host nation laws may prohibit the collection of some data on local nationals, i.e. fingerprints)?

AP10.2.5. Have outside fuse boxes/circuit breakers been modified so they can be locked at all times unless access is specifically required?

## AP10.3. FAMILY

AP10.3.1. Have you adopted a family security program including duress codes and alarms, crime watch practices, and conscious efforts to avoid patterns in daily activities?

AP10.3.2. Have all family members learned emergency telephone numbers? Have they been able to memorize them? Do all family members know how to summon police in the local language? Are they aware or do they carry instructions in wallet cards on how to work local telephones and ask for assistance?

AP10.3.3. Have emergency numbers been posted near each telephone? Do these listings give away the nature of the family's assignment (Ambassador's home phone should not be listed,

etc.) Have all family members been given a sanitized list of phone numbers they can carry with them at all times?

AP10.3.4. Do you have a system for keeping family members informed about each other's whereabouts at all times? Have you included a family duress or trouble signal as part of your family check-in system?

AP10.3.5. Have you removed all symbols or signs from the outside of your residence indicating nationality, rank or grade, title, and name?

AP10.3.6. Have you unnecessarily disseminated personal, family, and travel plans to casual acquaintances or domestic employees who do not need to know your personal schedule on an hourly or daily basis?

AP10.3.7. Have you learned and practiced emergency phrases in the local language such as "I need a policeman, a doctor, help, etc."? Have you written these down in transliteration as well as in the native language so you could show a 3 x 5 card to obtain assistance?

AP10.3.8. Do you and your family members know how to work local pay telephones? Does each family member carry a small quantity of money or phone cards necessary and sufficient to operate local pay telephones at all times? Alternatively, do family members carry cell phones?

AP10.3.9. Are residence doors and windows locked? Have additional security devices been added to door and window locks to increase resistance to intrusion and penetration?

AP10.3.10. Do you and your family members close draperies during periods of darkness? Are the draperies made of opaque, heavy material that provides maximum privacy (and can reduce the distribution of glass shards in the event windows are broken).

AP10.3.11. Have you considered obtaining a dog for protection of your house and grounds?

AP10.3.12. Do you avoid leaving a spare key in the mailbox or in a similar insecure place?

AP10.3.13. Are tools used by the family, particularly ladders, under lock?

AP10.3.14. Do you have a private place to leave notes for family members or do you tack notes on the door for family, friends, criminals, and terrorists to read?

AP10.3.15. Have you developed a response plan for yourself and family members in the event that an unauthorized person is suspected to be inside your home upon your return? Does your plan emphasize the need to contact the police or the security office immediately and discourage personal investigation of the possible intrusion?

AP10.3.16. Do you or family members automatically open the residence door to strangers? Do you or your family members use a peephole or CCTC monitor to identify callers? Do you request to see and verify credentials from utility, service, or other persons seeking to enter your residence?

AP10.3.17. Do you or your family members admit polltakers and salespersons to your home? Are you aware of the presence of peddlers and all strangers in your neighborhood? Are your family members equally aware? (Terrorists are known to have gathered substantial information relative to their victims using these deceptions.)

AP10.3.18. Have you and your family members reported frequent wrong numbers or nuisance telephone calls to the telephone company and the police? Have you considered that someone may be attempting to determine the presence of family members?

AP10.3.19. Have you reported the presence of strangers in the neighborhood? Does it appear that someone or some group may be trying to gain an intimate knowledge of your family's habits?

AP10.3.20. Do you and your family members watch for strange cars cruising or parked frequently in the area, particularly if one or more occupants remain in the car for extended periods? Have you made a note of occupants, license numbers and province designators of suspicious vehicles?

AP10.3.21. Do you discuss family activities with strangers?

AP10.3.22. Do you discuss family plans over the telephone?

AP10.3.23. Do you discuss detailed family or office plans over the telephone with people you do not personally know or know well?

AP10.3.24. Do you mail letters concerning family travel plans from your house or office? Are you sure that no one is intercepting your outbound mail, opening it, and then resealing it for delivery after collecting desired information enclosed in it?

AP10.3.25. Have you or family members accepted delivery of unordered or suspicious packages or letters?

AP10.3.26. Do you destroy all envelopes papers and other items that reflect your name, rank, SSN and other sensitive information?

AP10.3.27. Have you limited publicity concerning yourself and your family, which may appear in local news media?

AP10.3.28. Do you and your family shop on a set schedule? Do you and your family members always shop at the same stores? Do you and your family members always use the same routes to the office, to shopping, to school, and to after school activities?

AP10.3.29. Do you have a coordinated family emergency plan? Have you ensured that all family members know who to contact if they suspect another family member is in danger? Have you reviewed protective measures with all family members?

AP10.3.30. Have you made sure that each family member is prepared to evacuate the area quickly in the event of an emergency? Do you know where all critical documents such as passports, visas, shot and other medical records are kept? Are these current, and can you or other family members extract them from their secure storage place on very short notice?

AP10.3.31. Do you find yourself in disputes with citizens of the host country over traffic, commercial transactions, or other subjects? Have you or your family members precipitated any incidents involving host country nationals?

AP10.4. CHILDREN

AP10.4.1. Have the children been instructed not only to refuse rides from strangers, but also to stay out of reach if a stranger in a car approaches them?

AP10.4.2. Have you located the children's rooms in a part of the residence that is not easily accessible from the outside?

AP10.4.3. Do you ever leave your children at home alone or unattended?

AP104.4. Are you sure that the person with whom you leave your children is responsible and trustworthy?

AP10.4.5. Are you sure that outside doors and windows leading into the children's rooms are kept locked, especially in the evening?

AP10.4.6. Have you taught your children the following?

AP10.4.6.1. Never let strangers into your house.

AP10.4.6.2. Avoid strangers and never accept rides from anyone that he/she does not know.

AP10.4.6.3. Refuse gifts from strangers.

AP10.4.6.4. Never leave home without telling an adult where and with whom you are going.

AP10.4.6.5. How to call the police.

AP10.4.6.6. To call the police if ever you are away and they see a stranger around the house.

AP10.4.6.7. Whenever possible, walk on main thoroughfares.

AP10.4.6.8. Tell you if he or she notices a stranger hanging around your neighborhood.

AP10.4.6.9. Play in established community playgrounds rather than in isolated areas.

AP10.4.6.10. Give a false name if ever asked by a stranger.

AP10.5. SCHOOLS

AP10.5.1. Have you asked schools attended by your children to:

AP10.5.1.1. Not give out any information on your students to anyone unless you specifically authorize them to do so in advance? To avoid any kind of publicity in which students are named or their pictures are shown.

AP10.5.1.2. Not to release a student to someone other than his/her parents without first receiving authorization from a parent.

AP10.5.1.3. To allow children to talk to a parent on the telephone in the presence of school officials before allowing an authorized release to actually occur. (This practice provides protection against a kidnapper who calls and claims to be the child's parent.)

AP10.5.1.4. To report to the police if any strangers are seen loitering around the school or talking to students. If such strangers are in a car, the teacher should note its make, color, model, and tag number and pass this information on to the police.

AP10.5.1.5. To have teachers closely supervise outside play periods.

AP10.6. NEIGHBORS

AP10.6.1. Have you met your neighbors? Have you gotten them interested in maintaining and improving neighborhood security?

AP10.6.2. Have you exchanged telephone numbers?

AP10.6.3. Have you established some sort of system for alerting one another to trouble in neighborhood?

AP10.7. STRANGERS

AP10.7.1. Have all family members and domestic employees been instructed on the requirement that maintenance work is to be performed only when scheduled by a parent unless a clear emergency exists? Do you have procedures established on how to be contacted in the event that a utility emergency occurs and maintenance personnel must enter your residence? Do your family members and domestic employees know how to verify the identity of maintenance personnel?

AP10.7.2. Have you and your family discussed the kind of assistance you can offer to a person who comes to your door claiming to be the victim of an automobile accident, a mechanical breakdown, or some other kind of accident? Have you explained to your family they can offer to call the police, the fire department, or an ambulance, but under no circumstances should they allow the victim into the residence?

# AP11. APPENDIX 11
# HOUSEHOLD SECURITY CHECKLIST

## AP11.1. INTRODUCTION

AP11.1.1. This generic household checklist should be used to evaluate current and prospective residences when a locally specific checklist is not available. Prospective renters should attempt to negotiate security upgrades as part of the lease contract when and where appropriate. This could reduce costs to the DoD member by amortizing costs over period of the lease.

| AP11.2. EXTERIOR HOUSEHOLD SECURITY LIST | Yes | No |
|---|---|---|
| AP11.2.1. If you have a fence or tight hedge, have you evaluated it as a defense against intrusion? | _____ | _____ |
| AP11.2.2. Is your fence or wall in good repair? | _____ | _____ |
| AP11.2.3. Are the gates solid and in good repair? | _____ | _____ |
| AP11.2.4. Are the gates properly locked during the day and at night? | _____ | _____ |
| AP11.2.5. Do you check regularly to see that your gates are locked? | _____ | _____ |
| AP11.2.6. Have you eliminated trees, poles, ladders, boxes, etc., that might help an intruder to scale the fence, wall, or hedge? | _____ | _____ |
| AP11.2.7. Have you removed shrubbery near your gate, garage, or front door, which could conceal an intruder? | _____ | _____ |
| AP11.2.8. Do you have lights to illuminate all sides of your residence, garage area, patio, etc.? | _____ | _____ |
| AP11.2.9. Do you leave your lights on during hours of darkness? | _____ | _____ |
| AP11.2.10. Do you check regularly to see that the lights are working? | _____ | _____ |
| AP11.2.11. If you have a guard, does his post properly position him to have the best possible view of your grounds and residence? | _____ | _____ |
| AP11.2.12. Does your guard patrol your grounds during the hours of darkness? | _____ | _____ |

AP11.2.13. Has your guard been given verbal or written instructions, does he understand them? _____ _____

AP11.2.14. Do you have dogs or other pets that will sound an alarm if they spot an intruder? _____ _____

AP11.2.15. Have you considered installation of a camera system with record capabilities or dummy camera system as a deterrent? _____ _____

AP11.3. INTERIOR HOUSEHOLD SECURITY LIST Yes No

AP11.3.1. Are your perimeter doors made of metal or solid wood? _____ _____

AP11.3.2. Are the doorframes of good solid construction? _____ _____

AP11.3.3. Do you have an interview grill or optical viewer in your main entrance door? _____ _____

AP11.3.4. Do you use the interview grill or optical viewer? _____ _____

AP11.3.5. Are your perimeter doors properly secured with good heavy duty dead bolt locks? _____ _____

AP11.3.6. Are the locks in good working order? _____ _____

AP11.3.7. Can any of your door locks be by bypassed by breaking the glass or a panel of light wood? _____ _____

AP11.3.8. Have you permanently secured all unused doors? _____ _____

AP11.3.9. Are your windows protected by solid steel bars, ornamental or some other type of shutters? _____ _____

AP11.3.10. Do you close all shutters at night and when leaving your residence for extended periods of time? _____ _____

AP11.3.11. Are unused windows permanently closed and secured? _____ _____

AP11.3.12. Are your windows locked when they are shut? _____ _____

AP11.3.13. Are you as careful of second floor, or basement windows as you are of those on the ground floor? _____ _____

AP11.3.14. Have you secured sliding glass doors with a broom handle "charlie bar," or good patio door lock? _____ _____

AP11.3.15. If your residence has a skylight, roof latch, or roof doors, are they properly secured? _____ _____

AP11.3.16. Does your residence have an alarm system? _____ _____

AP11.3.17. Have you briefed your family and servants on good security procedures? _____ _____

AP11.3.18. Do you know the phone number of the police security force that services your neighborhood? _____ _____

AP11.4. GENERAL HOUSEHOLD SECURITY LIST Yes No

AP11.4.1. Are you and your family alert in your observations of persons who may have you under surveillance, or who may be casing your house in preparation for a burglary or other crime? _____ _____

AP11.4.2. Have you verified the references of your servants, and have you submitted their names for security checks? _____ _____

AP11.4.3. Have you told your family and servants what to do if they discover an intruder breaking into, or already in the house? _____ _____

AP11.4.4. Have you restricted the number of house keys? _____ _____

AP11.4.5. Do you know where all your house keys are? _____ _____

# AP12. APPENDIX 12
# GROUND TRANSPORTATION SECURITY TIPS

## AP12.1. INTRODUCTION

Criminal and terrorist acts against individuals usually occur outside the home and after the individual's habits have been established. Typically, most predictable habit is the route of travel from home to duty station or to commonly frequented local facilities.

## AP12.2. VEHICLES

AP12.2.1. ____ Select a plain car, minimize the "rich American" look.

AP12.2.2. ____ Consider not using a government car that announces ownership.

AP12.2.3. ____ Safeguard keys.

AP12.2.4. ____ Consider carrying a cell phone in your vehicle.

AP12.2.5. ____ Auto maintenance (when turning in a vehicle for maintenance, leave only the required keys):

AP12.2.5.1. ____ Keep vehicle in good repair. You don't want it to fail when you need it most.

AP12.2.5.2. ____ Keep gas tank at least 1/2 full at all times.

AP12.2.5.3. ____ Ensure tires have sufficient tread.

## AP12.3. PARKING

AP12.3.1. ____ Park in well lighted areas.

AP12.3.2. ____ Always lock your car...even when it's outside your house.

AP12.3.3. ____ Don't leave your car on the street overnight, if possible.

AP12.3.4. ____ Never get out without checking for suspicious persons. If in doubt, drive away.

AP12.3.5. ____ Avoid leaving keys with valet or parking attendants. If you must, leave only necessary vehicles keys.

AP12.3.6. ____ Don't allow entry to the trunk unless you're there to watch.

AP12.3.7. ____ Never leave garage doors open or unlocked.

AP12.3.8. ____ Use a remote garage door opener if available. Enter and exit your car in the security of the closed garage.

AP12.4. ON THE ROAD

AP12.4.1. ____ Before leaving buildings to get into your vehicle, check the surrounding area to determine if anything of a suspicious nature exists. Before leaving your vehicle, look around carefully to be confident you are not headed directly into a threatening situation.

AP12.4.2. ____ Before entering vehicles, check for suspicious objects on the seats. You may also look underneath the seats. Look for wires, tape or anything unusual.

AP12.4.3. ____ Guard against the establishment of routines by varying times, routes, and modes of travel. Avoid late night travel.

AP12.4.4. ____ Travel with companions or in convoy when possible.

AP12.4.5. ____ Avoid isolated roads and dark alleys when possible.

AP12.4.6. ____ Know locations of safe havens along routes of routine travel.

AP12.4.7. ____ Habitually ride with seatbelts buckled, doors locked, and windows closed.

AP12.4.8. ____ Do not allow your vehicle to be boxed in; maintain a minimum 8-foot interval between your vehicle and the vehicle in front; avoid the inner lanes.

AP12.4.9. ____ Be alert while driving or riding.

AP12.4.10. ____ Know how to react if surveillance is suspected or confirmed.

AP12.4.10.1. ____ Circle the block for confirmation of surveillance.

AP12.4.10.2. ____ Do not stop or take other actions, which could lead, to confrontation.

AP12.4.10.3. ____ Do not drive home.

AP12.4.10.4. ____ Get description of car and its occupants. Take a photograph if possible, but at a minimum, get the vehicle's license plate number.

AP12.4.10.5. ____ Go to nearest safehaven. Report incident to the nearest DoD counter-intelligence, security, or law enforcement organization.

AP12.4.11. ____ Recognize events that can signal the start of an attack, such as:

AP12.4.11.1. ____ Cyclist falling in front of your car.

AP12.4.11.2. ____ Flagman or workman stops your car.

AP12.4.11.3. ____ Fake police or Government checkpoint.

AP12.4.11.4. ____ Disabled vehicle or accident victims on the road.

AP12.4.11.5. ____ Unusual detours.

AP12.4.11.6. ____ An accident in which your car is struck.

AP12.4.11.7. ____ Cars or pedestrian traffic that box you in.

AP12.4.11.8. ____ Sudden activity or gunfire.

AP12.4.12. ____ Know what to do if under attack in a vehicle.

AP12.4.12.1. ____ Without subjecting yourself, passengers, or pedestrians to harm, try to draw attention to your car by sounding the horn.

AP12.4.12.2. ____ Put another vehicle between you and your pursuer.

AP12.4.12.3. ____ Execute immediate turn and escape; jump curb at 30-45-degree angle, 35 mph maximum.

AP12.4.12.4. ____ Ram blocking vehicle if necessary.

AP12.4.12.5. ____ Go to closest safehaven.

AP12.4.12.6. ____ Report incident to nearest DoD counter-intelligence, security, or law enforcement organization.

AP12.5. COMMERCIAL BUSES, TRAINS, AND TAXIS

AP12.5.1. ____ Vary mode of commercial transportation.

AP12.5.2. ____ Select busy stops. Avoid standing in a group while waiting.

AP12.5.3. ____ Don't always use the same taxi company.

AP12.5.4. ____ Don't let someone you don't know direct you to a specific cab.

AP12.5.5. ____ Ensure taxi is licensed and has safety equipment (seat belts at minimum).

AP12.5.6. ____ Ensure face of driver and picture on license are the same.

AP12.5.7. ____ Try to travel with a companion.

AP12.5.8. ____ If possible, specify the route you want taxi to follow.

# AP13. APPENDIX 13
# PERSONAL VEHICLE TIPS AND DRIVING SECURITY CHECKLIST

## AP13.1. INTRODUCTION

An extremely important aspect of personal security is the need for regular vehicle inspections. Many terrorist actions are accomplished by placing bombs in individual vehicles. This provides the terrorist less risk and increases the chance of "hitting" the appropriate target. The following are some relatively simply steps that every driver can take to reduce the likelihood of being hurt by a terrorist act centered on a personal automobile.

## AP13.2. VEHICLE INSPECTION TIPS

AP13.2.1. Every time you use your automobile, you should make a precautionary inspection. Bomb emplacement by terrorists is often rudimentary or hastily done, thereby providing the opportunity for easy detection. Make a habit of checking the vehicle and the surrounding area before entering and starting the vehicle.

AP13.2.1.1. Check interior of the vehicle for intruders or suspicious items.

AP13.2.1.2. Check electronic tamper device, if installed. A cheaper option is to use transparent tape on the hood, trunk, and doors to alert you to any tampering.

AP13.2.1.3. Check underneath the car and in the fender wells for any foreign objects, loose wires, etc.

AP13.2.1.4. Examine tires for stress marks and any evidence of tampering.

AP13.2.1.5. Check wheel lug nuts.

AP13.2.1.6. Check exterior for any fingerprints, smudges, or other signs of tampering.

AP13.2.2. You may consider the following suggestions in an effort to "harden" your vehicle:

AP13.2.2.1. Lock the hood with an additional lock and ensure that the factory latch is located inside.

AP13.2.2.2. Have oversized mirrors installed.

AP13.2.2.3. Use a locking gas cap.

AP13.2.2.4. Put two bolts through the exhaust pipe, perpendicular to one another. This prevents the insertion of explosive devices in the tail pipe.

AP13.2.2.5. Use steel-belted radial tires.

AP13.2.2.6. Install an intrusion alarm system and an extra battery.

AP13.2.2.7. In high-threat areas it may be appropriate to:

AP13.2.2.7.1. Install car armor.

AP13.2.2.7.2. Have an interior escape latch in the trunk.

AP13.2.2.7.3. Use fog lights.

AP13.2.2.7.4. Install bullet resistant glass.

AP13.3. SUPPLEMENTAL SECURITY CHECKLIST FOR DRIVING

The following items are suggested procedures to be used in operating personal and government motor vehicles in areas where terrorist activity is a concern. While adhering to these practices shall not necessarily prevent a terrorist incident, continual practice and attention to detail demanded by the procedures below shall enable many potential victims to escape to safety.

AP13.3.1. Keep the gasoline tank of your vehicle full or near full.

AP13.3.2. Keep the vehicle locked at all times. Do not park on the street at night. Vehicles in locked garages should also be kept locked. Use parking lots with attendants and where the vehicle can be kept locked. Lock unattended vehicles. No matter how short the time.

AP13.3.3. Check up and down the street before moving out of a house and/or building into your vehicle.

AP13.3.4. While approaching a vehicle, check its outside for evidence of tampering. Look for wires, strings, or objects attached to or hanging from vehicle.

AP13.3.5. Do not touch any unusual items protruding from the vehicle, call immediately for assistance.

AP13.3.6. Before entering the vehicle, check the floor (front and rear) to make certain the vehicle is not occupied.

AP13.3.7. As you drive away from the curb, be immediately alert for surveillance of your vehicle. Look for multiple vehicle surveillance, as most attacks on vehicles have included two or more vehicles.

AP13.3.8. Stay alert and be prepared to take evasive actions. Keep noise level within vehicle low. Eliminate loud playing of the radio or unnecessary conversation.

AP13.3.9. Keep the vehicle locked while driving and the windows closed. If open, keep them rolled to within two inches of the top. This practice prevents objects from being thrown into your vehicle.

AP13.3.10. When possible, drive in the lane nearest the center of the roadway. This practice puts attackers at a disadvantage, avoid being boxed in. Stay in the left lane where it is difficult for pursuing vehicles to run your vehicle off the road on multi-lane highways.

AP13.3.11. If you encounter a roadblock manned by uniformed police or military personnel, you should stop and remain seated inside your vehicle. If asked for identification, roll the window down enough to pass your identification to the officer. Do not unlock the doors.

AP13.3.12. Avoid suspicious roadblocks. Do not stop. Turn and go back or turn a corner to leave the area as quickly as possible.

AP13.3.13. A good driver is constantly aware of possible routes of escape or evasion while behind the steering wheel.

AP13.3.14. In the event of a firefight between local authorities and terrorists, get down and stay low. Unless you are in the direct line of fire, it is suggested that you do not move. Experience has shown that often times anything that moves gets shot.

# AP14. APPENDIX 14
# AIR TRAVEL SECURITY TIPS

## AP14.1. INTRODUCTION

Air travel, particularly through high-risk airports or countries, poses security problems different from those of ground transportation. Here are some simple precautions that can reduce vulnerabilities of a terrorist assault.

## AP14.2. MAKING TRAVEL ARRANGEMENTS

AP14.2.1. Use office symbols on orders or leave authorizations if the word description denotes a high or sensitive position.

AP14.2.2. Get an AOR specific threat briefing from your security officer, antiterrorism officer, or the appropriate counter-intelligence or security organization prior to overseas. This briefing is required prior to travel overseas and must occur within three months of travel according to reference (e).

AP14.2.3. Before traveling, consult the DoD Foreign Clearance Guide (available at www.fcg.pentagon.mil) (reference (az)) to ensure you know and can meet all requirements for travel to a particular country.

AP14.2.4. Use military air, USTRANSCOM/AMC military contract, or U.S. flag carriers if available and consistent with mission requirements.

AP14.2.5. Avoid scheduling through high-risk areas. If necessary, use foreign flag airlines and/or indirect routes to avoid high-risk airports.

AP14.2.6. Don't use rank or military address on tickets, travel documents, or hotel reservations.

AP14.2.7. Seats in the center of the aircraft tend to offer the greatest protection since they are farther from the usual center of hostile action, which is most often near the cockpit or terrorists at the rear of the aircraft.

AP14.2.8. Seats at an emergency exit may provide an opportunity to escape.

AP14.2.9. When available, use government quarters or contracted hotels as opposed to privately arranged off-base hotels.

AP14.3. PERSONAL IDENTIFICATION

AP14.3.1. Don't discuss your military affiliation with anyone.

AP14.3.2. Maintain unofficial form (s) of identification (tourist passport and/or driving license) to show airline and immigration officials as required.

AP14.3.3. Carry only limited DoD documentation on one's person (keep discreet). If you must carry these documents on your person, select a hiding place on board the aircraft in case of a hijacking. Don't carry classified documents unless they are absolutely mission-essential.

AP14.3.4. Consider use of a tourist passport, if you have one, with necessary visas, providing it's allowed by the country you are visiting.

AP14.4. LUGGAGE

AP14.4.1. Use plain, civilian luggage; avoid military looking bags, B-4 bags, duffel bags, etc.

AP14.4.2. Remove all military patches, logos, or decals from your luggage and briefcase.

AP14.4.3. Ensure luggage tags don't show your rank or military address.

AP14.4.4. Don't carry official papers in your briefcase.

AP14.5. CLOTHING

AP14.5.1. Travel in conservative civilian clothing when using commercial transportation or when traveling military airlift if you have to connect with a flight at a commercial terminal in a high-risk area.

AP14.5.2. Don't wear distinct military items such as organizational shirts, caps, or military issue shoes or glasses.

AP14.5.3. Don't wear U.S. identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.

AP14.5.4. Wear a long-sleeved shirt or bandage if your have a visible U.S. affiliated tattoo.

AP14.6. PRECAUTIONS AT THE AIRPORT

AP14.6.1. Arrive early; watch for suspicious activity.

AP14.6.2. Look for nervous passengers who maintain eye contact with others from a distance. Observe what people are carrying. Note behavior not consistent with that of others in the area.

AP14.6.3. No matter where you are in the terminal, identify objects suitable for cover in the event of attack. Pillars, trash cans, luggage, large planters, counters, and furniture can provide protection.

AP14.6.4. Don't linger near open public areas. Proceed through security checkpoints as soon as possible in order to be in a more secure area.

AP14.6.5. Be extremely observant of personal carry-on luggage. Thefts of briefcases designed for laptop computers are increasing at airports worldwide. Likewise, luggage not properly guarded provides an opportunity for a terrorist to place an unwanted object or device in your carry-on bag. As much as possible, do not pack anything you cannot afford to lose; if the documents are important, make a copy and carry the copy.

AP14.6.6. Avoid secluded areas that provide concealment for attackers.

AP14.6.7. Be aware of unattended baggage anywhere in the terminal.

AP14.6.8. Observe the baggage claim area from a distance. Do not retrieve your bags until the crowd clears. Proceed to customs lines at the edge of the crowd.

AP14.6.9. Report suspicious activity to airport security personnel.

AP14.6.10. Proceed through security checkpoints as soon as possible.

AP14.6.11. Be extremely observant of personal carry-on luggage.

AP14.7. ACTIONS IF ATTACKED IN AN AIRPORT

AP14.7.1. If being attacked by bomb or grenade, dive for cover. Do not run; running increases the probability of shrapnel hitting vital organs or the head.

AP14.7.2. If you must move, belly crawl or roll. Stay low to the ground, using available cover.

AP14.7.3. If you see grenades, seek immediate cover, lay flat on the floor, feet and knees tightly together with soles toward the grenade. In this position, your shoes, feet, and legs protect the rest of your body. Shrapnel shall rise in a cone from the point of detonation, passing over your body.

AP14.7.4. Place arms and elbows next to your ribcage to protect your lungs, heart, and chest. Cover your ears and head with your hands to protect neck, arteries, ears, and skull.

AP14.7.5. The responding security personnel shall not be able to distinguish you from attackers. Do not attempt to assist them in any way. Lay still until told to get up.

AP14.8. AIRPLANE HIJACKINGS

AP14.8.1. Determining the best response in a hostage situation is a critical judgment call. Passengers need to remain extremely alert and rational to try to understand the intentions of the hijackers. Sitting quietly may be prudent in most circumstances, but it is conceivable the situation may require actions to prevent hijackers from taking control of the aircraft. In all situations, it is important for individuals to remain alert to unexpected events, think clearly, and act responsibly. If hijackers are flying the plane, a suicide attack with the aircraft is highly probable, and a coordinated attack by the passengers may be appropriate.

AP14.8.2. Remain calm, be polite and cooperate with your captors.

AP14.8.3. Be aware that all hijackers may not reveal themselves at the same time. A lone hijacker may be used to draw out security personnel for neutralization by other hijackers.

AP14.8.4. Surrender your tourist passport in response to a general demand for identification.

AP14.8.5. Don't offer any information; confirm your military status if directly confronted with the fact. Be prepared to explain that you always travel on your personal passport and that no deceit was intended.

AP14.8.6. Discreetly dispose of any military or U.S. affiliated documents.

AP14.8.7. Don't draw attention to yourself with sudden body movements, verbal remarks, or hostile looks.

AP14.8.8. Prepare yourself for possible verbal and physical abuse, and lack of food, drink, and sanitary conditions.

AP14.8.9. If permitted, read, sleep, or write to occupy your time.

AP14.8.10. Discreetly observe your captors and memorize their physical descriptions. Include voice patterns and language distinctions, as well as clothing and unique physical characteristics. Observe how heavily they’re armed.

AP14.8.11. If possible, observe if the pilots remain in control of the aircraft.

AP14.8.12. Be aware there may be Federal authorities, such as Air Marshals, on the aircraft that may be best suited to take action.

AP14.8.13. Cooperate with any rescue attempt. Remain still and follow instructions of rescuers. If possible, lie on the floor until told to rise.

# AP15. APPENDIX 15
# USE OF PROTECTIVE SECURITY DETAILS (PSDs)

## AP15.1. INTRODUCTION

AP15.1.1. The use of PSDs is a policy decision. There are pros and cons to their use. The employment of large numbers of PSD members to protect a few senior officers or DoD officials may deter all but the most determined terrorist attack. On the other hand, the use of one or two PSD members may attract attention to the protected person that might otherwise not be given to that individual.

AP15.1.2. DoD personnel can be their own bodyguards if they follow the self-protection strategy outlined in this Handbook. Supplemented by a chauffeur trained in defensive driving and other security techniques, DoD executives should be relatively safe in most situations.

AP15.1.3. In high crisis situations, in areas where kidnapping is rampant, and during period of direct threats, use of PSDs for high-risk personnel should be strongly considered.

AP15.1.4. It is critical that members of PSDs be thoroughly trained to do their job. PSD training is intensive and cannot be done overnight, nor can individuals who have been trained retain levels of proficiency in driving, firearms, and close combat without continuous training. The PSD members must be physically and mentally fit so that their bodies and minds shall respond positively in crisis situations.

AP15.1.5. Since PSD members must both protect protectees and be their companions in personal and professional situations they must be particularly honest and discrete.

AP15.1.6. The training of bodyguards should begin by defining their role -- both as a technical aid to the executive they serve and as an individual who can direct the executive they protect to self-help. In an attack, PSD members may be killed or incapacitated. In their protective roles, PSD members should be constantly teaching protectees to protect themselves, to avoid attack, to respond to an attack, and to conduct themselves properly if captured.

## AP15.2. PSD MEMBER TRAINING OBJECTIVES

AP15.2.1. Members of PSDs should be instructed in the following areas:

AP15.2.1.1. History of threats from criminals and terrorists.

AP15.2.1.2. Assassinations/executions.

AP15.2.1.3. Kidnap/hostage/ransom actions.

AP15.2.1.4. Extortion actions.

AP15.2.1.5. Destruction of Government and Government-related facilities.

AP15.2.1.6. The psychology of criminals and extremists.

AP15.2.2. It is particularly important that the general instruction received as part of the general and professional military training of PSD members be supplemented by local information. Such information should emphasize terrorist activity in the area of operations where PSD members are to provide protection to senior officers and DoD officials.

AP15.3. TARGET CHARACTERISTICS

AP15.3.1. In developing a strategy for the use of PSD members to provide additional protection, it is essential that protectees examine their personal roles, missions, functions, and lifestyles to assess their individual and dependents risk and vulnerability to terrorist attack. The following considerations should be weighed in developing a PSD protective plan:

AP15.3.1.1. Official Role

AP15.3.1.1.1. PSDs should be assigned to high-risk personnel based on their duties, responsibilities, risk, vulnerability, and importance or criticality to DoD missions and functions. The following questions should be considered in determining the need for assignment PSD to senior officers or DoD officials.

AP15.3.1.1.1.1. What is the public profile of the officer or DoD official?

AP15.3.1.1.1.2. What is DoD, Combatant Command, or Embassy protection policy?

AP15.3.1.1.1.3. What are the strengths and weaknesses of the physical security system?

AP15.3.1.1.1.4. What are local DoD or Embassy security procedures?

AP15.3.1.1.1.5. What coordination occurs between local (host nation) law enforcement officials and U.S. Government, the Department of Defense, or Embassy security personnel?

AP15.3.1.1.1.6. How close are relations between the U.S. Government and the state, municipal, local or foreign host Government?

AP15.3.1.1.1.7. How much (quantity and quality) information on potential threats is being provided from all sources? How fast does this information arrive; how fast is it assessed, and how fast can it be disseminated for those with need to know?

AP15.3.1.2. The Protectee. In developing a plan for the protection of senior officers, DoD officials, and their dependents, the following personal characteristics, interests, and lifestyle considerations should be weighed:

AP15.3.1.2.1. The executive and his family.

AP15.3.1.2.2. Public and private profile.

AP15.3.1.2.3. Politics and psychology.

AP15.3.1.2.4. Zones of vulnerability.

AP15.3.1.2.5. Executive.

AP15.3.1.2.5.1. Residence.

AP15.3.1.2.5.2. Movement.

AP15.3.1.2.5.3. Work.

AP15.3.1.2.5.4. Social functions.

AP15.3.1.2.5.5. Recreation.

AP15.3.1.2.6. Family.

AP15.3.1.2.6.1. Residence.

AP15.3.1.2.6.2. Movement.

AP15.3.1.2.6.3. Shopping and/or school.

AP15.3.1.2.6.4. Social functions.

AP15.3.1.2.6.5. Recreation.

AP15.4. PSD MEMBERS AND THEIR RESPONSIBILITIES

AP15.4.1. Relationship to Executive PSD members may be asked to perform a wide variety of tasks in the context of providing additional security protection to senior officers and DoD officials. Protective services may be provided from the following positions or functions:

AP15.4.1.1. At fixed post.

AP15.4.1.2. As driver.

AP15.4.1.3. As all around bodyguard.

AP15.4.2. Discipline.

AP15.4.2.1. Conduct.

AP15.4.2.1.1. PSD members must be skilled in negotiation with protectees, their families, their colleagues, and their acquaintances over the proper balance between security considerations on the one hand, and family, social, and business activities on the other. They must retain their composure at all times, even if protectees and those around them do not, especially over matters of appropriate security arrangements for home, official business away from the office, and recreational activities.

AP15.4.2.1.2. PSD members must also be skilled in remaining focused on the need for protection, regardless of the behaviors or personal practices of protectees. In addition, PSD members shall have an opportunity to observe senior officers, DoD officials, and their families in close, personal situations. As there are often significant differences between public and private personalities, PSD members may be placed in positions where their ideals, personal values, expectations, and preferences differ significantly from the person or people they are protecting.

AP15.4.2.1.3. PSD members must be prepared to perform other duties as may be required to preserve their anonymity on the one hand, and the anonymity of the protectee on the other. If a protectee is scheduled to attend a meeting for which a secretary might be used to take notes, a member of the PSD team may be assigned the task of note taking, thereby keeping the size of the protectee's entourage small. By performing secretarial duties in connection with a PSD assignment, the PSD member does not reveal his or her special training to outside observers. In addition, he or she does not reveal U.S. Government concerns about the risk or vulnerability of the protected person to a terrorist attack.

AP15.4.2.2. Appearance.

AP15.4.2.2.1. PSD members must appear to be part of their protectees entourage. They must "fit in" with the protectee’s functions, roles, and lifestyles. As noted above, they may be asked to perform other duties not directly related to security in order to disguise their primary security duties.

AP15.4.2.2.2. PSD members should dress, groom, and act as part of the protectee's environment. Consider longer hairstyles, functional jewelry, low-key manicures, and even civilian attire for PSD members assigned to senior DoD officials. Consider more mature members of PSD details for assignment to senior officers as "aides" or "assistants" as well as younger members of PSDs as drivers and couriers.

AP15.4.2.3. Organizational Security Plans and Contingencies.

AP15.4.2.3.1. PSD members need to be kept informed of physical security and personnel security arrangements as they develop and change. It is essential that PSDs know the location of response forces and backup response forces, the communications links to reach such forces, communication links with local, municipal, and host country security resources (as necessary). PSD members should be given detailed information on the location of safe havens, pre-surveyed evacuation sites, pre-surveyed evacuation routes, and identified backup or alternatives.

AP15.4.2.3.2. PSD members should be invited to observe and to participate in crisis management training and exercises so that they can appreciate the roles and responsibilities of their protectees and identify positions from which they can continue to perform their responsibilities without interfering with other members of the crisis management team.

AP15.4.2.4. Tools and Techniques. PSD members bring a wide range of "tools" and "techniques" to their responsibilities of protecting senior officers and DoD officials. At the same time, protectees and their organizations need to be sensitive to some of the requirements or special considerations that PSDs may have in order to carry out their assignments. The following are some, but perhaps not all, of the considerations PSDs and host organizations need to examine.

AP15.4.2.4.1. At fixed post.

AP15.4.2.4.1.1. Need for secrecy, monitoring children, monitoring domestic staff.

AP15.4.2.4.1.2. Observation and/or surveillance.

AP15.4.2.4.1.3. Monitoring phone, mail, etc.

AP15.4.2.4.1.4. Monitoring pattern avoidance.

AP15.4.2.4.1.5. Emergency plans: fire, bomb threat, natural disaster, escape, threat notification, evacuation.

AP15.4.2.4.1.6. Penetration tests.

AP15.4.2.4.1.7. Dogs.

AP15.4.2.4.1.8. Lighting.

AP15.4.2.4.1.9. Alarm systems.

AP15.4.2.4.1.10. Weapons.

AP15.4.2.4.1.11. Security surveys and implementation.

AP15.4.2.4.1.12. Concealed personal survival equipment.

AP15.4.2.4.1.13. Hideouts/protected locations/safe rooms.

AP15.4.2.4.1.13.1. What to do until help arrives.

AP15.4.2.4.1.13.2. Emergency communications and response.

AP15.4.2.4.1.13.3. Attacker confusion and neutralization devices and techniques.

AP15.4.2.4.1.13.4. The family emergency plan.

AP15.4.2.4.2. As driver. What to expect from attacker.

AP15.4.2.4.2.1. Vulnerability through pattern development.

AP15.4.2.4.2.2. Element of surprise.

AP15.4.2.4.2.3. Single vehicle cutoff.

AP15.4.2.4.2.4. Two vehicle cutoff.

AP15.4.2.4.2.5. Road blocks.

AP15.4.2.4.3. How to respond (Protected vehicles: escorted, unescorted).

AP15.4.2.4.3.1. Selection of vehicle and security modifications.

AP15.4.2.4.3.1.1. Horsepower/body style.

AP15.4.2.4.3.1.2. Tires.

AP15.4.2.4.3.1.3. Mirrors.

AP15.4.2.4.3.1.4. Glass.

AP15.4.2.4.3.1.5. Concealed weapons.

AP15.4.2.4.3.1.6. Armor.

AP15.4.2.4.3.1.7. Lights.

AP15.4.2.4.3.1.8. Noise and/or sirens.

AP15.4.2.4.3.1.9. Communications.

AP15.4.2.4.3.2. Defensive Driving.

AP15.4.2.4.3.2.1. Alertness and observation.

AP15.4.2.4.3.2.2. Drive ahead and plan ahead.

AP15.4.2.4.3.2.3. Pattern avoidance.

AP15.4.2.4.3.2.4. Neutralizing forms of attack.

AP15.4.2.4.3.2.5. Escape routes and safe havens.

AP15.4.2.4.3.2.6. Locked car as barrier.

AP15.4.2.4.3.2.7. Defensive driving techniques.

AP15.4.2.4.3.2.8. Chemical irritants.

AP15.4.3.4.3.2.9. First aid.

AP15.4.3.4.3.2.10. Coping with fire.

AP15.4.3.4.3.2.11. Bomb recognition and handling.

AP15.4.3.4.3.2.12. Photography

AP15.5. WHAT PSD MEMBERS MUST TEACH PROTECTEES

AP15.5.1. PSD members and their protectees must jointly develop routines to detect, classify, assess, and respond to threats to the protectees security. The following issues must be addressed and plans jointly developed and practiced.

AP15.5.1.1. Duress signals.

AP15.5.1.2. Call-in.

AP15.5.1.3. Carrying duress notes written on money.

AP15.5.1.4. Duress alarms and/or radio links.

AP15.5.1.5. Varying routines.

AP15.5.1.6. Clothing changes.

AP15.5.1.7. Mutual observation.

AP15.5.1.8. Contact with police.

AP15.5.1.9. Hazards of swimming, fishing, boating, etc.

AP15.5.1.10. What to do if taken captive.

AP15.5.1.10.1. Cooperate and stay calm.

AP15.5.1.10.2. Avoidance of psychological link with kidnappers.

AP15.5.1.10.3. Prepared stories.

AP15.5.1.10.4. Use of codes.

AP15.5.1.10.5. Verbal contact.

AP15.5.1.10.6. Concealed aids.

AP15.5.2. These considerations must be discussed jointly because the protectee and PSD members shall be much more likely to remember during an emergency those plans and procedures jointly developed. Practice of these plans should occur on a continuing basis, especially during periods of high threat.

# AP16. APPENDIX 16
# PHYSICAL SECURITY EVALUATION GUIDE (DD FORM 2637)

WHEN FILLED IN

**PHYSICAL SECURITY EVALUATION GUIDE**

*(FOR LOCAL USE ONLY - Do not forward to higher authorities unless specifically requested)*

**SECTION I - GENERAL PHYSICAL SECURITY**

**PART A - GENERAL INFORMATION**

| | |
|---|---|
| 1. INDIVIDUAL(S) CONDUCTING SURVEY *(Add additional names in Section IV)* | |
| a. NAME *(Last, First, Middle Initial)* | |
| b. RANK/GRADE | |
| c. ORGANIZATION | |
| d. TELEPHONE NUMBER *(Include Area Code)* | e. SURVEY DATE *(YYMMDD)* |
| 2. DESCRIPTION OF FACILITY SURVEYED | |
| DESCRIBE FACILITY *(Activities, functions, facility(ies) to be protected, in accordance with DoD 5200.8-R)* | |
| 3. INDIVIDUAL(S) INTERVIEWED *(Please continue in Section IV)* | |

| | INTERVIEWEE 1 (1) | INTERVIEWEE 2 (2) | INTERVIEWEE 3 (3) |
|---|---|---|---|
| a. NAME *(Last, First, Middle Initial)* | | | |
| b. RANK/GRADE | | | |
| c. ORGANIZATION | | | |
| d. TELEPHONE NUMBER *(Include Area Code)* | | | |

4. ATTACH PLOT PLAN OF THE ENTIRE FACILITY SHOWING:
- Compass rose showing north.
- All existing buildings and their function, all interior and exterior roads, all fences, and other physical barriers.
- Railroad sidings or main track.
- Airfield facilities including runways, taxiways, helipads, supporting utilities, or utilities lying beneath such surfaces.
- Location of gates *(active and inactive)*.
- Any planned remodeling or expansion of facilities.
- If facility borders a body of water, also submit DD Form 2638.

5. ATTACH AS-BUILT DRAWING OF THE OFFICE OR RESIDENCE STRUCTURE SHOWING:
- Construction of exterior and interior walls.
- Location of all windows, doors, and skylights.
- Location and size of all vents, utility openings, and other building penetrations.
- Electrical runs, outlets, and switches for all voltages.

| |
|---|
| 6. LOCATION OF FACILITY *(Briefly describe appropriate category(ies)):* |
| a. URBAN? |
| b. SUBURBAN? |
| c. INCORPORATED? |
| d. UNINCORPORATED? |
| e. GOVERNMENT INSTALLATION? |
| f. OTHER? |

**DD Form 2637, JAN 93 (EG)** Page 1 of _____ Pages

WHEN FILLED IN

Designed using Perform Pro, WHS/DIOR, Jul 96

**WHEN FILLED IN**

| 7. SOCIOECONOMIC ENVIROMENT *(Briefly describe as applicable):* | f. COMMENTS |
|---|---|
| a. RESIDENTIAL | |
| b. INDUSTRIAL | |
| c. COMMERCIAL | |
| d. AGRICULTURAL | |
| e. NEIGHBORING AREA IS *(Briefly describe as applicable):* | |
| (1) AFFLUENT | |
| (2) MIDDLE CLASS | |
| (3) POOR | |

| 8. AREA CRIME RATE *(Briefly describe in applicable spaces):* |
|---|
| a. HIGH? |
| b. MODERATE? |
| c. LOW |
| d. NEIGHBORHOOD VIOLENCE *(Briefly describe as applicable in accordance with instructions):* |
| (1) CIVIL UNREST |
| (2) ROBBERIES |
| (3) BURGLARIES |
| (4) ASSAULTS |
| (5) HOMICIDES |
| (6) NARCOTICS TRAFFICKING |
| (7) SEXUAL ASSAULTS |
| (8) OTHER CRIMES *(Extortion/kidnapping/vandalism, etc.)* |

| e. IS THERE A HISTORY OF LOSS AT THIS FACILITY? | | YES | | NO IF YES, COMPLETE 8f: | |
|---|---|---|---|---|---|
| f. TYPE OF LOSS | NUMBER OF TIMES (a) | | VALUE (b) | | DATE(S) (c) |
| (1) PILFERAGE | | | | | |
| (2) INTERNAL THEFT | | | | | |
| (3) BURGLARY/BREAKING AND ENTERING | | | | | |
| (4) VANDALISM | | | | | |
| (5) PROPERTY LOSS | | | | | |
| (6) CRIMES AGAINST PERSONS | | | | | |

| g. COMMENTS *(Weapons used/tools used/modes of attack)* |
|---|
| |

**DD Form 2637, JAN 93**

Page 2 of _____ Pages

**WHEN FILLED IN**

**WHEN FILLED IN**

| 9. LAW ENFORCEMENT AGENCY HAVING JURISDICTION | | |
|---|---|---|
| a. AGENCY NAME | | |
| b. CHIEF/SUPERVISOR *(Last Name, First, Middle Initial)* | | |
| c. TELEPHONE NUMBER *(Include Area Code)* | | |
| d. LOCATION *(Include Street, City, State, and 9-digit ZIP Code)* | | |
| e. AVERAGE RESPONSE TIME | | |
| YES | NO | *(X and complete as applicable - if answer is No, explain why)* |
| | | 10. IS LIAISON MAINTAINED WITH LOCAL AND STATE LAW ENFORCEMENT AGENCIES? |
| | | 11. IS THERE AN ACTIVE SECURITY AWARENESS PROGRAM? |
| | | 12. ARE BACKGROUND INVESTIGATIONS CONDUCTED PRIOR TO EMPLOYMENT OF PERSONNEL? |
| a. CATEGORY(IES) OF PERSONNEL INVESTIGATED | | |
| b. EXTENT OF INVESTIGATION *(National Agency Check, Background Investigation, Special Background Investigation, etc.)* | | |

| 13. NUMBER OF EMPLOYEES *(Fill in appropriate blocks)* | | | | | | |
|---|---|---|---|---|---|---|
| a. CIVILIAN | | | | b. MILITARY | | c. OTHER (Specify) |
| (1) GS PROFESSIONAL | (2) GS CLERICAL | (3) WAGE GRADE | (4) CONTRACTORS | (1) OFFICERS | (2) ENLISTED | |
| | | | | | | |
| | | | | | | |

| 14. ACCESS TO FACILITY | | |
|---|---|---|
| a. NUMBER OF PERSONNEL REQUIRING ENTRANCE AND EXIT TO STRUCTURE/OFFICE AREA DURING THE FOLLOWING TIME PERIODS: | | |
| (1) 0001 - 0400 | (3) 0801 - 1200 | (5) 1601 - 2000 |
| (2) 0401 - 0800 | (4) 1201 - 1600 | (6) 2001 - 2400 |
| b. COMMENTS *(Regarding access, by time of day, type of employee, etc.)* | | |

**DD Form 2637, JAN 93**

Page 3 of _____ Pages

**WHEN FILLED IN**

WHEN FILLED IN

## PART B - PERIMETER SECURITY

| YES | NO | 15. PHYSICAL BARRIERS *(X and complete as applicable. Continue items or make comments on separate sheets if necessary.)* |
|---|---|---|
| | | IS THERE SOME TYPE OF PHYSICAL BARRIER; I.E. WALL, FENCE, ETC., AROUND THIS FACILITY? IF YES, DESCRIBE. |
| | | a. DOES THE BARRIER ESTABLISH THE PROPERTY LINE? |
| | | b. IS IT A DETERRENT TO ENTRY? |
| | | c. DOES IT ESTABLISH PERSONNEL CONTROL? |
| | | d. DOES IT ESTABLISH VEHICLE CONTROL? |
| | | e. ARE THERE ANY HOLES IN THE FENCE? IF YES, WHERE ARE THEY LOCATED? |
| | | f. ARE THERE ANY PLACES ALONG THE FENCE WHERE THE GROUND IS WASHED AWAY? |
| | | g. ARE THERE ANY PLACES WHERE STREAMS CIRCUMVENT THE FENCE? IF YES, HOW ARE THESE AREAS PROTECTED? |
| | | h. IS THERE A CLEAR ZONE EXISTING ON BOTH SIDES OF THE FENCE? |
| | | i. IS THE CLEAR ZONE OBSTRUCTED BY MATERIAL STORED NEAR THE FENCE? |
| | | j. ARE THERE ANY POLES NEAR THE FENCE WHICH CAN BE USED FOR ENTRY OR EXIT? |
| | | k. ARE THERE ANY TREES IN THE CLEAR ZONE? |
| | | l. IF THERE ARE TREES, SHOULD THEY BE REMOVED OR TRIMMED? |
| | | m. IS THERE ANY SHRUBBERY, UNDERBRUSH, OR HIGH GRASS IN THE CLEAR ZONE? |
| | | n. IS THERE SCHEDULED ACTION TAKEN TO REMOVE OR KEEP GROWTH IN THE CLEAR ZONE CUT SO THAT IT DOES NOT OBSTRUCT A CLEAR VIEW OF THE FENCE? |
| | | o. ARE THERE ANY OPENINGS OTHER THAN GATES AND DOORS IN THE FENCE WHICH ARE NOT PROTECTED? |
| | | p. IF PROTECTED, IS PROTECTION ADEQUATE? |
| | | q. ARE THERE "NO TRESPASSING" SIGNS POSTED ON THE OUTSIDE OF THE FENCE AT REGULAR INTERVALS? |
| | | r. ARE POSTED SIGNS PRINTED IN COMMON LOCAL LANGUAGES AS WELL AS ENGLISH? |
| | | s. IS THE ENTIRE FENCE LINE WITHIN EASY VIEW OF PATROLLING GUARDS OR CLOSED-CIRCUIT TELEVISION (CCTV)? |
| | | t. IS THE ENTIRE FENCE LINE IN VIEW OF ASSIGNED PERSONNEL DURING NORMAL WORKING HOURS? |
| | | u. IS THE FENCE REGULARLY INSPECTED? IF YES, HOW OFTEN AND BY WHOM? |
| | | v. IS IMMEDIATE ACTION TAKEN TO REPAIR REPORTED FENCE DAMAGE? |
| | | w. ARE VEHICLES ALLOWED TO PARK NEAR PERIMETER PHYSICAL BARRIER? |
| | | x. IS MATERIAL STACKED NEAR PERIMETER PHYSICAL BARRIER THAT WOULD ACT AS A STEP LADDER OR OTHERWISE |
| | | y. HOW MUCH TIME WOULD BE REQUIRED TO PENETRATE THE BARRIER USING ONE OF THE FOLLOWING? *(Please* |

| (1) WIRE CUTTERS | (2) OTHER HAND TOOLS | (3) POWER TOOLS | (4) VEHICLE ≤ 5000 LBS | (5) VEHICLE ≥ 5000 LBS | (6) EXPLOSIVES |
|---|---|---|---|---|---|
| | | | | | |

16. GATES AND DOORS

| a. HOW MANY GATES ARE THERE THROUGH THE PERIMETER? | b. HOW MANY DOORS ARE THERE THROUGH THE PERIMETER? |
|---|---|
| | |

c. LIST ALL DOORS AND GATES, DESIGNATING THE USE OF EACH *(Including those not used) (Include doors and gates through the perimeter used for employees (if separate categories of employees, use different doors or gates, designate the category for each), those used for visitors, private vehicles, delivery and shipment trucks, railroad sidings, those rarely used, and those not used at all. Each gate should be identified by number or name, the hours used, and how each is controlled and/or monitored. Continue in Section IV, if necessary.)*

**DD Form 2637, JAN 93**



WHEN FILLED IN

**WHEN FILLED IN**

| YES | NO | 16. GATES AND DOORS *(Continued) (X and/or complete as applicable. Shaded items either require a written response or will be followed by a set of questions. Use Section IV, as necessary.)* |
|---|---|---|
| | | d. ARE ALL GATES SECURED AND OPERATING PROPERLY? *(State how they are secured.)* |
| | | e. DO SWING GATES CLOSE WITHOUT LEAVING A GAP? |
| | | f. ARE GATES WHICH ARE NOT USED OR ONLY RARELY USED EQUIPPED WITH PROPER LOCKS AND SEALS? |
| | | g. WILL THE CHAINS AND LOCKS SECURE GATES WHEN CLOSED? |
| | | h. ARE ALARM DEVICES USED ON ANY GATES? |
| | | i. ARE EXIT ALARMS USED ON PERIMETER FIRE DOORS OR OTHER DOORS WHICH ARE NOT AVAILABLE FOR GENERAL USE? |
| | | j. IF EXIT ALARMS ARE USED, DO THEY PROVIDE: |
| | | (1) A LOCAL SIGNAL? |
| | | (2) A SIGNAL AT A GUARD OFFICE? |
| | | k. ARE ANY OF THE ENTRANCES OR EXITS THROUGH THE PERIMETER PRESENTLY CONTROLLED BY CCTV AND/OR CARD-KEY LOCKS AND TURNSTILES? IF YES, INDICATE WHICH ONES. |
| | | l. ARE THERE ANY DOORS OR GATES THROUGH THE PERIMETER WHERE CCTV COULD BE USED TO CONTROL ADMITTANCE AND EXITS? IF YES, INDICATE WHICH ONES. |
| | | (1) HOW MANY PERSONS USE THESE DOORS OR GATES AT PEAK PERIODS? |
| | | (2) WOULD THESE DOORS OR GATES HAVE TO BE AVAILABLE FOR USE AT ODD HOURS? |
| | | m. ARE THERE ANY GATES OR DOORS WHERE CCTV COULD BE USED FOR INGRESS AND EGRESS OF VEHICLES AND TRAINS? IF YES, INDICATE WHICH ONES. |
| | | (1) WHAT ARE THE PEAK PERIODS OF TRAFFIC THROUGH THESE GATES? |
| | | (2) ARE THESE GATES OR DOORS USED ROUTINELY DURING OPERATING PERIODS? IF YES, HOW OFTEN? |
| | | (3) ARE THESE GATES OR DOORS USED ROUTINELY DURING CLOSED PERIODS? IF YES, HOW OFTEN? |
| | | (4) WHAT IS THE AVERAGE NUMBER OF VEHICLES/RAILROAD CARS THAT WOULD PASS THROUGH DURING A 24-HOUR PERIOD? |
| | | n. COULD ANY PERIMETER DOORS OR GATES BE SECURED BY PERMITTING ENTRY AND EXIT WITH A CARD-KEY OPERATED TURNSTILE-TYPE GATE WITHOUT THE USE OF CCTV? |
| | | o. ARE GATES AND DOORS THROUGH THE PERIMETER POSTED WITH "NO TRESPASSING" SIGNS IN ENGLISH AND OTHER LOCALLY-USED LANGUAGES? |
| | | p. CAN VEHICLES DRIVE UP TO THE BARRIER AND BE USED AS A STEPLADDER FOR ENTRY OR EXIT? |
| | | q. IS THERE A RAILROAD GATE? IF YES, INDICATE WHICH ONE(S). |
| | | (1) DOES THE RAILROAD HAVE A LOCK ON THE GATE? |
| | | (2) DOES THE DOD ACTIVITY HAVE A LOCK ON THE GATE? |

r. ADDITIONAL COMMENTS ON GATES AND DOORS *(Discuss resistance against hand and power tools, conditions of door jams, hinges, on supporting structure. Use Section IV, as necessary.)*

**DD Form 2637, JAN 93** Page 5 of _____ Pages

**WHEN FILLED IN**

WHEN FILLED IN

## PART C - PERIMETER LOCK SYSTEM

17. LOCKS

| LOCK a. | LOCATION b. | TYPE *(See 17i) c.* | MANUFACTURER d. | DATE *(YYMMDD)* e. | LAST CHANGED *(YYMMDD)* f. | LAST INSPECTED *(YYMMDD)* g. | CONDITION *(Rusted, cracked cases, bent, etc.)* h. |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

i. LOCK TYPES *(For use in 17c)*

| | | |
|---|---|---|
| (1) CYLINDRICAL | (5) PADLOCK WITH KEY | (9) MORTIS |
| (2) CYLINDRICAL WITH DEAD BOLT FUNCTION | (6) PADLOCK WITH COMBINATION | (10) RIM |
| (3) CYLINDER DEAD BOLT | (7) HIGH SECURITY LOCK | (11) OTHER *(Specify)* |
| (4) CYLINDER DEAD BOLT WITH LOCK | (8) HIGH SECURITY LOCK WITH HASP | |

j. HOW MANY MINUTES OF RESISTANCE TO FORCED ENTRY ARE PROVIDED BY EACH LOCK? *(Use numbers from 17a to identify locks)*

| YES | NO | *(X one. If response is needed, refer to locks by chart entry numbers)* |
|---|---|---|
| | | k. ARE CYLINDERS REMOVABLE? *(If yes, state which locks)* |
| | | l. ARE LOCKS CHANGED WHEN SECURITY IS COMPROMISED? |
| | | m. ARE LOCKS EQUIPPED WITH: *(Specify)* |
| | | (1) CASED HARDENED PADLOCKS? |
| | | (2) CASE HARDENED CHAINS? |
| | | n. ARE ALL LOCK NUMBERS RECORDED? |
| | | o. ARE LOCK NUMBERS OBLITERATED? |
| | | p. ARE DOOR LOCKS AND PADLOCKS SEPARATE SYSTEMS? |

18. ADDITIONAL COMMENTS ON LOCK SYSTEM

**DD Form 2637, JAN 93** Page 6 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## PART D - KEY CONTROL

19. DESCRIBE KEY CONTROL SYSTEM

20. WHO IS RESPONSIBLE FOR KEY CONTROL?

21. MASTER KEYS

| a. NUMBER | b. ISSUED T0 | c. POSITION |
|---|---|---|
| | | |

| YES | NO | 22. KEY CONTROL DETAILS |
|---|---|---|
| | | a. ARE KEYS SIGNED FOR? |
| | | b. ARE ALL KEYS ACCOUNTED FOR? |
| | | c. IS ISSUANCE OF KEYS RECORDED? |
| | | d. IF YES, IS REPORT KEPT UP TO DATE? |
| | | e. ARE KEYS REMOVED FROM VEHICLES AT NIGHT AND ON WEEKENDS? |

f. DESCRIBE THE PROCEDURE FOR RETURN OF KEYS WHEN EMPLOYEE IS TERMINATED OR TRANSFERRED

23. ADDITIONAL COMMENTS ON KEY CONTROL

## PART E - PERIMETER ALARM SYSTEM

24. PERIMETER ALARM SYSTEM

| YES | NO | *(X and complete as applicable)* |
|---|---|---|
| | | ARE PERIMETER ALARMS EMPLOYED? IF YES, COMPLETE a. THROUGH f., BELOW, FOR EACH SYSTEM. USE SECTION IV, AS REQUIRED. |
| | | a. NAME OF MANUFACTURER |
| | | b. IS THE ALARM: |
| | | (1) LOCAL? |
| | | (2) CENTRAL STATION? |
| | | (3) SILENT? |
| | | (4) DIRECT (POLICE)? |

| c. INSTALLATION DATE *(YYMMDD)* | d. HOW MANY POINTS ARE ALARMED? | e. LOCATION OF MASTER CONTROL BOX |
|---|---|---|
| | | |

f. LOCATION OF EACH ALARM CONTACT *(Use Section IV, or additional sheets, as required.)*



WHEN FILLED IN

WHEN FILLED IN

| 25. INSPECTION AND MAINTENANCE *(For each additional alarm system, use Section IV, as necessary)* | | |
|---|---|---|
| a. DATE OF LAST INSPECTION *(YYMMDD)* | b. INSPECTED BY | |
| | (1) NAME *(Last, First, Middle Initial)* | (2) TITLE |
| c. DATE OF LAST SERVICE *(YYMMDD)* | d. SERVICED BY | |
| | (1) NAME *(Last, First, Middle Initial)* | (2) TITLE |
| e. IS THERE A MAINTENANCE CONTRACT? | | f. MAINTENANCE COST |
| 26. WHAT ARE THE LOCAL POLICIES/LAWS REGARDING FALSE ALARMS? | | |
| 27. WHAT IS THE RESPONSE TIME TO AN ALARM? | | |

| 28. ALARM SYSTEM DETAILS | | |
|---|---|---|
| YES | NO | *(X as appropriate and add any additional comments)* |
| | | a. ARE WIRES GOING TO THE LOCAL ALARM PROTECTED; I.E., IN CONDUIT? |
| | | b. IF A PERIMETER ALARM DETECTOR IS USED, DOES RESTORING DOOR OR WINDOW TO ORIGINAL POSITION STOP THE |
| | | c. DOES ALARM HAVE A BATTERY BACK-UP? |
| | | d. IS BATTERY CHECKED PERIODICALLY FOR SUITABLE CHARGE? |
| | | e. ARE DURESS ALARMS USED AT ANY POINT? |
| 29. ADDITIONAL COMMENTS ON ALARM SYSTEM | | |

## PART F - PERIMETER LIGHTING

| YES | NO | PERIMETER LIGHTING *(X and complete as applicable)* |
|---|---|---|
| | | 30. ARE ALL PERIMETER AREAS LIGHTED DURING HOURS OF DARKNESS? |
| | | a. IF YES, WHAT TYPE OF LIGHTING IS USED? |
| | | b. IF NO, EXPLAIN |
| | | 31. LIGHTING SYSTEM DETAILS |
| | | a. IS LIGHTING: |
| | | (1) MANUAL? |
| | | (2) AUTOMATIC |
| | | b. ARE ALL ENTRANCE AND EXIT GATES WELL LIGHTED? *(If any exceptions, explain)* |
| | | c. DOES PERIMETER LIGHTING ALSO COVER THE BUILDINGS? |
| | | d. IF LIGHTS BURN OUT, DO LIGHT PATTERNS OVERLAP? |
| | | e. WHO IS RESPONSIBLE FOR TURNING LIGHTS ON AND OFF? |
| | | f. WHO IS RESPONSIBLE FOR LIGHTING MAINTENANCE? |
| | | g. ARE THERE SUPPLIES ON HAND FOR MAINTENANCE OF LIGHTING SYSTEM *(Bulbs, fuses, etc.)*? |
| | | h. ARE GUARDS: |
| | | (1) EXPOSED BY LIGHTING? |
| | | (2) PROTECTED BY LIGHTING? |
| | | i. ARE GATES LIGHTED? |
| | | j. DO LIGHTS AT GATE ILLUMINATE INTERIOR OF VEHICLES? |
| | | k. ARE CRITICAL AND VULNERABLE AREAS WELL ILLUMINATED? |

WHEN FILLED IN

| 31. LIGHTING SYSTEM DETAILS *(Continued)* | | |
|---|---|---|
| YES | NO | |
| | | l. ARE PERIMETER LIGHTS WIRED IN: |
| | | (1) SERIES? |
| | | (2) PARALLEL? |
| | | m. IS THERE AN AUXILIARY POWER SOURCE AVAILABLE? |
| | | n. IF THERE IS AN AUXILIARY POWER SOURCE, IS THERE AN AUTOMATIC SWITCH? |
| | | o. IF THERE IS AN AUTOMATIC SWITCH FOR THE AUXILIARY POWER SOURCE, HOW LONG DOES IT TAKE TO SWITCH TO AUXILIARY POWER? |
| | | p. IF THERE IS AN AUXILIARY POWER SOURCE, IS THERE A MANUAL SWITCH? |
| | | q. IF THERE IS A MANUAL SWITCH FOR THE AUXILIARY POWER SOURCE, WHO IS RESPONSIBLE FOR IT? |

32. ADDITIONAL COMMENTS ON LIGHTING SYSTEM

## PART G - GUARD SERVICE

| YES | NO | *(X one)* | |
|---|---|---|---|
| | | 33. IS A GUARD SERVICE EMPLOYED? IF YES, PROVIDE DETAILS IN THE APPROPRIATE SPACE. | |
| | | a. CONTRACTOR | b. U.S. MILITARY SERVICE |
| | | c. FOREIGN MILITARY ORGANIZATION | d. FOREIGN POLICE AGENCY |

34. AGENCY/CONTRACTOR PROVIDING GUARD SERVICES

a. AGENCY/CONTRACTOR NAME

b. ADDRESS *(Include Street, City, State, and 9-digit ZIP Code, Country (if outside CONUS))*

| c. REPRESENTATIVE NAME *(Last, First, Middle Initial)* | d. TELEPHONE NUMBER *(Include area code)* |
|---|---|
| | |

35. HAVE WRITTEN INSTRUCTIONS BEEN ISSUED TO THE GUARDS AS TO THEIR DUTIES AND ASSIGNMENTS?

a. WHAT "EXTRA DUTIES" ARE PERFORMED BY GUARDS? WHAT IMPACT DO THESE DUTIES HAVE ON PROTECTIVE DUTIES?

b. WHAT DAY(S) IS THE FACILITY PROTECTED BY GUARDS?

☐ SUNDAY ☐ MONDAY ☐ TUESDAY ☐ WEDNESDAY ☐ THURSDAY ☐ FRIDAY ☐ SATURDAY

c. GUARD FORCE HOURS

| HOURS (1) | NUMBER OF GUARDS (2) |
|---|---|
| (a) DAY SHIFT | |
| (b) EVENING SHIFT | |
| (c) NIGHT SHIFT | |

36. CURRENT WAGES PAID FOR GUARD SERVICE

| a. HOURLY WAGE RATE FOR GUARDS | b. IS THIS COMPARABLE TO WAGES PAID TO GUARDS AT OTHER LOCAL FACILITIES? | c. IS THERE A CONTRACT IN EFFECT? |
|---|---|---|
| | | |

d. COMMENTS



WHEN FILLED IN

WHEN FILLED IN

| YES | NO | (X and complete as applicable) | |
|---|---|---|---|
| | | 37. DOES THE GUARD SERVICE HAVE INSURANCE AND OTHER COVERAGE FOR THE FOLLOWING: | |
| | | a. LIABILITY? | |
| | | b. WORKMEN'S COMPENSATION? | |
| | | c. HOLIDAYS? | |
| | | d. VACATION? | |
| | | e. SICK LEAVE? | |
| | | f. HOSPITALIZATION? | |
| | | g. DISABILITY INSURANCE? | |
| | | h. ACCIDENTAL DEATH? | |
| | | 38. ARE CLOCK STATIONS USED? | |
| | | a. IF YES, HOW MANY? | |
| | | b. ARE ALL CLOCK CHARTS REVIEWED DAILY? | |
| | | c. IF YES, BY WHOM? | |
| | | 39. ARE ACTIVITY REPORTS PREPARED BY GUARDS FOR EACH SHIFT? | |
| | | a. ARE IRREGULARITY REPORTS PREPARED? | |
| | | b. WHO REVIEWS REPORTS? | |
| | | 40. DO GUARDS HAVE KEYS TO: | |
| | | a. GATES? | |
| | | b. BUILDINGS? | |
| | | c. IF YES, HOW ARE KEYS CONTROLLED? | |
| | | 41. ARE GUARDS ARMED? IF YES, DESCRIBE EQUIPMENT. | |
| | | HAVE THEY RECEIVED WEAPONS INSTRUCTION? IF YES: | |
| | | a. HOW OFTEN? | b. BY WHOM? |
| | | 42. DO GUARDS TAKE PERIODIC POLYGRAPH EXAMINATIONS? IF YES: | |
| | | a. HOW OFTEN? | b. WHO GIVES THEM? |

| 43. WHAT TYPE OF COMMUNICATION SYSTEM IS USED? *(Enter "P" for Primary, "B" for Backup)* |
|---|
| (a) TELEPHONE? |
| (b) RADIO? |
| (c) PAK SETS? |
| (d) ALARM SWITCH? |
| (e) OTHER? |
| 44. ADDITIONAL COMMENTS ON GUARD SERVICE *(Compare and contrast guard service and compensation at DoD facility with other local commercial facilities given comparable protection)* |

**DD Form 2637, JAN 93** Page 10 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| PART H - INTERIOR<br>*(Use a separate page for each office, building, or residence)* | | |
|---|---|---|
| 45. DESCRIPTION OF BUILDING | | |
| a. CONSTRUCTION | b. LOCATION | c. PHYSICAL SECURITY ARRANGEMENTS |
| | | |
| | | |
| 46. PURPOSE/FUNCTION OF BUILDING *(Offices, residence, shop, laboratory, motor pool, etc.)* | | |
| 47. DOORS OR OPENINGS | | |
| a. DESCRIBE DOORWAY CONSTRUCTION; I.E., WOOD, STEEL, ETC. LIST IN SECTION FOR APPROPRIATE DOOR TYPE. USE ADDITIONAL SHEETS FOR MORE DOORS. | | |
| (1) EXTERNAL DOOR - VEHICLE | (2) EXTERNAL DOOR - | (3) INTERNAL FIRE DOOR |
| (a) DOOR FRAME | (a) DOOR FRAME | (a) DOOR FRAME |
| (b) DOOR JAM | (b) DOOR JAM | (b) DOOR JAM |
| (c) DOOR HINGES | (c) DOOR HINGES | (c) DOOR HINGES |
| (d) DOOR STRUCTURE | (d) DOOR STRUCTURE | (d) DOOR STRUCTURE |
| (e) REINFORCING MATERIALS | (e) REINFORCING MATERIALS | (e) REINFORCING MATERIALS |
| (f) OTHER *(Specify)* | (f) OTHER *(Specify)* | (f) OTHER *(Specify)* |
| (4) INTERNAL SECURITY DOOR | (5) INTERNAL DIVIDER DOOR | (6) OTHER DOOR |
| (a) DOOR FRAME | (a) DOOR FRAME | (a) DOOR FRAME |
| (b) DOOR JAM | (b) DOOR JAM | (b) DOOR JAM |
| (c) DOOR HINGES | (c) DOOR HINGES | (c) DOOR HINGES |
| (d) DOOR STRUCTURE | (d) DOOR STRUCTURE | (d) DOOR STRUCTURE |
| (e) REINFORCING MATERIALS | (e) REINFORCING MATERIALS | (e) REINFORCING MATERIALS |
| (f) OTHER *(Specify)* | (f) OTHER *(Specify)* | (f) OTHER *(Specify)* |
| b. DESCRIBE TYPES OF SECURITY LOCKS USED *(Include name of manufacturer. Use additional sheets as necessary.)* | | |
| c. HOW ARE DOORS LOCKED OR SECURED DURING NONWORKING HOURS? | | |
| d. WHO IS RESPONSIBLE FOR MAKING SURE DOORS ARE LOCKED? | | |
| e. DESCRIBE WINDOW CONSTRUCTION | | |

| YES | NO | *(X and complete as applicable)* |
|---|---|---|
| | | (1) ARE HINGES AND LOCK HASPS SECURELY INSTALLED? |
| | | (2) ARE ALL WINDOWS THAT ARE NOT USED PERMANENTLY LOCKED? |
| | | (3) ARE ALL ACCESSIBLE WINDOWS PROTECTED BY HEAVY WIRE MESH OR BARS? |
| | | (4) IF WINDOWS ARE COVERED BY WIRE MESH, ARE THE MESH COVERINGS: |
| | | (a) FASTENED FROM THE INSIDE? |
| | | (b) SECURED WITH LOCKS? |
| | | (5) DESCRIBE WINDOW FRAMES IN TERMS OF MATERIALS USED AND TYPE OF CONSTRUCTION. |
| | | (6) HAVE WINDOW PANES BEEN HARDENED? IF YES, HOW? |
| | | (7) IF WINDOWS CAN BE OPENED AND ARE LOCKED, ARE THEY PROTECTED BY: |
| | | (a) ORDINARY WINDOW LEVER LOCKS? |
| | | (b) KEY LOCKS? |
| | | (8) ARE WINDOWS FACING ON THE PERIMETER SECURED? |
| | | (9) ARE ALL ACCESSIBLE SKYLIGHTS, DOORS, AND OTHER OPENINGS ADEQUATELY SECURED? |
| | | (10) ARE THERE ANY LADDERS (PERMANENT AND NONPERMANENT) THAT SHOULD BE REMOVED, SECURED, OR BLOCKED FROM UNAUTHORIZED USE? |

**DD Form 2637, JAN 93** Page 11 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## PART I - OBSCURE OPENINGS

| YES | NO | OBSCURE OPENINGS *(X and complete as applicable)* |
|---|---|---|
| | | 48. ARE THERE ANY SIDEWALK ELEVATORS AT THIS FACILITY? IF YES: |
| | | a. ARE SIDEWALK ELEVATORS PROPERLY SECURED WHEN NOT IN OPERATION? |
| | | b. ARE SIDEWALK ELEVATORS SECURED DURING OPERATION? |
| | | 49. DO STORM SEWERS OR UTILITY TUNNELS BREACH THE OUTER BARRIER? IF YES: |
| | | a. ARE THESE SEWERS OR TUNNELS SECURED? |
| | | b. ARE THERE ANY OPENINGS FROM THESE SEWERS OR TUNNELS; I.E., MANHOLES INSIDE THE FACILITY? IF YES, DESCRIBE. |

50. DESCRIBE PROTECTION AFFORDED TO ALL POWER FACILITIES, TRANSFORMERS, AND UTILITIES EQUIPMENT.

## PART J - OFFICE OPERATIONS/ACCESS CONTROL

51. WHAT ARE NORMAL WORKING HOURS?

| | HOURS (1) | NUMBER OF PERSONNEL (2) | NUMBER OF SUPERVISORS (3) |
|---|---|---|---|
| a. DAY SHIFT | | | |
| b. EVENING SHIFT | | | |
| c. NIGHT SHIFT | | | |

52. HOURS OF OPERATION PER DAY

| SUNDAY | MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY | SATURDAY |
|---|---|---|---|---|---|---|
| | | | | | | |

| YES | NO | 53. EMPLOYEE IDENTIFICATION *(X and complete as applicable)* | | |
|---|---|---|---|---|
| | | a. IS EMPLOYEE INGRESS/EGRESS RESTRICTED TO CONTROLLED ENTRANCES AND EXITS? | | |
| | | b. IF YES, IS ACCESS CONTROLLED BY: *(Explain briefly in appropriate blocks)* | | |
| | | (1) BADGE | (2) GUARD | (3) RECEPTIONIST |
| | | (4) PASS | (5) KEY | |
| | | (6) COMMENTS | | |
| | | c. DO ALL EMPLOYEES HAVE BADGES? | | |
| | | d. DO ALL EMPLOYEES WEAR BADGES WITH PICTURES ON THEM? | | |
| | | e. IS THE INGRESS/EGRESS CONTROL POINT USED FOR EMPLOYEES THE SAME AS THE ONE USED FOR VISITORS, VENDORS, REPAIRMEN, ETC.? | | |

54. WHO OPENS THE FACILITY IN THE MORNING?

55. WHO CLOSES THE FACILITY IN THE EVENING?

56. ARE THERE ANY OTHER OBSCURE OPENINGS CAUSED BY ANIMALS, CHILDREN, EROSION, ETC.?

57. ADDITIONAL COMMENTS ON ACCESS CONTROL.

WHEN FILLED IN

## PART K - PARKING

58. PARKING AREA(S) *(Use extra sheets as necessary.)*

| | a. OUTSIDE OF BARRIER | b. INSIDE OF BARRIER | c. INSIDE OF BUILDINGS |
|---|---|---|---|
| (1) SIZE | | | |
| (2) SURFACE TYPE | | | |
| (3) LIGHTING | | | |
| (4) NUMBER OF VEHICLES DAILY | | | |
| (5) DISTANCE TO FENCE | | | |
| (6) DISTANCE TO NEAREST BUILDING | | | |
| (7) SURVEILLANCE BY | | | |
| (a) CCTV | | | |
| (b) GUARD | | | |
| (c) ROVING PATROL | | | |
| (8) NOT SUBJECT TO SURVEILLANCE | | | |
| (9) CONTROLLED BY PERMITS OR DECALS | | | |

59. LOCATION OF VISITOR PARKING

60. ADDITIONAL COMMENTS ON PARKING *(Topography of parking areas, obstructions, access to streets, etc.)*

61. PARKING AREA(S) *(Fill in one set for each parking area. Use additional sheets as necessary.)*

a. APPROXIMATE SIZE

| b. IS THIS PARKING AREA INSIDE FACILITY FENCE? | c. IS THIS PARKING AREA OUTSIDE FACILITY FENCE? |
|---|---|
| d. DISTANCE FROM NEAREST VEHICLE TO FENCE | e. NUMBER OF VEHICLES PARKED DAILY |

## PART L - VENDOR AND VISITOR CONTROL

62. HOW ARE VENDORS CONTROLLED? *(Describe briefly)*

a. PERMANENT (DAILY) VENDORS

| (1) ESCORTED | (2) BADGE | (3) LOG *(Sign in/out)* |
|---|---|---|

b. PERIODIC VENDORS

| (1) ESCORTED | (2) BADGE | (3) LOG *(Sign in/out)* |
|---|---|---|

63. HOW ARE VISITORS CONTROLLED? *(X as applicable)*

| (1) ESCORTED | (2) BADGE | (3) LOG *(Sign in/out)* |
|---|---|---|

| YES | NO | *(X each question as appropriate)* |
|---|---|---|
| | | 64. ARE VEHICLES INSPECTED? |
| | | 65. IS A SINGLE INGRESS/EGRESS POINT USED FOR ALL VISITORS, INCLUDING VENDORS, REPAIRMEN, ETC.? |
| | | 66. IS A PROPERTY PASS SYSTEM USED FOR PROPERTY REMOVAL? |

**DD Form 2637, JAN 93** Page 13 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| PART L - VENDOR AND VISITOR CONTROL *(Continued)* | | | |
|---|---|---|---|
| 67. ADDITIONAL COMMENTS ON VENDOR/VISITOR CONTROL | | | |
| **PART M - CONTRACT PERSONNEL** | | | |
| 68. JANITORIAL SERVICE | | | |
| a. CONTRACTOR NAME | | | |
| b. NAME OF SUPERVISOR *(Last, First, Middle Initial)* | | | |
| c. ADDRESS *(Include Street, City, State, and 9-digit ZIP Code)* | | | |
| d. HOW LONG HAS SERVICE BEEN SUPPLIED? | e. WORKING PERIOD | f. NUMBER OF PERSONNEL | |
| 69. OTHER CONTRACTORS WORKING IN THE FACILITY *(Not guard, alarm, or janitorial. Attach separate sheet for each contractor)* | | | |
| a. CONTRACTOR NAME | | | |
| b. ADDRESS *(Include Street, City, State, and 9-digit ZIP Code)* | | | |
| c. TYPE OF WORK | | | |

| YES | NO | 70. CONTRACTOR DETAILS *(X as appropriate)* |
|---|---|---|
| | | a. DO CONTRACTOR PERSONNEL HAVE TO SIGN REGISTER WHEN ENTERING OR LEAVING FACILITY? |
| | | b. IS THERE AN UP-TO-DATE LIST OF NAMES AND ADDRESS OF ALL CONTRACTOR PERSONNEL? |
| | | c. DO VEHICLES OF CONTRACTOR EMPLOYEES WHO ENTER THE FACILITY HAVE AN IDENTIFYING DECAL? |
| | | d. ARE THE VEHICLES OF CONTRACTORS INSPECTED? |
| | | e. IS THERE AN IDENTIFICATION SYSTEM FOR CONTRACTORS? |

71. ADDITIONAL COMMENTS ON CONTRACT PERSONNEL

**DD Form 2637, JAN 93** Page 14 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## PART N - TRASH DISPOSAL

72. TRASH REMOVAL SERVICE

a. CONTRACTOR NAME

b. ADDRESS *(Include Street, City, State, and 9-digit ZIP Code)*

73. HOW OFTEN IS TRASH REMOVED?

| YES | NO | |
|---|---|---|
| | | a. IS TRASH PERIODICALLY INSPECTED? *(Explain)* |
| | | b. IS TRASH REMOVED FROM FACILITY UNDER SUPERVISION? *(Explain)* |

74. ADDITIONAL COMMENTS ON TRASH DISPOSAL

## PART O - EMERGENCY PLANS

75. WHO IS RESPONSIBLE FOR EMERGENCY PLANS FOR: *(Indicate by X whether a plan exists)*

| INCIDENT/THREAT | PLAN a. | RESPONSIBLE OFFICE b. | POINT OF CONTACT c. |
|---|---|---|---|
| (1) BOMB THREAT | | | |
| (2) FIRE | | | |
| (3) TORNADO | | | |
| (4) HURRICANE | | | |
| (5) FLOOD | | | |
| (6) EARTHQUAKE | | | |
| (7) EXPLOSION | | | |
| (8) LOSS OF UTILITY SERVICE | | | |
| (9) CIVIL DISORDER | | | |
| (10) HAZARDOUS MATERIAL INCIDENT | | | |

| YES | NO | |
|---|---|---|
| | | 76. PERSONNEL SAFETY |
| | | a. NAME OF SAFETY SUPERVISOR *(Last, First, Middle Initial)* |
| | | b. ARE SAFETY PLANS POSTED? IF YES, ARE THEY: |
| | | (1) UP-TO-DATE? |
| | | (2) CLEAR AND CONCISE? |
| | | 77. IS THERE AN EMERGENCY PLAN COORDINATOR? IF YES, ENTER: |
| | | NAME *(Last, First, Middle Initial)* |
| | | 78. HAVE EMERGENCY PLANS BEEN TESTED? IF YES, WHEN WAS LAST TEST? |
| | | 79. ARE DRILLS CONDUCTED? |

80. ADDITIONAL COMMENTS ON EMERGENCY PLANS

**DD Form 2637, JAN 93** Page 15 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## PART P - OFFICE PROCEDURES

81. MAIL HANDLING

a. WHO HANDLES MAIL?

| (1) INCOMING | (2) OUTGOING |
|---|---|
| | |

b. WHERE IS MAIL OPENED?

| YES | NO | *(For each item, X one and explain any pertinent procedures)* |
|---|---|---|
| | | c. ARE ALL PACKAGES DISTRIBUTED? *(If No, explain pickup procedures)* |
| | | d. HAVE INDIVIDUALS INVOLVED IN MAIL HANDLING BEEN INSTRUCTED ABOUT LETTER BOMBS AND PROCEDURES FOR HANDLING? |
| | | 82. IS THERE A FACILITY POLICY REQUIRING WRITTEN OFFICE PROCEDURES? IF SO, WHERE ARE COPIES KEPT? |

83. ADDITIONAL COMMENTS ON OFFICE PROCEDURES

## PART Q - INTERIOR ALARM SYSTEMS

| YES | NO | 84. ARE ALARMS USED IN BUILDINGS? IF YES, DESCRIBE FOR EACH SYSTEM. USE ADDITIONAL SHEETS AS NECESSARY. |
|---|---|---|
| | | |

a. MANUFACTURER

| b. TYPE | c. DATE OF INSTALLATION *(YYMMDD)* |
|---|---|
| d. SERVICED BY | e. DATE OF LAST INSPECTION *(YYMMDD)* |

f. DESCRIBE PROCEDURE FOR ACTIVATING AND DEACTIVATING ALARM SYSTEM

g. WHICH EMPLOYEES ARE ALLOWED TO TURN OFF THE ALARM SYSTEM?

## PART R - MISCELLANEOUS

| YES | NO | MISCELLANEOUS *(For each item, X one and explain any pertinent procedures)* |
|---|---|---|
| | | 85. ARE ALL BUILDINGS LOCKED AT NIGHT? IF YES, WHO IS RESPONSIBLE? |
| | | 86. ARE LIGHTS LEFT ON IN BUILDINGS AT NIGHT? IF YES: |
| | | a. TYPE OF LIGHTING / b. WHO IS RESPONSIBLE |
| | | 87. ARE FIRE STAIRWELLS USED ON A DAILY BASIS? |
| | | 88. DOES THE FACILITY USE ELEVATORS? IF YES: |
| | | a. WHAT CONTROL IS EXTENDED OVER THEIR USE? |
| | | b. DO ELEVATORS CONNECT CONTROLLED ACCESS FLOORS WITH PUBLIC ACCESS FLOORS? IF YES, DESCRIBE CONTROLS ON CONTROLLED ACCESS FLOORS. |

**DD Form 2637, JAN 93** Page 16 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| SECTION II - RESIDENTIAL SECURITY |
|---|
| **PART A - GENERAL INFORMATION** |
| 1. TYPE OF RESIDENCE |
| 2. ADDRESS/LOCATION *(Include Street, City, State, and 9-digit ZIP Code)* |
| 3. INDIVIDUAL(S) CONDUCTING SURVEY |
| a. NAME *(Last, First, Middle Initial)* |
| b. RANK/GRADE |
| c. ORGANIZATION |
| d. TELEPHONE NUMBER *(Include Area Code)* |
| 4. SURVEY DATE *(YYMMDD)* |
| 5. DESCRIPTION OF RESIDENCE *(Construction, location, plat, obstructed views, etc.)* |
| 6. INDIVIDUAL(S) INTERVIEWED *(Add additional names in Section IV.)* |
| a. NAME *(Last, First, Middle Initial)* |
| b. RANK/GRADE |
| c. ORGANIZATION |
| d. TELEPHONE NUMBER *(Include Area Code)* |
| 7. LOCATION OF RESIDENCE *(Comment next to appropriate item(s))* |
| a. URBAN |
| b. SUBURBAN |
| c. INCORPORATED |
| d. UNINCORPORATED |
| e. GOVERNMENT INSTALLATION |
| f. OTHER |
| 8. ATTACH PLOT PLAN OF RESIDENCE SHOWING:<br>● Compass rose showing north.<br>● Perimeter barrier with gates.<br>● Parking areas/facilities.<br>● Any planned remodeling or expansion of residence. |
| 9. ATTACH AS-BUILT DRAWING OF THE RESIDENCE SHOWING:<br>● Construction of exterior/interior walls.<br>● Location of all windows, doors, and skylights.<br>● Location and size of all vents, utility openings, etc.<br>● Electrical runs, outlets, and switches. |

**DD Form 2637, JAN 93** Page 17 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| PART B - EXTERIOR | | |
|---|---|---|
| YES | NO | EXTERIOR *(X and complete as applicable)* |
| | | 10. IS EXTERIOR LIGHTING CHECKED REGULARLY AND BULBS REPLACED? *(If Yes, by whom?)* |
| | | 11. IS EXTERIOR FENCE/WALL CHECKED REGULARLY AND ANY BREAKS OR WASHOUTS REPAIRED? |
| | | 12. IS VEGETATION CUT BACK NEAR HOUSE AND EXTERIOR WALL/FENCE? *(If Yes:)* |
| | | a. HOW OFTEN? / b. WHO IS RESPONSIBLE? |

| PART C - RESIDENTIAL BUILDING | | |
|---|---|---|
| YES | NO | BUILDING *(X as applicable and comment if applicable. Use continuation sheets as necessary.)* |
| | | 13. ARE DOORS KEPT LOCKED WHEN AT HOME? |
| | | 14. ARE EXTERIOR DOORS DOUBLE LOCKED? |
| | | 15. IS THERE A SECONDARY INTERIOR DOOR THAT IS DOUBLE LOCKED OR HAS THROW BOLTS? |
| | | 16. ARE WINDOWS LEFT OPEN WHEN NO ONE IS HOME? |
| | | 17. ARE WINDOWS LEFT OPEN WHEN RESIDENTS ARE SLEEPING? |
| | | a. DO THEY HAVE GRILLES OR BARS? |
| | | b. DO THEY HAVE SECURITY PINS TO HOLD THEM PARTIALLY OPEN? |
| | | 18. ARE INTERIOR LIGHTS TURNED OFF AT NIGHT? |
| | | 19. ARE SPARE KEYS HIDDEN UNDER MAT OR OTHERWISE NEAR ENTRANCE? |
| | | 20. IS NAME OF RESIDENT ON MAILBOX OR NEAR DOORBELL? |
| 21. DESCRIBE RESISTANCE OF BUILDING TO PENETRATION BY: | | |
| a. HAND TOOLS | b. POWER ASSISTED HAND TOOLS | c. POWER TOOLS / d. EXPLOSIVE CUTTING TOOLS / e. OTHER DEVICES |

| PART D - OPERATIONAL CONSIDERATIONS | | |
|---|---|---|
| YES | NO | OPERATIONAL CONSIDERATIONS *(X as applicable)* |
| | | 22. IS THERE A FAMILY DOG? |
| | | IF YES, DOES IT REACT TO EXTERNAL NOISE? |
| | | 23. DURING EXTENDED ABSENCES: |
| | | a. DOES SOMEONE HOUSE-SIT OR CHECK THE RESIDENCE ON A DAILY BASIS? |
| | | b. ARE LIGHTS, RADIO, OR TV TURNED ON AND OFF AUTOMATICALLY BY TIMERS IN THE EVENING? |
| | | 24. WHEN THE RESIDENCE IS UNOCCUPIED IN THE EVENING, ARE LIGHTS AND RADIO/TV LEFT ON? |
| | | 25. ARE WORKMEN ALLOWED TO BE IN HOUSE OR EXTERIOR GROUNDS WHEN RESIDENTS ARE ABSENT? |
| | | 26. ARE WORKMEN SCHEDULED IN ADVANCE? |
| | | 27. ARE SERVANTS CHECKED BY SECURITY? |

| PART E - SAFEHAVEN | | |
|---|---|---|
| YES | NO | SAFEHAVEN *(X as applicable. Use continuation sheets as necessary for detail.)* |
| | | 28. DO SAFEHAVEN WALLS PROVIDE 15 MINUTES OF PENETRATION RESISTANCE? |
| | | 29. ARE DOORS EQUIPPED WITH BOLTWORKS, THROWBOLTS OR SIMILAR SECURITY DEVICES? |
| | | 30. DO DOORS PROVIDE 15 MINUTES OF PENETRATION RESISTANCE AND BALLISTIC PROTECTION *(See 28 above.) (Describe)* |
| | | 31. ARE PRIMARY/SECONDARY COMMUNICATIONS PROVIDED? IF YES: |
| | | a. DESCRIBE |
| | | b. DO THEY OPERATE? |
| | | c. WHO DO THEY NET WITH? |
| | | 32. ARE THE FOLLOWING ITEMS AVAILABLE: |
| | | a. FLASHLIGHTS? |
| | | b. CANDLES? |
| | | c. RADIO? |
| | | d. FIRE EXTINGUISHER? |
| | | e. FIREARMS AND AMMUNITION? |
| | | f. WATER? |
| | | g. TELEPHONE DIRECTORY/EMERGENCY NUMBERS? |

**DD Form 2637, JAN 93** Page 18 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## SECTION III - HIGH-RISE COMMERCIAL BUILDINGS

### PART A - PRESURVEY INFORMATION AND MATERIAL TO BE OBTAINED

1. LOCATION/ADDRESS OF BUILDING *(Include Street, City, State, and 9-digit ZIP Code)*

2. SURVEY DATE *(YYMMDD)*

3. INDIVIDUAL(S) INTERVIEWED *(Add additional names in Section IV.)*

| a. NAME *(Last, First, Middle Initial)* | b. RANK/GRADE/TITLE | |
|---|---|---|
| c. ORGANIZATION | d. TELEPHONE NUMBER *(Include Area Code)* | e. SURVEY DATE *(YYMMDD)* |

4. DESCRIPTION OF ENTIRE PREMISES BEING SURVEYED *(Construction, materials, tenants, services, functions performed by tenants, etc.)*

5. ATTACH PLOT PLAN OF THE BUILDING(S):
- Show first floor, basement, and any other floors that differ in comparison to the design of the other floors.
- It may suffice to have a plan of only one floor above the first if all others are similar and contain no unique areas or features relating to security.
- Show any floors reserved for service equipment.
- Show all doors at street level used by pedestrians, delivery, fire exit doors, etc.

6. IS THE PREMISES A SINGLE BUILDING, OR IS THERE MORE THAN ONE BUILDING INVOLVED?

a. IF MORE THAN ONE, HOW DO THESE BUILDINGS RELATE TO EACH OTHER? *(Underground connection, walkway, breezeway, parking area, open space, etc.)*

b. HOW FAR APART ARE THEY?

| YES | NO | |
|---|---|---|
| | | 7. ARE THERE ANY OUTSIDE GROUNDS INVOLVED? |
| | | 8. ARE THERE ANY CONNECTING PARKING AREAS EITHER INSIDE OR OUTSIDE THE BUILDING COMPLEX? |
| | | 9. WHAT TYPES OF TENANTS DOES THE BUILDING HOUSE? |
| | | a. RETAIL STORES? |
| | | b. BUSINESS OFFICES? |
| | | c. PROFESSIONAL OFFICES? |
| | | d. BANKS? |
| | | 10. IS THERE ONE MAJOR TENANT IN THE BUILDING? IF YES: |
| | | a. HOW MANY FLOORS DOES THIS TENANT OCCUPY? / b. WHICH FLOORS? |

**DD Form 2637, JAN 93** Page 19 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| PART B - SECURITY AT STREET LEVEL AND BELOW | | |
|---|---|---|
| 11. HOW MANY DOORS ARE THERE AT STREET LEVEL USED BY PEDESTRIANS? | | |
| 12. DESCRIBE LOCATION AND DESIGNATION OF PEDESTRIAN DOORS *(These should also be marked on attached plot plan.)* | | |
| 13. ARE THERE ANY OTHER DOORS AT STREET LEVEL USED FOR DELIVERY, FIRE EXITS, ETC.? | | |
| 14. DESCRIBE LOCATION AND DESIGNATION OF OTHER DOORS *(These should also be marked on attached plot plan.)* | | |
| 15. HOW ARE DOORS SECURED TO PREVENT UNAUTHORIZED USE? | | |
| 16. HOW ARE DOORS CONTROLLED WHEN OPEN? | | |
| 17. WINDOWS | | |
| a. HOW MANY WINDOWS ARE THERE AT GROUND LEVEL OR BELOW? | | |
| b. HOW ARE THESE WINDOWS PROTECTED AGAINST UNAUTHORIZED ENTRY/EXIT? | | |
| YES | NO | c. COULD ANY WINDOW BE OPENED OR REMOVED FROM THE OUTSIDE? *(X one. If yes, explain.)* |
| | | 18. DOES THE BUILDING HAVE A SIDEWALK ELEVATOR? *(If Yes:)* |
| a. WHAT SECURITY IS PROVIDED WHEN THE ELEVATOR IS IN USE? | | |
| b. HOW IS ELEVATOR SECURED WHEN NOT IN USE? | | |
| YES | NO | 19. ARE THERE ANY STORM SEWERS OR UTILITY TUNNELS ENTERING OR RUNNING UNDER THE BUILDING? *(If Yes:)* |
| | | a. ARE THESE OF SUFFICIENT SIZE *(96 square inches)* OR SO LOCATED AS TO PERMIT ILLEGAL ENTRY? |
| b. IF YES, HOW CAN THEY BE PROTECTED TO DENY SUCH ENTRY? | | |

**DD Form 2637, JAN 93** Page 20 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## PART C - LOBBY

20. OPEN PERIODS

a. DURING WHAT HOURS IS THE LOBBY OPEN TO THE GENERAL PUBLIC?

| (1) SUNDAY | (2) MONDAY | (3) TUESDAY | (4) WEDNESDAY | (5) THURSDAY | (6) FRIDAY | (7) SATURDAY |
|---|---|---|---|---|---|---|
| | | | | | | |

| YES | NO | *(X and complete as applicable)* |
|---|---|---|
| | | b. IS ANY CONTROL EXERCISED OVER PERSONNEL MOVEMENT DURING THIS TIME? |
| | | c. IS IT POSSIBLE TO HAVE ANY PERSONNEL CONTROL IN THE LOBBY DURING OPEN PERIODS? |

d. DESCRIBE CONTROLS CURRENTLY IN FORCE

e. HOW MANY BANKS OF ELEVATORS ARE THERE IN THE LOBBY?

| YES | NO | *(X and complete as applicable)* |
|---|---|---|
| | | f. ARE THERE ANY CONTROLS EXERCISED AT THE ELEVATORS? |
| | | g. DO ALL OR PART OF THE ELEVATORS DESCEND TO LOWER FLOORS? |
| | | h. IF YES, WHICH LEVELS DO THEY SERVE? |
| | | i. ARE SPECIAL ELEVATORS USED FOR FREIGHT? IF YES: |
| | | (1) DO FREIGHT ELEVATORS OPEN INTO THE LOBBY? |
| | | (2) IS THERE DIRECT ACCESS TO FREIGHT ELEVATORS FROM OUTSIDE THE BUILDING OR FROM LOADING DOCKS? |
| | | (3) IF YES, IS ANY TYPE OF PROTECTION PROVIDED AGAINST SURREPTITIOUS USE OF SUCH ELEVATORS FROM THESE AREAS? |
| | | j. ARE ELEVATORS: |
| | | (1) MANUALLY OPERATED? |
| | | (2) AUTOMATICALLY OPERATED? |
| | | k. DO ELEVATORS THAT SERVICE THE PARKING AREAS STOP AT THE LOBBY EXIT? |
| | | l. ARE ELEVATORS OR ESCALATORS SUPERVISED? IF YES, TO WHAT EXTENT? |
| | | m. ARE THERE ANY OPEN STAIRWAYS TO LOWER OR UPPER LEVELS OF THE BUILDING? |
| | | n. DO DOORS FROM FIRE STAIRWAYS LEADING TO UPPER FLOORS ENTER THE LOBBY OR FLOORS BELOW? |

o. IF YES, WHAT PROTECTION IS PROVIDED FROM UNAUTHORIZED AND/OR FORCED ENTRY FROM OUTSIDE THROUGH THESE DOORS?

21. CLOSED PERIODS

a. DURING WHAT HOURS IS THE BUILDING OPEN TO TENANTS BUT CLOSED TO THE GENERAL PUBLIC?

| (1) SUNDAY | (2) MONDAY | (3) TUESDAY | (4) WEDNESDAY | (5) THURSDAY | (6) FRIDAY | (7) SATURDAY |
|---|---|---|---|---|---|---|
| | | | | | | |

b. HOW ARE DOORS AND OTHER OPENINGS CONTROLLED DURING THESE SEMI-CLOSED PERIODS?

| YES | NO | |
|---|---|---|
| | | c. IS THERE ANY CONTROL OVER TENANTS ENTERING OR LEAVING WHEN THE BUILDING IS CLOSED TO THE GENERAL PUBLIC? |

d. IF YES, HOW ARE THESE PERSONS IDENTIFIED AND CHECKED IN AND OUT?



WHEN FILLED IN

WHEN FILLED IN

| 21. CLOSED PERIODS *(Continued)* | | |
|---|---|---|
| YES | NO | e. ARE EQUIPMENT REPAIRMEN PERMITTED IN THE BUILDING DURING THESE SEMI-CLOSED PERIODS? |
| | | f. IF YES, HOW ARE THESE PERSONS CONTROLLED? |
| YES | NO | *(X and complete as applicable)* |
| | | g. ARE THERE ANY RULES PERTAINING TO THE REMOVAL OF EQUIPMENT, PACKAGES, ETC., DURING THESE PERIODS? |
| | | h. IS THERE ANY TIME THAT THE BUILDING IS CLOSED TO BOTH PUBLIC AND TENANTS? |
| | | i. IF YES, HOW IS THIS ACCOMPLISHED? |
| | | j. IS THERE A PROCEDURE ESTABLISHED TO ADMIT TENANTS, WORKMEN, ETC., ON AN EMERGENCY BASIS WHEN THE BUILDING IS COMPLETELY CLOSED? |

## PART D - CUSTODIAL PERSONNEL

| | | |
|---|---|---|
| 22. IS THE CUSTODIAL WORK IN THE BUILDING DONE BY BUILDING EMPLOYEES OR BY CONTRACT PERSONNEL? | | |
| 23. DURING WHAT HOURS DO CUSTODIAL PERSONNEL WORK? | | |
| 24. HOW IS CUSTODIAL SERVICE SUPERVISED? | | |
| YES | NO | *(X and complete as applicable)* |
| | | 25. DO CUSTODIAL PERSONNEL HAVE KEYS TO THE VARIOUS AREAS? |
| | | 26. DO ANY TENANTS HAVE THEIR OWN CUSTODIAL OR MAID SERVICE? IF YES: |
| | | a. DURING WHAT HOURS DO CUSTODIAL PERSONNEL OR MAIDS WORK? |
| | | b. HOW IS THIS SERVICE SUPERVISED? |
| | | c. TO WHICH AREAS DO CUSTODIAL PERSONNEL OR MAIDS HAVE KEYS? |
| 27. HOW ARE CUSTODIAL PASS KEYS CONTROLLED? | | |
| YES | NO | *(X and complete as applicable)* |
| | | 28. IS TRASH REMOVED BY CUSTODIAL PERSONNEL OR MAIDS? IF YES, WHAT SECURITY PROCEDURES ARE FOLLOWED? |
| | | 29. IS THERE ANY CONTROL EXERCISED OVER THE ENTERING AND LEAVING OF CUSTODIAL PERSONNEL OR MAIDS? IF YES, HOW IS THIS ACCOMPLISHED? |
| | | 30. ARE PACKAGES CARRIED BY CUSTODIAL PERSONNEL INSPECTED WHEN ENTERING OR LEAVING THE BUILDING? IF NO, EXPLAIN. |



WHEN FILLED IN

WHEN FILLED IN

| PART E - BUSINESS FIRMS IN THE BUILDING | | |
|---|---|---|
| YES | NO | *(X and complete as applicable)* |
| | | 31. ARE THERE ANY RETAIL BUSINESS FIRMS IN THE BUILDING? IF YES: |
| | | a. ARE THEY CONFINED TO THE STREET FLOOR AND BELOW? |
| | | b. ARE THE AREAS OCCUPIED BY THESE FIRMS TO BE INCLUDED IN THE SURVEY? |
| | | c. DO THESE BUSINESSES AFFECT THE SECURITY OF THE BUILDING WHEN OTHER PARTS OF IT ARE CLOSED? |
| | | 32. ARE THERE ANY BUSINESSES OR PROFESSIONAL OFFICES THAT HAVE TO BE OPENED TO THE PUBLIC DURING NORMALLY CLOSED OR SEMI-CLOSED HOURS FOR THE BUILDING? IF YES: |
| a. HOW DOES THIS AFFECT THE OVERALL SECURITY? | | |
| b. HOW IS IT HANDLED? | | |
| YES | NO | |
| | | 33. ARE ANY OF THE BUSINESS ESTABLISHMENTS OR OFFICES PROTECTED BY SEPARATE ANTI-INTRUSION ALARMS WHEN |
| | | 34. DO SECURITY PERSONNEL HAVE ANY RESPONSIBILITY IN CONNECTION WITH THESE ALARM SYSTEMS? |
| **PART F - BASEMENTS, SUB-BASEMENTS, AND PARKING** | | |
| 35. HOW MANY LEVELS OF OPERATING AREA ARE THERE IN THE BUILDING BELOW GROUND? | | |
| 36. HOW IS ENTRANCE MADE TO THESE AREAS FROM OUTSIDE? | | |
| YES | NO | *(X and complete as applicable)* |
| | | 37. ARE EQUIPMENT ROOMS, POWER ROOMS, SHOPS, AND STOREROOMS LOCKED WHEN NOT OCCUPIED BY OPERATING PERSONNEL? |
| | | 38. DOES THE BUILDING HAVE SUBLEVEL PARKING? IF YES: |
| | | a. HOW MANY LEVELS ARE THERE? |
| | | b. IS THIS FOR TENANT PARKING ONLY? |
| | | c. IS IT OPEN TO THE PUBLIC? |
| d. HOW IS THE PARKING FACILITY OPERATED OR CONTROLLED? | | |
| e. WHAT ARE THE LIGHTING CONDITIONS IN THE PARKING LEVELS? | | |
| f. ARE THESE AREAS COVERED BY CCTV? | | |
| g. DO SECURITY PERSONNEL TOUR PARKING LEVELS? | | |
| h. HOW ARE ENTRANCES AND EXITS TO PARKING AREAS CONTROLLED? | | |
| i. DURING WHAT HOURS ARE THEY OPEN? | | |

**DD Form 2637, JAN 93** Page 23 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

## PART G - ROOF AREAS

| YES | NO | ROOF AREAS |
|---|---|---|
| | | 39. DOES ANY PART OF THE ROOF OF THE BUILDING PERMIT ENTRY TO THE BUILDING BY CROSSING TO THE ROOF FROM THE ROOF OF ANOTHER BUILDING? |
| 40. HOW ARE EXITS FROM THE BUILDING TO THE ROOF CONTROLLED? | | |
| YES | NO | |
| | | 41. HAVE ANY MEASURES BEEN TAKEN TO DENY ACCESS TO THE ROOF FROM ADJACENT BUILDINGS? |
| | | 42. IS THE ROOF OF THE BUILDING USED FOR PERSONNEL ACTIVITIES, SUCH AS SWIMMING, DANCING, OTHER FORMS OF RECREATION, RESTAURANTS, OBSERVATION, ETC.? *(If Yes:)* |
| a. HOW IS THE ROOF PROTECTED AGAINST FIRE? | | |
| YES | NO | b. IS A FIRE INSPECTION MADE OF ROOFS WHEN SPECIAL ACTIVITIES ARE COMPLETED OR WHEN THE BUILDING IS SEMI-CLOSED OR CLOSED? |
| | | |
| c. IF YES, HOW SOON AFTER SPECIAL ACTIVITIES OR WHEN THE BUILDING IS SEMI-CLOSED OR CLOSED DOES THIS INSPECTION TAKE PLACE? | | |

## PART H - FIRE PROTECTION

| YES | NO | *(X and complete as applicable)* |
|---|---|---|
| | | 43. IS THE BUILDING EQUIPPED WITH A SPRINKLER SYSTEM? |
| | | a. IF YES, IS THE ENTIRE BUILDING SO PROTECTED? |
| | | b. IF NO, WHICH AREAS ARE COVERED OR NOT COVERED, WHICHEVER IS GREATER? |
| | | c. IF THE ENTIRE BUILDING DOES NOT HAVE A SPRINKLER SYSTEM, WHAT TYPE OF FIRE DETECTION IS USED? |
| 44. DESCRIBE THE FIRE PROTECTION SYSTEM, AND INDICATE THOSE PARTS OF THE BUILDING WHICH HAVE NO AUTOMATIC PROTECTION. *(Continue in Section IV, as necessary)* | | |
| 45. SPRINKLER SYSTEM DETAILS *(If applicable)* | | |
| a. HOW MANY RISERS FEED THE SPRINKLER SYSTEM? | | |
| YES | NO | |
| | | b. ARE THE RISERS EQUIPPED WITH WATERFLOW ALARMS? |
| | | c. IF YES, ARE THE ALARMS: |
| | | (1) LOCAL? |
| | | (2) PROPRIETARY? |
| | | (3) CENTRAL STATION? |
| | | (4) CONNECTED TO THE FIRE STATION? |
| | | 46. IS THE BUILDING EQUIPPED WITH AN AUDIBLE LOCAL ALARM SYSTEM TO ALERT TENANTS? IF YES: |
| | | a. IS THIS A CODED SYSTEM TO DESIGNATE WHICH FLOOR THE ALARM CAME FROM? |
| | | b. ARE THE ALARMS LOUD ENOUGH AND SO LOCATED AS TO ALERT ALL TENANTS IN THE BUILDING? |
| | | c. IS THE FIRST ALARM SILENT EXCEPT TO BUILDING MANAGEMENT EMPLOYEES, WHO IN TURN MUST SOUND THE GENERAL ALARM MANUALLY IF REQUIRED? |
| | | d. ARE THERE MANUAL FIRE-ALARM PULLBOXES LOCATED STRATEGICALLY ON EACH FLOOR OF THE BUILDING? |
| | | 47. IS EACH FLOOR OF THE BUILDING EQUIPPED WITH A NUMBER OF STRATEGICALLY LOCATED FIRE EXTINGUISHERS? |
| | | IF YES, ARE THESE EXTINGUISHERS REGULARLY INSPECTED OR CONDITIONED? |
| | | 48. IS EACH FLOOR OF THE BUILDING EQUIPPED WITH ONE OR MORE FIRE HOSES IN WALL CABINETS OR RACKS? IF YES: |
| | | a. ARE THE HOSE LINES CONNECTED TO THOSE RISERS WHICH ARE USED FOR THE SPRINKLER SYSTEM? |
| | | b. IF YES, IS WATER PRESSURE IN THE RISERS ON ALL FLOORS SUFFICIENT TO HANDLE BOTH SPRINKLERS AND |

**DD Form 2637, JAN 93** Page 24 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| YES | NO | |
|---|---|---|
| | | 48. (Continued) |
| | | c. IF NO, IS THE BUILDING EQUIPPED WITH FIRE PUMPS TO KEEP PRESSURE IN THESE LINES HIGH ENOUGH TO BE EFFECTIVE? IF YES: |
| | | (1) WHERE ARE THESE PUMPS LOCATED? |
| | | (2) WHO IS RESPONSIBLE FOR THESE PUMPS? (3) HOW OFTEN ARE THESE PUMPS TESTED? |
| | | d. ARE FIRE HOSE VALVES AT EACH HOSE STATION TESTED REGULARLY? |
| | | e. IS THE FIRE HOSE AND PLAY PIPE TESTED TO INSURE THAT IT IS NOT ROTTED, CUT, OR OBSTRUCTED? |
| | | 49. ARE THERE ANY FIRE WALLS DIVIDING FLOORS OF THE BUILDING? IF YES: |
| | | a. ARE OPENINGS BETWEEN PROTECTED BY FIRE DOORS? |
| | | b. ARE THE FIRE DOORS NORMALLY OPEN OR CLOSED? |
| | | c. IF OPEN, ARE THEY EQUIPPED WITH AUTOMATIC CLOSURES *(magnetic releases)* WHICH WOULD ACTIVATE IF A FIRE OCCURRED? |
| | | 50. IS THE BUILDING EQUIPPED WITH: |
| | | a. FIRE ESCAPES? |
| | | b. FIRE STAIRWELLS? |
| | | c. IF FIRE STAIRWELLS ARE USED: |
| | | (1) ARE THEY EQUIPPED WITH FANS TO BRING AIR FROM OUTSIDE TO BUILD UP POSITIVE AIR PRESSURE AND PREVENT SMOKE FROM SEEPING INTO THEM DURING FIRES? |
| | | (2) ARE THEY COMPARTMENTALIZED TO PROTECT AGAINST SMOKE SEEPAGE? |
| | | d. ARE FIRE DOORS TO FIRE STAIRWELLS MADE OF FIRE-RESISTANT OR FIREPROOF MATERIAL? |
| | | (1) ARE THESE DOORS EQUIPPED WITH APPROVED PANIC HARDWARE? |
| | | (2) ARE THESE DOORS KEPT CLOSED AT ALL TIMES? |
| | | (3) IF KEPT OPEN, ARE THESE DOORS EQUIPPED WITH CLOSURES *(magnetic releases)* WHICH WILL OPERATE IF A FIRE |
| | | 51. DOES EACH FLOOR OF THE BUILDING FORM A COMPARTMENT WHICH WOULD EFFECTIVELY BLOCK FIRE FROM SPREADING TO OTHER FLOORS? |
| | | 52. ARE AIR CONDITIONING AND VENTILATING FLUES EQUIPPED WITH DAMPERS WHICH WOULD CLOSE AUTOMATICALLY IN CASE OF FIRE? |
| | | IF YES, ARE THESE DAMPERS REGULARLY MAINTAINED AND TESTED? |
| | | 53. ARE OPENINGS WHERE WATER PIPES, WIRES, ETC., PASS THROUGH SOLID WALLS SEALED TO ELIMINATE SMOKE SEEPAGE FROM OTHER AREAS? |
| | | 54. ARE ELEVATORS TO BE USED FOR FIRE EVACUATION? IF YES: |
| | | a. ARE THE SHAFTS SEALED OR EQUIPPED WITH PRESSURE FANS TO RAISE POSITIVE AIR PRESSURE TO FORCE OUT |
| | | b. IS THERE A PLAN FOR AN ORDERLY METHOD OF EVACUATING EACH FLOOR? |
| | | 55. DOES THE FIRE DEPARTMENT HAVE LADDER TRUCKS THAT WILL REACH THE TOP FLOORS AND ROOF OF THE BUILDING? IF NO: |
| | | a. ARE PROCEDURES IN PLACE FOR HELICOPTER EVACUATION FROM THE ROOF? |
| | | b. WILL THE HELICOPTER EVACUATION PROCEDURES HANDLE THE TENANT POPULATION? |
| | | 56. ARE CERTAIN ELEVATORS SET ASIDE FOR USE BY THE FIRE DEPARTMENT? |
| | | 57. ARE ALL OS&V VALVES IN THE RISERS IN AN OPEN POSITION AND SEALED? |
| | | 58. HOW MANY PUBLIC FIRE DEPARTMENTS ARE AVAILABLE WITHIN A CITY BLOCK IN ANY DIRECTION FROM THE BUILDING? |
| | | 59. HOW MANY FIRE DEPARTMENT HOOKUPS ARE THERE ON THE OUTSIDE OF THE BUILDING? |
| | | 60. ARE THE BOILER ROOM AND OTHER MAINTENANCE AREAS PROPERLY POLICED? |
| | | 61. ARE THE TRASH CONTAINERS IN SERVICE HALLWAYS, CLOSETS, AND MAINTENANCE AREAS PROPERLY COVERED AND OF METAL CONSTRUCTION? |
| | | 62. IS ALL COMBUSTIBLE TRASH EITHER IMMEDIATELY REMOVED OR SAFELY STORED TO AVOID FIRES? |
| | | 63. ARE COMBUSTIBLES, SUCH AS PAINT, OIL, GASOLINE, ETC., STORED IN THE BUILDING? |
| | | 64. IS ALL FIRE-FIGHTING EQUIPMENT INSPECTED REGULARLY? |
| | | 65. IS A RECORD OF INSPECTION MAINTAINED? |
| | | 66. ARE CLEAR AND CONCISE INSTRUCTIONS POSTED FOR THE USE OF FIRE EXTINGUISHERS AND HOSES? |
| | | 67. ARE FIRE EXTINGUISHER AND HOSE LOCATIONS PROPERLY MARKED SO THAT THEY CAN BE EASILY LOCATED BY TENANTS DURING A FIRE? |

**DD Form 2637, JAN 93** Page 25 of _____ Pages

WHEN FILLED IN

WHEN FILLED IN

| SECTION IV - ADDITIONAL INFORMATION | | |
|---|---|---|
| Use this section to add pertinent information for your particular installation or activity.<br>Attach additional copies of this continuation page, as necessary. | | |
| **1. TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA, ETC.** | **2. PROJECT OFFICE/OFFICER** | **3. DATE** *(YYMMDD)* |

| NO. | ITEM<br>*(Assign a number to each item.)* | | | |
|---|---|---|---|---|
| | | | | |

DD Form 2637, JAN 93

Page 26 of _____ Pages

WHEN FILLED IN

# AP17. APPENDIX 17
# WATERSIDE PHYSICAL SECURITY MEASURES AND EVALUATION GUIDE

## AP17.1. INTRODUCTION

AP17.1.1. DoD facilities and installations located adjacent to bodies of water such as ports, airfields, R&D facilities, and training areas face all of the terrorist threats as land-locked facilities or installations. In addition, they must be defended against waterside assault.

AP17.1.2. Measures discussed in this appendix are intended to address the following types of terrorist threats and potential consequences below.

**Table AP17.T1. Waterborne Terrorist Threats to DoD Assets.**

| Threat | Target | Potential Consequences of Attack |
|---|---|---|
| Mines | Ships and boats; navigation aids; and wharves and piers. | If mine detonates against a ship or small boat, it can cause massive casualties, high property losses, and severe loss of capability, depending upon the asset attacked. Like terrorist bombs ashore, mines are an ideal terror weapon. Their random use can effectively close down waterborne commerce, and create serious diplomatic and political problems for U.S. friends and allies. |
| Swimmers | Ships, boats, shore facilities and harbor facilities. | Depends on the target selected by the terrorists. |
| Small boat assault with small arms | Personnel ashore or on ship. | Depends on the number of persons hit, extent of injuries, and criticality to DoD of individuals struck down. |
| Explosive laden small boat | Ships at anchor or moored to buoy, pier, or wharf; piers and wharves; structures built near the | Depends on the nature of the asset attacked; consequences could be very serious if, for example, a terrorist "boat |

| Threat | Target | Potential Consequences of Attack |
|---|---|---|
| | land/water interface (e.g. Officer clubs) small boat anchorage's at DoD installations Bridges or tunnels leading to or from DoD facilities accessible from the water. | bomb" were to successfully attack a major combatant vessel, e.g. an aircraft carrier, while making a foreign port call. |
| Small boat assault with rocket propelled ordnance | Same as above. | In general, consequences of rocket propelled ordnance attacks shall be less than those of a "boat bomb"; if however, critical assets are attacked and disabled, destroyed, or killed, then such an attack would be as damaging as explosive laden small boat attack. |
| Terrorist hijacking/ hostage taking | VIPs aboard ship; VIPs ashore; and innocents who happen to be in the wrong place at the wrong time | No substantial difference in the consequences of hijacking/hostage taking at sea, political consequences may be more noticeable as ships are generally assumed to be more difficult to seize than other facilities ashore. |

AP17.1.3. This Appendix also builds on the concept of a physical security system intended to protect a broad range of DoD assets as listed in table AP17.T2.

**Table AP17.T2. DoD Waterside Assets.**

| DoD Waterside Assets | |
|---|---|
| • Pleasure craft | • Passenger and cargo vessels |
| • Pier/port complex | • Military support vessels |
| • Waterfront facility | • Warships |
| • Passenger ships and terminals | • Navigational aids |

| DoD Waterside Assets | |
|---|---|
| • Other structures erected in shallow water (e.g. oil drilling platforms)<br>• Shore facilities connectors such as causeways, tunnels, cables, utility towers, and bridges<br>• Airfields | • VIP's (aboard ship or at a shore facility)<br>• Other shore facilities, unauthorized access to which might be gained from an approach made from the waterside of a DoD installation or facility |

AP17.1.4. Terrorist attacks from the waterside of DoD facilities are not fundamentally different than terrorist attacks from the landside of an installation or facility. The waterborne terrorist attack poses some difficult challenges for the physical security system designed to protect the DoD asset from attack. In the following section the physical security system functions are reviewed, and some of the differences between waterborne and landside terrorist attacks are identified and discussed.

AP17.2. SECURITY SYSTEM FUNCTIONS

AP17.2.1. Security system functions performed in the protection of a landlocked DoD installation or facility must also be performed when the installation has an interface with a body of water or is itself surrounded by water. Threat detection, classification and identification, response, delay, and incident resolution must be performed.

AP17.2.2. The medium of water presents unique challenges and some opportunities for the physical security system. The principal problem in protecting DoD assets from terrorist attacks from the water is detecting, classifying, and responding to the threat. Detection is often difficult because it is difficult to establish security perimeters and keep legitimate users from wandering into the security zone by accident. Classification of an intrusion as hostile is difficult because there are a myriad of legitimate reasons that might account for the presence of craft or persons in a declared security zone such as mechanical failure, disorientation, wind or current drift, or even illness.

AP17.2.3. The medium of water makes stressful demands on physical resources and equipment used to build a physical security system. As shall be discussed in greater detail below, many of the techniques used to erect barriers, detect and classify intrusions, and respond to intrusions at landlocked installations or facilities are not feasible on the waterside of a DoD

installation. On the other hand, some surveillance systems that do not work particularly well at land locked installations may be applied with good success on the waterside of DoD installations, facilities, or assets afloat.

AP17.2.4. Table AP17.T3. below identifies some of the special concerns related to security system functions and each of the threats identified above. In the section that follows, the discussion shall identify waterside physical security system components, the integration of the components into a physical security system, and the operation of the physical security system in response to various threats identified above.

**Table AP17.T3. Physical Security System Functions and Special Challenges Applied To Waterborne Threats.**

| Security System Function | Threat Type | Security System Challenge |
|---|---|---|
| Detection | Mines | Difficult to detect until one detonates or washes ashore. |
| | Swimmer | Very quiet, difficult to detect with acoustic systems, difficult to detect with visual systems at night. |
| | Explosives laden small boat | Difficult to detect. |
| | Standoff attack mounted from small boat | Can be difficult to detect. |
| | Kidnapping/hostage taking | Difficult to detect without good intelligence; passengers are rarely checked as they debark vessels such as cruise ships, ferries, or pleasure craft. |
| Classification and Identification | Mines | Objects in the water can make classification and identification of homemade mines (IEDs) very difficult, especially to untrained observers. |
| | Swimmer | Even if swimmers are detected, it is difficult to classify them as threats if: |

| Security System Function | Threat Type | Security System Challenge |
|---|---|---|
| | | recreational swimming, water skiing, or scuba diving are not prohibited; even if swimming is not generally allowed, swimmers in the water may have other benign reasons for being in the water. |
| | Explosive-laden small boat | There are often many small boats of a wide variety of types in the water; the presence of other small craft can create problems in the detection, identification, and classification of small craft in a restricted area as hostile. |
| | Stand-off attack mounted from small boat | Classifying a small boat moving at a high rate of speed as hostile is difficult to justify in view of the large number of similar actions in any port. |
| | Kidnapping/hostage Taking | It is difficult to classify individuals as threatening or hostile if they disembark from a ferryboat, cruise ship, ocean liner, or pleasure craft in a peaceful manner. |
| Response | Mines | Verify presence of mines: neutralize identified mines; locating additional mines. |
| | Swimmer | Isolating swimmer from background; identifying and classifying threat posed by swimmer to DoD assets in the area; stopping and apprehending swimmer with minimum force. |
| | Explosive-laden small boat | Intercepting at distance from asset, redirecting suspect boat away from asset or stopping it using minimum necessary |

| Security System Function | Threat Type | Security System Challenge |
|---|---|---|
| | | means. |
| | Standoff attack mounted from small boat | Intercepting at distance from asset; redirecting or stopping it at a distance from the asset using minimum necessary means |
| | Kidnapping/hostage taking | Detecting a kidnapping or hostage taking situation is very difficult; isolating incident from press, additional supporters, and logistical support is somewhat easier for incidents afloat than on land; recovery of vessel, platform, and victims can be very difficult |

AP17.3. WATERSIDE PHYSICAL SECURITY SYSTEM COMPONENTS

AP17.3.1. Barriers. Barriers on the waterside of a DoD installation, facility, or asset afloat perform many basic functions performed on land, such as: establish boundary; isolate activity and discourage visitors; and impede passage by boat or swimmer.

AP17.3.1.1. Some of the functions performed by barriers on the landside of a DoD installation cannot be readily performed on the waterside. Barriers on the waterside to obscure activities on land are difficult to erect on the water. They can be installed at the land/water interface or at the mean high-water mark. Similarly, intrusion detection devices cannot be easily installed on most barriers used to establish boundaries of a DoD installation or facility when those boundaries extend several hundred meters to more than 1000 meters into the water. Some intrusion detection devices can be mounted on fixed installations that extend into the water such as wharves or piers or navigation aid platforms.

AP17.3.1.2. The fact that the barriers have to work on the surface and beneath the surface against a wide variety of threats without harming benign intrusions complicates the design and implementation of barriers.

AP17.3.2. Boundaries.

AP17.3.2.1. Several devices can be used to establish boundaries separating the DoD installation, facility, or asset from the surrounding or bordering waters. Among the devices that can be used to establish a boundary are the following:

AP17.3.2.1.1. Buoys or floats.

AP17.3.2.1.2. Nets (where allowed).

AP17.3.2.1.3. Anchored or pile mounted navigation aids and signaling devices.

AP17.3.2.1.4. Log booms, blue barrels, 55-gallon drums, Dunlops.

AP17.3.2.1.5. Barges.

AP17.3.2.1.6. Gig-boats, whaleboats, and other small workboats at anchor.

AP17.3.2.1.7. Roving patrols by security boats.

AP17.3.2.2. Once boundaries are established, they can be used to provide areas of operation for floating security patrols as well as Contact and Escort (C & E) services and Tactical Reaction activities.

AP17.3.2.3. It must be emphasized that rules of navigation allow for inadvertent and innocent penetration of certain types of barriers, as may occur with small craft engine failure, sail boats, and in some waters, "weekend" sailors whose enthusiasm for water sports exceeds their navigational and operational skill. Unlike fences around DoD installations, penetration of floating or fixed perimeter barriers on the waterside of a DoD installation or facility cannot immediately be assumed to be hostile.

AP17.3.3. Isolate Activity and Restrict Access.

AP17.3.3.1. Some of the barriers noted above can be used to restrict waterside access to DoD installations. For example, use of floating nets (where allowed), especially those made of wire mesh and anchored to the floor of the body of water, can be used to deny access to swimmer delivery vehicles, small commercial-type submarines, or divers. Barges can be used to create a physical barrier of considerable penetration resistance to small craft. The barges should be secured bow to stern with the lead and aft barges being secured to the pier or landside mooring point. The primary purpose for deploying a barrier of this type is to absorb a large portion of the blast from an explosive laden vessel that has managed to elude initial defenses.

AP17.3.3.2. Use of patrol boats is probably the most effective means of isolating a DoD activity and discouraging uninvited visits from benign or curious intruders. Effective use of patrol boats require the establishment of a perimeter, surveillance of activity beyond the perimeter to identify potential intrusions, and dispatch of C& E boats to the intruder at some distance away from an inner zone (Reaction Zone) which is the range of weapons thought to be in the hands of terrorists. As a general rule, it is recommended that boats be allowed no closer than 500 meters to a DoD asset being protected from terrorist attack.

AP17.3.4. Impede Passage.

AP17.3.4.1. Several of the barriers described above can be used to slow or impede access to DoD facilities by boats or swimmers. Nets (where allowed) are among the best barriers for this purpose. Well-marked partially submerged objects can also be used; there are legal implications regarding the emplacement of barriers, which constitute a hazard to navigation; such devices should be employed only after exhaustive consultations with appropriate legal authorities.

AP17.3.4.2. Again, patrol activity by C & E boats or Tactical Reaction Boats can be very effective.

AP17.3.5. Surveillance/Intrusion Detection Systems.

AP17.3.5.1. There are a number of surveillance systems that are appropriate for use in connection with waterside security. Table AP17.T4. provides a partial list.

**Table AP17.T4. Waterside Surveillance Sensors.**

| Potential Threat | Surveillance Technique Daytime | Surveillance Technique Nighttime |
|---|---|---|
| Mines | Patrols by boats | EOD teams |
| Swimmers | Patrols by boats. Shore patrols seeking evidence of swimmers having been inserted from nearby shore positions. Acoustic underwater sensors. | Patrols by boat. Shore patrols, observers equipped with night vision devices on shore and lookouts with night vision devices posted aboard ships. Acoustic underwater sensors. |

| Potential Threat | Surveillance Technique Daytime | Surveillance Technique Nighttime |
|---|---|---|
| Small Craft laden with explosives or terrorists armed with standoff weapons | Patrols. Shore-based surveillance. Helicopter surveillance. Acoustic underwater sensors. | Patrols. Central radar monitoring waterside area (warship radar, shipping/harbor control radar, expedient use of mast mounted radar on-shore). Lookouts posted topside on ships with night vision devices; in high threat environments, consider E-2C or helicopters. Acoustic underwater sensors. |

AP17.3.5.2. There is a substantial difference in surveillance of waterside activities during the day and during the night. During hours of darkness, a substantial reduction in surface activity occurs. As a result, nighttime surveillance of waterside activity can rely on active measures such as radar with comparatively good success in locating and partially identifying potential problems.

AP17.3.6. Classification/identification.

AP17.3.6.1. As in the case of landside security systems, once a potential intruder has been detected it must be classified and identified in order to ensure that proper security measures are undertaken. Waterside security measures respond to the detection of threat by trying to gain more information. In some instances, detected intruders can be identified as either swimmers or vessels; such identification is not sufficient information upon which to base a response.

AP17.3.6.2. There may be many benign reasons to account for the presence of a swimmer or vessel in an area that is not usually open for such intrusions. Lost sailors and swimmers, mechanical failure, curiosity seekers, currents, tides, winds, etc. can be as much responsible for a barrier penetration as hostile intent. Being able to classify detected targets quickly in terms of hostility/benign is critically important.

AP17.3.7. Response.

AP17.3.7.1. Establishment of Security Zones.

AP17.3.7.1.1. Waterside security is enforced by establishing at least two zones of activity. The area extended from the mean high water mark to the outer edge of a zone of control is termed the security zone. Within this area, security forces notify vessels, craft, and swimmers that they are entering restricted waters and should alter course to take them away from protected DoD assets. Security forces may stop and search intruders if necessary, although as a general rule, such engagements in the security zone are not a high priority. Security zones usually extend

at least 1000 meters from the nearest DoD asset; in some port areas this large security zone is not possible, and a smaller security zone must be adopted.

AP17.3.7.1.2. Within the security zone, extending from the high water mark to a distance beyond the maximum range of anticipated waterborne threats is a reaction zone. Within this zone, security forces shall stop and challenge intruders, taking all actions necessary to stop a potential threat.

AP17.3.7.1.3. The zone closest to protected assets extended from the asset to the maximum range of anticipated threat weapons (hundreds of yards for small arms and rocket propelled grenades to several thousand yards for man-portable anti-tank weapons) is a "keep-out" zone. Security forces should endeavor to prevent the entry of hostile craft or vessels into this zone; local defenses may be engaged if hostile craft or vessels enter this zone. Techniques described below may be used to disrupt swimmer attacks within this zone.

AP17.3.7.2. Response Forces In General.

AP17.3.7.2.1. Three types of waterborne security forces are employed to maintain perimeter security and enforce security zone restrictions. Depending on the location of the DoD installation, the nature of the waterside facilities and activities, and the jurisdiction under which waterside security is conducted, security forces may be provided by the U.S. Coast Guard, state or local police, host-government forces if overseas, other DoD security forces, or composite forces as appropriate.

AP17.3.7.2.2. A patrol force is deployed to cruise the security zone, provide detection and identification information to a central command post, and to aid other security forces as necessary. The patrol force may be dedicated to patrol, or may perform other security services as directed.

AP17.3.7.2.3. A C&E force is deployed in the outer security zone. This force is responsible for making initial contact with intruders, positioning the C&E boats between intruders and protected assets, and providing navigational assistance and escort services to ensure that intruders leave the restricted waters of the security zone as quickly as possible.

AP17.3.7.2.4. A Tactical Response Boat (TRB) force is deployed close to or within the reaction zone. This force is responsible for engaging intruders and terminating incidents before intruders reach the "keep out" zone if at all possible.

AP17.3.7.2.5. In addition to the three forces outlined above, it is recommended that waterside security force planners include a tactical response command boat that can perform command and control functions during engagements conducted by C & E boats or tactical response boats. The command TRB shadows the TRB and should be the largest vessel assigned to the security operation. In addition to radar, the command TRB should have illumination pyrotechnics aboard in support of perimeter night operations. Its station shall be at the 500-meter mark or less from the protected asset. Although available to address an aggressor if the TRB needs assistance or additional directed fire, its primary responsibilities are to coordinate and direct vessel responses if the command post does not have a clear observation point over the area of operations, to serve as a backup command post, and to engage a second aggressor when observed and hostile intent is confirmed. In the event of limited boat resources, the command TRB may also be used as a relief boat for the other patrolling vessels when refueling or changing out crews.

AP17.3.7.2.6. It is also recommended that a security force equipped with vehicles, communications equipment, and personal protection equipment be deployed to patrol the land-water interface. It is essential that command, control, and communications systems used by waterside security forces be fully integrated with landside security forces. Table AP17.T5. provides a list of equipment that should be provided to all boats performing supporting security forces.

**Table AP17.T5. Patrol Boat Security Equipment.**

| |
|---|
| ➢ Compatible communications between boats and shore elements |
| ➢ Signal and illumination pyrotechnics |
| ➢ Night vision equipment |
| ➢ Standard boarding firearms and associated equipment |
| ➢ Body armor |
| ➢ Loud hailers (installed or portable) |
| ➢ Flood lights (installed or portable) |
| ➢ Blue light and Siren |

AP17.3.7.2.7. Boats and craft employed as tactical response boats may also be equipped with crew-serve weapons i.e., machine guns or other similar armaments as appropriate.

AP17.3.7.2.8. The primary source of small boat communication is of course, the VHF-FM radio. If available, secure communications should be used. If not available, authentication tables must be used to avoid compromise. Also, when working with DoD forces, additional or alternate communication equipment must be shared to provide a compatible means of communication between forces. A single primary tactical frequency should be designated for small boat security operations. This frequency should not be one routinely used by non-operation forces in the area.

AP17.3.7.2.9. No boarding should be conducted by patrolling small boats or any other vessels assigned to the security zone. If a boarding becomes necessary, it should be conducted by the contact/escort vessels, if employed, local or state law enforcement officers, or by designated boarding teams transported to the scene by a standby vessel. In all cases, the boarding should take place outside the security zone at a secure location.

AP17.4. SECURITY SYSTEM COMPONENT INTEGRATION

AP17.4.1. Patrol Techniques.

AP17.4.1.1. Resource Allocation.

AP17.4.1.1.1. Designate Sectors. Divide the water approaches to the asset into sectors utilizing sector boundary lines that converge at the asset. Each sector should be lettered.

AP17.4.1.1.2. Number of Sectors Required. Normally no more than 4 sectors are necessary in the inner perimeter. The number of sectors within the Security Zone need not necessarily coincide exactly with those in the reaction zone. It may vary accordingly with the number of small boats available for patrol.

AP17.4.1.1.3. Patrol Areas. Small boats should patrol the outer boundary of the zone within the sector to which they are assigned.

AP17.4.1.1.4. Patrol Boat Designations. The patrol boats should be referred to using a basic numbering system (i.e., Boat 1, Boat 2, etc.). Randomly changing call signs is not tactically necessary and shall only confuse crews conducting tactical operations. Most security zone enforcement is conducted with one or two small boats patrolling the perimeter. The techniques for patrolling a security zone are as follows:

AP17.4.1.1.4.1. One-Boat Security Zone. In one-boat security zone enforcement, the security boat shall maintain a position near the centerline of the zone at the outer boundary.

This position allows maximum visibility for observing the established security zone and for warning local vessel traffic.

AP17.4.1.1.4.2. Two-Boat Security Zone. In two-boat security zone enforcement, the zone should be divided into two halves with each security boat maintaining a position near the centerline of their assigned half at the outer boundary. If either boat must leave their assigned position, the second security boat should move to the centerline of the whole zone at the outer boundary as in one-boat enforcement. The second boat should return to its original assigned position only after the previously engaged security boat has returned to its original assigned position.

AP17.4.1.1.5. Intercept Procedures. If the security boat leaves its position to intercept an incoming vessel, to escort a vessel transiting the zone, or to inform a vessel without VHF-FM radio communications of security zone restrictions, the coxswain should return to the centerline position as soon as possible to allow for full monitoring of the zone.

AP17.4.1.1.6. Maneuvering. If safe and practical, all turns should be made to the outside of the zone so that the boat crew never has its back toward the outer boundary of the zone and can maintain surveillance of the zone boundaries.

AP17.4.1.1.7. Moving Security Zone. In a moving security zone (protected asset underway), a two-boat minimum is recommended. Additional security vessels may be used if the threat indicates a need.

AP17.4.1.1.7.1. Position. The first boat, preferably the largest assigned, shall maintain a position directly forward of the protected asset. The second boat, preferably the fastest assigned, shall take position directly aft. Additional security vessels, if and when needed, shall support fore and aft security vessels by deploying on the asset's port and starboard beam.

AP17.4.1.1.7.2. Duties. The first boat leads the moving zone through visual presence (flashing blue light/official U.S. Coast Guard markings) and communications with compliant vessels. The second boat is responsible for intercepting any vessels attempting to enter or interfere with the moving security zone. The second boat shall maintain 360° visual and radar lookout at all times.

AP17.4.1.1.8. Security Zone Enforcement at Anchorage. The tactics previously discussed in these paragraphs may be adapted for 360° coverage of assets at anchorage. In heightened threat environments, tactics discussed may also be adapted for 360° coverage.

AP17.4.1.1.9. Defensive Boat Tactics. Defensive measures provide a response mechanism for actively intercepting and neutralizing an identified, incoming hostile threat. This section shall provide guidance on how small boats can be used to protect a designated asset. The asset can be a ship, pier, waterfront facility, or any area or object vital to national security that requires protection from a waterborne threat. These tactics were developed for use primarily in a Low Intensity Conflict (LIC) environment. However, the tactics may be used at any level of FPCON in support of security zone enforcement by modifying the use of force and Rules of Engagement (ROE) to meet the current threat.

AP17.4.1.1.10. Security operations in a hostile environment without declared war require extraordinary measures to separate friend (or neutral) from foe. In a CONUS LIC environment, the DoD Components as well as other U.S. Government agencies and departments participating in security operations must continually maintain a law enforcement posture that recognizes the constitutional rights and privileges of the citizenry to use the waterways of the nation.

AP17.4.1.1.11. Peacetime/wartime security operations against an adversary, once identified, are the easiest part of the equation. The following tactics are designed to assist friendly forces in determining friend from foe.

AP17.4.1.1.12. The first level of response with this tactical doctrine is to notify transiting vessels of the security zone and to determine their intentions. Non-aggressors shall simply be escorted out of the area. The utilization of these tactics in security zone enforcement shall ensure that a system shall be in place to effectively respond to a wide range of threats. Without them, the Department of Defense and other U.S. Government security forces and the protected asset may suffer unnecessary casualties with devastating consequences.

AP17.4.2. Boat Intrusion Response.

AP17.4.2.1. Screen Vessel Contact with Intruder.

AP17.4.2.1.1. Screen Vessel Responsibilities. The vessel patrolling the sector being penetrated, in the outer most zone (i.e., the reaction zone for two-boat operations, the security zone for three boat operations) shall intercept the incoming vessel at the outer boundary of the security zone, directly on a line between it and the asset. The intercepting vessel (known as the screen vessel) is charged with the responsibility of determining if the incoming vessel is hostile or not (this process shall be discussed later). If the incoming vessel is determined to be hostile, the screen vessel shall then "clear" the "field of fire" by turning at a 90 degree angle to the course

of the incoming vessel. This turn shall always be to the outside of the assigned sector, away from the center line, so as not to cross into the field of fire and to deliver supporting fire if necessary (the direction of turn may be changed if on scene conditions and zone configuration so dictate).

AP17.4.2.1.2. Screen Vessel Tactics. These tactics have been developed around the realization that the command decision to designate an intruder as hostile and to use appropriate force to neutralize the threat shall be extremely difficult, and the evaluation time is likely to be limited to 1 to 2 minutes.

AP17.4.2.1.3. Screen Vessel Movements. The approach to the inbound vessel by the screen vessel should initially be "head on" utilizing siren, blue light, radio/loud hailer, and flood/spot light (into the cabin). As the incoming vessel turns to avoid a head on situation the screen vessel should turn in the same direction on a parallel course, staying between the inbound vessel and the protected asset. The screen vessel should "herd" the incoming vessel out of the security zone. Never allow the potential aggressor a clear line of progression to the asset; this is another method of screening out the innocent boater and a further step in the identification of the intruder vessel as having hostile intent. The obvious actions of a fully marked and identified U.S. Coast Guard boat or similar host-nation vessel if overseas with blue light, weapons at the ready, and siren/loud-hailer/radio calls in the blocking of an incoming vessel's track-line is a positive indication of Coast Guard/host nation enforcement or interdiction action. If the aggressor evades the screen and proceeds toward the asset, the screen vessel must immediately communicate with the command center and clear the TRB's field of fire in the manner previously discussed. If so directed by the command center, if there is a clear field of fire, and if a warning (both loud-hailer and radio) has been given, the screen vessel may take the hostile inbound vessel under fire in support of the TRB.

AP17.4.2.2. TRB Response to Intrusion.

AP17.4.2.2.1. Initial Reaction. While the screen vessel is maneuvering, the TRB patrolling the reaction zone shall be stationed directly on a line between the aggressor and the asset at the outer boundary of the reaction zone. This shall provide a stationary weapons platform for directing fire on the hostile vessel should the command center direct. Once the screen vessel is clear, the TRB may take the aggressor under fire, if necessary and approved by the command center. If any degree of doubt exists as to the status of the intruder, he can be kept under observation of the TRB and fired upon if hostile intent is confirmed. Keep in mind, that at

this point the potential aggressor has been well screened and been given ample warning. If the screen vessel must break off, hostile intent by the inbound vessel is likely.

AP17.4.2.2.2. TRB Response Techniques. Once the screen vessel has initiated contact with an inbound vessel, the designated TRB shall assume a station along the reaction zone boundary directly between the screen vessel's/inbound vessel's location and the asset.

AP17.4.2.2.3. TRB Aspect. The aspect that the TRB assumes in relation to the incoming vessel shall vary depending upon the type of small boat used (i.e., head on for small utility boat, broadside for larger utility boat or patrol boat). The important factor is that the small boat's weapons (usually M-60's) must be able to cover the incoming vessel wherever it maneuvers.

AP17.4.2.2.4. TRB Movements. Once in position, the TRB should come dead-in-the-water (DIW) and maneuver only to maintain a position between the incoming vessel and the asset. This is simplified by the fact that larger course changes by the incoming vessel can be compensated for by relatively small movements along the zone boundary. Attempting to bring the aggressor under fire from a moving platform is not recommended. Experience and testing have shown that accurate weapons fire is extremely difficult from a moving small boat.

AP17.4.2.2.5. Command TRB Response. A single boat (if available) shall be retained in close proximity to the protected asset. This boat (Command TRB) shall be held in reserve to engage follow-on aggressors in a sector already engaged with aggressors and to perform other Command TRB functions as may become necessary.

AP17.4.2.3. Night Operations. Night operations vary from daylight operations in the method of locating and identifying potential aggressors. Unless sufficient boats are available to allow patrolling of the entire boundary of the security zone, the movement of the screen vessels must be controlled by a central command radar system (e.g., ship's radar). Due to the limitations of small boat radar, the screen vessels should be directed by an established command center to intercept approaching vessels. Observation posts should be employed along the shoreline at strategic locations to prevent aggressors from making contact along the shoreline. All screen vessels should be equipped with parachute illumination flares for use during hostile activity to illuminate aggressors. Night vision devices should also be used to assist in visually acquiring incoming vessels.

AP17.4.2.4. Swimmer Deterrence and Countermeasures. The threat to vessels, waterfront facilities, port complexes, bridges, and other assets in the maritime environment from

hostile swimmers is a viable one. Swimmers present a method by which aggressors may conduct a wide range of terrorist and/or LIC operations without the use of complex hardware. It is important that while committing resources to surface craft and waterside threats, the underwater threat is not forgotten.

AP17.4.2.4.1. General Swimmer Capabilities. The nominal speed for a swimmer, depending on distance and equipment carried, is 1 knot. Even a minor current shall cause the swimmer to limit his attack direction. Swimmers shall take advantage of currents to reach their targets. This should be taken into consideration when orienting a defense. However, if intelligence indicates that hostilities are sophisticated enough to have swimmer delivery vehicles or swimmer propulsion units, a 360° defense (including under pier areas) should be maintained.

AP17.4.2.4.2. Swimmer Countermeasures. Security patrols in support of swimmer defense should be conducted as follows:

AP17.4.2.4.2.1. Waterside Patrols. The alert port security patrol is an important element in defending against a swimmer attack. Properly equipped, the port security patrol offers the most sophisticated detection, classification, and neutralization capability yet developed. They can operate in daylight or darkness, are capable of kill or capture (depending on the ROE) and can alert others to a swimmer threat. Patrol effectiveness is determined by location, equipment, understanding of the threat, and alertness. Port security personnel should patrol in darkened areas, shielded from artificial lighting and as far forward in the area of threat as possible to eliminate background noise and other detection obstructions. When applicable and available, binoculars, night vision devices, and/or thermal imagers should be utilized to assist in detection. Anything that appears to be moving toward the protected asset should be treated as a possible attack. Drifting debris is often used to camouflage a swimmer or mine and should be immediately investigated.

AP17.4.2.4.2.2. Waterside Patrols. If there is an identified swimmer threat, boats should be assigned to the swimmer defense mission. They should patrol likely launch points for both surface craft and all-terrain vehicles delivering hostile swimmers. The random presence of a vessel with turning screws and an alert crew is a respectable deterrent to unsophisticated divers. If the threat is high and believed to be from accomplished divers, the boats assigned to swimmer defense should drag heavy lines with attached grapple hooks or large fishing hooks. The area or district commander may only authorize the use of draglines for swimmer defense within CONUS.

AP17.4.2.4.2.3. Pier, Hull, and In-Water Structure Inspections.

AP17.4.2.4.2.3.1. Prior to a ship's arrival, if current threat information indicates, the pier area should be inspected by divers for any pre-positioned explosive devices. U.S. Navy Explosive Ordnance Disposal (EOD) Units, if available, should be used for this mission. However, if they are not available, many local, state police and host nation agencies have similar capabilities. Throughout the vessel's port stay in the established security zone, the pier area and the ship's hull should be inspected periodically by both landside personnel and waterside patrols (e.g., Coast Guard in CONUS).

AP17.4.2.4.2.3.2. Other structures that may be at risk of terrorist attack such as navigation aids, bridges, utility cable towers, tunnels, etc. should also be inspected for underwater explosive devices on a periodic basis. Frequency of inspections should be increased based on the current threat information.

AP17.4.2.4.2.3.3. Use of Concussion Grenades. The use of concussion grenades is extremely effective in swimmer defense operations. The "kill range" of a standard concussion grenade is approximately 5 feet. The "stun range" reaches out 25 to 30 feet in diameter from the concussion blast. Although the kill range is not large, the random use of concussion grenades in several locations around the protected asset shall force most swimmers out of the area. Care must be taken to ensure that a recognizable time pattern is not established. To be an effective deterrent, maximum discharge intervals in the random pattern should not exceed 10 minutes.

AP17.4.2.4.2.3.4. Additional Measures. If the protected asset is a ship, or if a ship is moored near the protected asset, turning the ship's screw, maintaining sea suction, and shifting the rudder on a random basis can be an effective deterrence. However, these methods are generally effective only against unsophisticated swimmers. Establishing lighting around the protected asset that does not interfere with the security personnel's vision or give away their positions or movements is effective in locating surface swimmers and "bubble trails" from "open circuit" SCUBA divers. Portable lighting, search/spot lights, and illumination flares should be available for emergency responses. Periodic activation of the ship's sonar can be an effective deterrent through delivery of its high-pitched "ping."

AP17.5. WATERSIDE SECURITY EVALUATION GUIDE (DD FORM 2638).

AP17.5.1. This survey form is a tool to assist field personnel in developing information about individual facilities within their jurisdiction. It is not intended to address every issue or

contingency, and may be modified for local use as necessary. Although the following guide addresses Port Security, the analytical techniques and security issues identified are equally applicable to DoD installations and facilities that are adjacent to water areas including rivers, lakes, bays, or similar bodies of water but have no significant port facilities. As used in this questionnaire, Port refers to waterside security areas.

WHEN FILLED IN

## WATERSIDE SECURITY EVALUATION GUIDE

*(FOR LOCAL USE ONLY - Do not forward to higher authorities unless specifically requested)*

### PART A - GENERAL WATERSIDE SECURITY INFORMATION

1. UNIT/ACTIVITY BEING SURVEYED

2. SECURITY OFFICER

a. NAME *(Last, First, Middle Initial)*

b. OFFICE ADDRESS

c. ORGANIZATION

d. TELEPHONE NUMBER *(Include Area Code)*

e. SURVEY DATE *(YYMMDD)*

| YES | NO | |
|---|---|---|
| | | 3. IS THE SECURITY OFFICER INCLUDED IN ALL INITIAL CONSTRUCTION REVIEW PROCESSES? *(If No, give details. Use additional sheets as necessary.)* |

### PART B - SECURITY PLANNING

| YES | NO | |
|---|---|---|
| | | 4. DOES THE PORT FACILITY HAVE A CURRENT PORT SECURITY PLAN (PSP)? |
| | | IF YES, GIVE THE DATE OF THE PLAN. |
| | | 5. DOES THE PSP INCLUDE: |
| | | a. PREVENTIVE MEASURES TO REDUCE OPPORTUNITIES FOR INTRODUCTION TO BOMBS? |
| | | b. PROCEDURES FOR EVALUATING AND HANDLING BOMB THREATS? |
| | | c. POLICY FOR EVACUATION AND SAFETY OF PERSONNEL? |
| | | d. PROCEDURES TO BE USED TO SEARCH FOR BOMBS? |
| | | e. PROCEDURES IN THE EVENT A BOMB OR SUSPECTED BOMB IS FOUND ON THE PORT? |
| | | f. PROCEDURES FOR OBTAINING ASSISTANCE AND SUPPORT OF LAW ENFORCEMENT AND EXPLOSIVE ORDNANCE DISPOSAL UNITS? |
| | | g. PROCEDURES TO BE TAKEN IN THE EVENT OF A BOMB EXPLOSION OR DETONATION? |
| | | 6. DOES THE PORT HAVE A COUNTER SABOTAGE PROGRAM? |
| | | 7. DOES THE SECURITY OFFICER ENSURE THAT PHYSICAL SECURITY SURVEYS ARE CONDUCTED AT LEAST ANNUALLY? |

8. HOW OFTEN DOES THE PORT REQUEST A THREAT ASSESSMENT?

9. COMMENTS ON SECURITY PLANNING

DD Form 2638, JAN 93 (EG)

WHEN FILLED IN

Page 1 of _____ Pages

Designed using Perform Pro, WHS/DIOR, Aug 98

_____ WHEN FILLED IN

| PART C - SECURITY MEASURES | | |
|---|---|---|
| YES | NO | |
| | | 10. DOES THE PORT FACILITY HAVE A LOSS PREVENTION PLAN? |
| | | 11. WHAT IS THE DATE OF THE PORT FACILITIES MOST RECENT RISK AND THREAT ANALYSIS? |
| | | 12. HAVE AREAS BEEN DESIGNATED IN WRITING BY THE PORT OPERATOR AS RESTRICTED AREAS AS NECESSARY? |
| | | 13. ARE THE BASIC SECURITY MEASURES FOR RESTRICTED AREAS IN EFFECT? |
| | | 14. ARE ALL RESTRICTED AREA POINTS APPROPRIATELY POSTED? |
| | | 15. ARE SECURITY MEASURES IN EFFECT TO PROTECT: |
| | | a. ELECTRICAL POWER SUPPLIES AND TRANSMISSION FACILITIES? |
| | | b. COMMUNICATION CENTERS/EQUIPMENT? |
| | | c. ARMS, AMMUNITION AND DANGEROUS CARGOES? |
| | | 16. ARE PHYSICAL SURVEYS OF THE PORT CONDUCTED AT LEAST ANNUALLY UNDER THE AUSPICES OF THE SECURITY OFFICER? |
| | | 17. WHAT IS THE DATE OF THE MOST RECENT PHYSICAL SECURITY INSPECTION, AUDIT, OR REVIEW BY AN IMMEDIATE SUPERVISOR IN THE PORT? |
| | | 18. DOES THE PORT HAVE AN AFTER-HOURS OR WEEKEND RESTRICTED AREA SECURITY CHECK BY THE SECURITY FORCE? |
| | | ARE THE RESULTS OF SECURITY CHECKS PROMPTLY REPORTED TO THE PORT SECURITY OFFICER? |
| | | 19. DOES THE PORT HAVE A PRIVATELY OWNED VEHICLE (POV) PARKING PLAN? IF YES, DOES IT INCLUDE: |
| | | a. RESTRICTION OF POV PARKING IN EXCLUSIVE AND LIMITED AREAS? |
| | | b. FENCE/ENCLAVE PARKING IN CONTROLLED AREAS? |
| | | 20. DOES THE PORT HAVE A TRAFFIC CONTROL PROGRAM? |
| 21. COMMENTS ON SECURITY MEASURES | | |

| PART D - THE SECURITY FORCE | | |
|---|---|---|
| YES | NO | |
| | | 22. IS THE PRESENT SECURITY FORCE STRENGTH AND COMPOSITION COMMENSURATE WITH THE DEGREE OF SECURITY PROTECTION REQUIRED BY DOD/DOT REGULATION? |
| | | 23. ARE ALL SECURITY POSTS, FIXED AND MOBILE, PROVIDED WITH SECURITY FORCE ORDERS? |
| | | 24. ARE SECURITY FORCE ORDERS REVIEWED BY THE SECURITY OFFICER FOR CURRENCY AT LEAST MONTHLY? |
| | | 25. ARE SECURITY FORCE PERSONNEL INSPECTED BY A SUPERVISOR PRIOR TO BEING POSTED? |
| | | 26. DO SUPERVISORS INSPECT EACH POST/PATROL/ACTIVITY AT LEAST TWICE PER SHIFT? |
| | | 27. DOES PORT OF LOCAL COMMUNITY MAINTAIN AN ORGANIZED AND EQUIPPED CRISIS RESPONSE FORCE? |
| | | 28. DOES THE CRISIS RESPONSE FORCE RECEIVE ADEQUATE TRAINING? |
| | | 29. HOW MANY PERSONNEL ARE AVAILABLE WITHIN THE PORT? |
| | | 30. OUTSIDE THE PORT, HOW MANY ADDITIONAL SECURITY FORCES COULD BE BROUGHT IN WITH: |
| | | a. ONE HOUR NOTICE? |
| | | b. FOUR HOUR NOTICE? |
| | | c. ANY PERTINENT COMMENTS? |
| | | 31. HAS LIAISON BEEN ESTABLISHED WITH LOCAL, STATE, AND FEDERAL LAW ENFORCEMENT AGENCIES WHEREBY EARLY WARNING OF A THREAT SITUATION WILL BE PROVIDED? |
| | | 32. DO SECURITY FORCE PERSONNEL RECORD OR REPORT THEIR PRESENCE AT KEY POINTS IN THE PORT BY MEANS OF: |
| | | a. PORTABLE WATCH CLOCKS? |
| | | b. GENERAL WATCH CLOCK STATIONS? |
| | | c. TELEPHONES? |
| | | d. TWO-WAY RADIO COMMUNICATIONS EQUIPMENT? |
| | | e. OTHER? |
| | | f. ARE GUARD ASSIGNMENTS, TIMES AND PATROL ROUTES VARIED AT FREQUENT INTERVALS TO AVOID ESTABLISHING ROUTINES? |
| | | g. IF YES, WHAT ARE THE INTERVALS? |

DD Form 2638, JAN 93

_____ WHEN FILLED IN

Page 2 of _____ Pages

_____ WHEN FILLED IN

| PART D - THE SECURITY FORCE *(Continued)* | | |
|---|---|---|
| 33. COMMENTS ON THE SECURITY FORCE | | |

| PART E - SECURITY FORCE TRAINING | | |
|---|---|---|
| YES | NO | |
| | | 34. DOES THE PORT FACILITY PROVIDE PRESCRIBED SECURITY FORCE TRAINING? |
| | | 35. DOES THE PORT FACILITY PROVIDE LESSON PLANS TO COVER ALL FACETS OF SECURITY AND LAW ENFORCEMENT? |
| | | 36. IS "OUTSIDE" LAW ENFORCEMENT/SECURITY TRAINING PROVIDED? |
| | | IF YES, LIST NAME(S) OF SCHOOL(S): |
| | | 37. ARE INDIVIDUAL TRAINING RECORDS MAINTAINED FOR SECURITY FORCE PERSONNEL? |
| | | 38. DO ALL SECURITY FORCE PERSONNEL, WHO ARE REQUIRED TO BEAR FIREARMS, RECEIVE TRAINING? |
| | | 39. DO ALL SECURITY PERSONNEL RECEIVE INDOCTRINATION IN THE USE OF FORCE? |
| 40. COMMENTS ON SECURITY FORCE TRAINING | | |

| PART F - SECURITY FORCE COMMUNICATIONS | | |
|---|---|---|
| YES | NO | |
| | | 41. DOES THE ACTIVITY SECURITY FORCE HAVE ITS OWN COMMUNICATIONS SYSTEM WITH DIRECT COMMUNICATIONS BETWEEN SECURITY HEADQUARTERS AND SECURITY ELEMENTS? |
| | | 42. IS THERE AN AUXILIARY POWER SUPPLY FOR THE COMMUNICATIONS SYSTEMS? |
| | | 43. IS THERE SUFFICIENT EQUIPMENT TO MAINTAIN CONTINUOUS COMMUNICATIONS WITH EACH ELEMENT OF THE SECURITY FORCE? |
| | | 44. IS THERE ALTERNATE MEANS OF COMMUNICATION AVAILABLE TO THE SECURITY FORCE? |
| | | IF YES, IS IT COMPARABLE TO THE MAIN SOURCE OF COMMUNICATIONS? |
| | | 45. WHAT IS THE PRIMARY MEANS OF COMMUNICATION FOR THE SECURITY FORCE? |
| | | 46. WHAT IS THE ALTERNATE MEANS OF COMMUNICATION FOR THE SECURITY FORCE? |
| | | 47. RADIO COMMUNICATIONS: |
| | | a. ARE PROPER RADIO PROCEDURES PRACTICED? |
| | | b. IS ALL COMMUNICATIONS EQUIPMENT PROPERLY MAINTAINED? |
| | | c. ARE THERE AT LEAST TWO DEDICATED RADIO FREQUENCIES FOR SECURITY FORCE USE? |
| | | d. ARE PORTABLE RADIOS EQUIPPED WITH MULTIPLE-FREQUENCY CAPABILITY? |
| | | e. ARE PORTABLE RADIOS EQUIPPED WITH AN AUTOMATIC-TILT OR SWITCH-ACTIVATED DURESS FREQUENCY? |
| | | 48. DOES THE SECURITY FORCE USE A DURESS CODE FOR EMERGENCY SITUATIONS? |
| | | 49. IS THE DURESS CODE CHANGED AT LEAST MONTHLY? |
| | | 50. IS THE COMMUNICATIONS CENTER AFFORDED ADEQUATE PHYSICAL SECURITY AGAINST ARMED INTRUSION? |
| | | 51. ARE COMMUNICATION SYSTEMS CAPABLE OF BEING USED TO TRANSMIT INSTRUCTIONS TO ALL KEY POSTS SIMULTANEOUSLY IN A RAPID AND TIMELY MANNER? |
| 52. COMMENTS ON SECURITY FORCE COMMUNICATIONS | | |

DD Form 2638, JAN 93

_____ WHEN FILLED IN

Page 3 of _____ Pages

_____ WHEN FILLED IN

| PART G - SECURITY EQUIPMENT | | |
|---|---|---|
| YES | NO | |
| | | 53. DOES THE SECURITY FORCE HAVE SUFFICIENT VEHICLES TO MAINTAIN PATROLS, RESPOND TO ALARMS AND EMERGENCIES, AND MAINTAIN SUPERVISION? |
| | | a. ARE SECURITY FORCE VEHICLES EQUIPPED WITH: |
| | | (1) SIGNS CONSPICUOUSLY IDENTIFYING THE VEHICLES AS SECURITY POLICE VEHICLES? |
| | | (2) EMERGENCY EXTERIOR OVERHEAD LIGHTS? |
| | | (3) ELECTRONIC SIREN? |
| | | b. DO SECURITY FORCE VEHICLES HAVE RELATIVELY LOW MILEAGE? |
| | | 54. HOW OFTEN DO THE SECURITY OFFICERS AND SUPERVISORY PERSONNEL REVIEW THE FIREARMS AND AMMUNITION REQUIREMENTS TO ENSURE THEIR ADEQUACY? |
| | | 55. DO OBSERVATION TOWERS PROVIDE SECURITY PERSONNEL WITH OBSERVATIONS OF SECURITY AREAS? |
| | | 56. WHAT TYPE OF AMMUNITION IS USED BY ARMED SECURITY FORCE PERSONNEL? |
| | | 57. IS AMMUNITION PROPERLY SECURED FOR AND ISSUED ONLY TO AUTHORIZED PERSONNEL? |
| | | 58. ARE WEAPONS STORED AND SECURED WHEN NOT IN USE? |
| | | 59. ARE DUTIES OTHER THAN THOSE RELATED TO SECURITY PERFORMED BY SECURITY PERSONNEL? |
| | | 60. DOES THE PORT FACILITY PROVIDE DEVICES AND SPECIALIZED EQUIPMENT FOR USE BY THE SECURITY FORCE? |
| | | 61. DOES THE PORT PROVIDE SECURITY FORCE PERSONNEL WITH INDIVIDUAL EQUIPMENT? |
| 62. COMMENTS ON SECURITY EQUIPMENT | | |

DD Form 2638, JAN 93

_____ WHEN FILLED IN

Page 4 of _____ Pages

_____ WHEN FILLED IN

| PART H - PERSONNEL AND VEHICLE MOVEMENT CONTROL | | |
|---|---|---|
| YES | NO | |
| | | 63. IS A PASS OR BADGE IDENTIFICATION SYSTEM IN EFFECT TO IDENTIFY ALL PERSONNEL WITHIN THE CONFINES OF RESTRICTED AREAS? |
| | | 64. ARE PERSONNEL WHO REQUIRE INFREQUENT ACCESS TO A RESTRICTED AREA OR HAVE NOT BEEN ISSUED A PERMANENT PASS OR BADGE FOR SUCH, TREATED AS "VISITORS," AND ISSUED A VISITORS BADGE OR PASS? |
| | | 65. DO GUARDS AT CONTROL POINTS COMPARE BADGES TO BEARERS, BOTH UPON ENTRY AND EXIT? |
| | | a. IF NO, UPON ENTRY ONLY? |
| | | b. IF NO, UPON EXIT ONLY? |
| | | 66. IS THE PERSONNEL IDENTIFICATION AND CONTROL SYSTEM SUPERVISED AT ALL LEVELS? |
| | | 67. ARE BADGES AND SERIAL NUMBERS RECORDED AND CONTROLLED BY RIGID ACCOUNTABILITY PROCEDURES? |
| | | 68. ARE LOST BADGES REPLACED WITH BADGES BEARING DIFFERENT SERIAL NUMBERS? |
| | | 69. HAVE PROCEDURES BEEN ESTABLISHED THAT PROVIDE FOR ISSUANCE OF TEMPORARY BADGES FOR INDIVIDUALS WHO HAVE FORGOTTEN THEIR PERMANENT BADGES? |
| | | 70. ARE BADGES OF SUCH DESIGN AND APPEARANCE AS TO ENABLE GUARDS, AND OTHER PERSONNEL TO RECOGNIZE QUICKLY AND POSITIVELY THE AUTHORIZATIONS AND LIMITATIONS APPLICABLE TO THE BEARER? |
| | | 71. ARE PROCEDURES IN EXISTENCE TO ENSURE THE RETURN OF IDENTIFICATION BADGES UPON TERMINATION OF EMPLOYMENT OR ASSIGNMENT? |
| | | 72. HAVE EFFECTIVE VISITOR ESCORT PROCEDURES BEEN ESTABLISHED WHEN NECESSARY? |
| | | 73. ARE VISITORS ESCORTED WITHIN RESTRICTED AREAS WHEN NECESSARY? |
| | | 74. ARE PERMANENT RECORDS OF VISITS MAINTAINED? |
| | | IF YES, BY WHOM ARE THESE RECORDS KEPT? |
| | | 75. ARE POVS AND CONTRACTOR VEHICLES WHICH ARE ALLOWED ROUTINE ACCESS TO THE INSTALLATION REGISTERED WITH THE SECURITY OFFICE? |
| | | 76. ARE RANDOM ADMINISTRATIVE INSPECTIONS MADE OF AUTOMOBILES? |
| | | 77. ARE ADMINISTRATIVE INSPECTION PROCEDURES ISSUED BY THE PORT AUTHORITY? |
| | | IF YES, ARE THEY CONCISE AND SPECIFIC? |
| 78. COMMENTS ON PERSONNEL AND VEHICLE MOVEMENT CONTROL | | |

DD Form 2638, JAN 93

_____ WHEN FILLED IN

Page 5 of _____ Pages

_____ WHEN FILLED IN

| PART I - BARRIERS AND OPENINGS | | |
|---|---|---|
| YES | NO | |
| | | 79. DOES THE FENCED PORTION OF THE PORT AREA BARRIER MEET THE MINIMUM SPECIFICATIONS FOR SECURITY FENCING? |
| | | a. IS IT OF CHAIN LINK (CYCLONE) COMPOSITION? |
| | | b. IS IT CONSTRUCTED OF 9-GAUGE OR HEAVIER WIRE? |
| | | c. IS THE MESH OPENING NO LARGER THAN TWO INCHES? |
| | | d. IS THE SALVAGE TWISTED AND BARBED AT TOP AND BOTTOM? |
| | | e. IS THE BOTTOM OF THE FENCE WITHIN TWO INCHES OF SOLID GROUND? |
| | | IN AREAS WHERE THE FENCE EXCEEDS TWO INCHES FROM SOLID GROUND, HAVE COMPENSATORY MEASURES BEEN TAKEN? |
| | | f. IS THE TOP GUARD STRUNG WITH BARBED WIRE (OR BARBED TAPE/RAZOR EDGE) AND ANGLED OUTWARD FROM THE PROTECTED SITE AND UPWARD AT A 45-DEGREE ANGLE? |
| | | g. IS THE FENCE AT LEAST EIGHT FEET IN HEIGHT (INCLUDING OUTRIGGER) IN ALL REQUIRED AREAS? |
| | | 80. DOES THE PORT FACILITY PROVIDE FOR SECURITY FORCE INSPECTION OF THE SECURITY BARRIER, INCLUDING CLEAR ZONES, AT LEAST ONCE PER MONTH? |
| | | a. ARE DEFICIENCIES NOTED? |
| | | b. ARE REMEDIAL ACTIONS PROMPTLY EFFECTED? |
| | | 81. IS MASONRY WALL USED AS PART OF THE BARRIER? |
| | | IF YES, DOES IT MEET MINIMUM SPECIFICATIONS FOR SECURITY FENCING? |
| | | 82. DO BUILDING WALLS, FLOORS AND ROOFS FORM A PART OF THE BARRIER? |
| | | IF YES, DO THEY PROVIDE SECURITY EQUIVALENT TO THAT PROVIDED BY THE SECURITY BARRIER? |
| | | 83. ARE ALL OPENINGS PROPERLY SECURED? |
| | | 84. DOES A BUILDING FORM A PART OF THE BARRIER? |
| | | IF YES, DOES IT PRESENT A POTENTIAL PENETRATION HAZARD AT THE POINT OF JUNCTURE WITH THE PERIMETER SECURITY FENCING? |
| | | 85. DOES A BODY OF WATER FORM ANY PART OF THE BARRIER? |
| | | IF YES, ARE ADDITIONAL SECURITY MEASURES PROVIDED? |
| | | 86. ARE OPENINGS SUCH AS CULVERTS, TUNNELS, AND MANHOLES FOR SEWERS AND UTILITY ACCESS, AND SIDEWALK ELEVATORS WHICH PERMIT ACCESS TO THE PORT RESTRICTED AND SECURED? |
| | | 87. ARE ALL PORTALS IN PERIMETER BARRIERS GUARDED AND/OR SECURED? |
| | | 88. DO THE GATES AND/OR OTHER ENTRANCES IN PERIMETER BARRIERS EXCEED THE NUMBER REQUIRED FOR SAFE AND EFFICIENT OPERATIONS? |
| | | 89. ARE ALL PERIMETER BARRIER PORTALS EQUIPPED WITH SECURE LOCKING DEVICES? |
| | | ARE THEY LOCKED WHEN NOT IN USE? |
| | | 90. DO ALL GATES PROVIDE PROTECTION EQUIVALENT TO THAT PROVIDED BY THE BARRIER OF WHICH THEY ARE PART? |
| | | 91. ARE PRESCRIBED CLEAR ZONES MAINTAINED ON BOTH SIDES OF THE RESTRICTED AREA BARRIERS? |
| | | 92. IF CLEAR ZONE REQUIREMENTS CANNOT BE MET, HAVE COMPENSATORY SECURITY MEASURES BEEN IMPLEMENTED? |
| | | 93. ARE ANY PERIMETERS PROTECTED BY INTRUSION DETECTION SYSTEMS (IDS)? |
| 94. COMMENTS ON BARRIERS AND OPENINGS | | |

_____ WHEN FILLED IN

| PART J - PROTECTIVE LIGHTING | | |
|---|---|---|
| YES | NO | |
| | | 95. IS THE PERIMETER AND RESTRICTED AREA PROVIDED PROTECTIVE LIGHTING? IF YES: |
| | | a. DOES THE PROTECTIVE LIGHTING MEET ADEQUATE INTENSITY REQUIREMENTS? |
| | | b. ARE THE ZONES OF ILLUMINATION FROM LAMPS DIRECTED DOWNWARD AND AWAY FROM GUARD PERSONNEL? |
| | | c. IS PERIMETER PROTECTIVE LIGHTING UTILIZED SO THAT SECURITY FORCE PATROL PERSONNEL REMAIN IN COMPARATIVE DARKNESS? |
| | | d. ARE LIGHTS CHECKED AT LEAST WEEKLY FOR PROPER OPERATION PRIOR TO DARKNESS? |
| | | e. ARE REPAIRS TO LIGHTS AND REPLACEMENT OF INOPERATIVE LAMPS EFFECTED IMMEDIATELY OR IN A REASONABLE TIME? |
| | | 96. IS ADDITIONAL LIGHTING PROVIDED AT ACTIVE PORTALS AND POINTS OF POSSIBLE INTRUSION? |
| | | 97. DOES THE PORT FACILITY HAVE A DEPENDABLE SOURCE OF POWER FOR ITS PROTECTIVE LIGHTING SYSTEM? |
| | | 98. DOES THE PORT FACILITY HAVE A DEPENDABLE AUXILIARY (EMERGENCY) SOURCE OF POWER FOR PROTECTIVE LIGHTING? |
| | | IF YES, IS THE POWER SUPPLY FOR THE PROTECTIVE LIGHTING SYSTEM PROTECTED? |
| | | 99. ARE THERE PROVISIONS FOR STANDBY OR EMERGENCY PROTECTIVE LIGHTING? |
| | | IF YES, IS THE STANDBY OR THE EMERGENCY EQUIPMENT TESTED AT LEAST MONTHLY? |
| | | 100. CAN THE EMERGENCY BACKUP POWER SUPPLY BE RAPIDLY SWITCHED INTO OPERATION WHEN NEEDED? |
| | | 101. IS THE EMERGENCY BACKUP POWER SUPPLY SELF-STARTED? |
| | | 102. IS THE PROTECTIVE LIGHTING/EMERGENCY OR STANDBY POWER SOURCE LOCATED WITHIN A RESTRICTED AREA? |
| | | 103. IS PARALLEL CIRCUITRY USED IN THE WIRING? |
| | | 104. ARE MULTIPLE CIRCUITS USED? |
| | | IF YES, ARE PROPER SWITCHING ARRANGEMENTS PROVIDED? |
| | | 105. ARE SWITCHES AND CONTROLS PROPERLY LOCATED, CONTROLLED AND PROTECTED? |
| | | a. ARE THEY WEATHERPROOF AND TEMPER-RESISTANT? |
| | | b. ARE THEY READILY ACCESSIBLE TO SECURITY PERSONNEL? |
| | | c. ARE THEY LOCATED SO THAT THEY ARE INACCESSIBLE FROM OUTSIDE THE PERIMETER BARRIER? |
| | | d. IS THERE A CENTRALLY LOCATED SWITCH TO CONTROL PROTECTIVE LIGHTING? |
| | | 106. IS THE PROTECTIVE LIGHTING SYSTEM DESIGNED AND LOCATIONS RECORDED SO THAT REPAIRS CAN BE MADE RAPIDLY IN AN EMERGENCY? |
| | | 107. ARE MATERIALS AND EQUIPMENT IN SHIPPING AND STORAGE AREAS PROPERLY ARRANGED TO PROVIDE ADEQUATE LIGHTING? |
| | | 108. IF BODIES OF WATER FORM A PART OF THE PERIMETER, IS ADEQUATE LIGHTING PROVIDED WHERE DEEMED APPROPRIATE? |
| 109. COMMENTS ON PROTECTIVE LIGHTING | | |

DD Form 2638, JAN 93

_____ WHEN FILLED IN

Page 7 of _____ Pages

_____ WHEN FILLED IN

| PART K- INTRUSION DETECTION SYSTEM | | |
|---|---|---|
| YES | NO | |
| | | 110. DOES THE PORT FACILITY EMPLOY IDS? |
| | | 111. DOES THE IDS, WHERE UTILIZED, MEET THE FOLLOWING REQUIREMENTS? |
| | | a. ARE IDS SIGNALS MONITORED AT ONE CENTRAL POINT AND IS THE SECURITY FORCE RESPONSE INITIATED FROM THAT POINT? |
| | | b. ARE ALL SENSOR EQUIPMENT, DOORS, DRAWERS, AND REMOVABLE PANELS SECURED WITH KEY LOCKS OR SCREWS AND EQUIPPED WITH TAMPER SWITCHES? |
| | | c. HAVE POWER SUPPLIES BEEN PROTECTED AGAINST OVERLOAD BY FUSES OR CIRCUIT BREAKERS? |
| | | d. ARE ANNUNCIATOR, CONTROL AND DISPLAY SUBSYSTEMS LOCATED IN A SEPARATE AREA/CLOSED OFF FROM PUBLIC VIEW? |
| | | e. ARE ZONE NUMBERS ASSIGNED TO IDS SENSOR LOCATIONS INSTEAD OF BUILDING/ROOM NUMBERS? |
| | | 112. IS THE SYSTEM BACKUP BY SECURITY ALERT TEAMS? |
| | | 113. IS THE ALARM SYSTEM FOR ACTIVE AREAS OR STRUCTURES PLACED IN ACCESS MODE DURING NORMAL WORKING HOURS? |
| | | 114. IS THE SYSTEM TESTED PRIOR TO ACTIVATION? |
| | | 115. IS THE SYSTEM INSPECTED AT LEAST MONTHLY? |
| | | 116. IS THE EXTERIOR IDS SYSTEM WEATHERPROOF? |
| | | 117. IS THERE AN ALTERNATE OR INDEPENDENT POWER SOURCE AVAILABLE FOR USE ON THE SYSTEM IN THE EVENT OF POWER FAILURE? |
| | | 118. IS THE EMERGENCY POWER SOURCE DESIGNED TO CUT IN AND OPERATE AUTOMATICALLY WHEN AC POWER GOES DOWN? |
| | | 119. IS THE IDS SYSTEM MAINTEIND BY TRAINED AND PROPERLY CLEARED PERSONNEL? |
| | | 120. ARE FREQUENT TESTS CONDUCTED TO DETERMINE THE ADEQUACY AND PROMPTNESS OF RESPONSE TO ALARM SYSTEMS? |
| 121. COMMENTS ON INTRUSION DETECTION SYSTEM | | |

| PART L - EMPLOYEE SECURITY EDUCATION PROGRAM | | |
|---|---|---|
| YES | NO | |
| | | 122. DOES THE ACTIVITY HAVE A CURRENT EMPLOYEE SECURITY EDUCATION PROGRAM ADDRESSING PORT SECURITY MATTERS? |
| | | 123. ARE ALL ASSIGNED PERSONNEL PROVIDED PORT SECURITY INDOCTRINATION? |
| | | 124. IS FORMAL SECURITY EDUCATION TRAINING CONDUCTED AT LEAST ANNUALLY FOR ALL PERSONNEL? |
| | | 125. ARE ALL PERSONNEL INDOCTRINATED IN SECURITY PROCEDURES WHICH APPLY IN THE PERFORMANCE OF THEIR DUTIES? |
| | | 126. IF YES, DOES THE PROGRAM COVER SUCH TOPICS AS: |
| | | a. PASS AND BADGE SYSTEMS? |
| | | b. PRIVATELY OWNED VEHICLE IDENTIFICATION AND CONTROL? |
| | | c. RANDOM PACKAGE AND VEHICLE INSPECTIONS? |
| | | d. PROCEDURES FOR PROMPT REPORTING OF SECURITY BREACHES? |
| | | e. LAYOUT OF THE WATERFRONT FACILITY TO WHICH THE SECURITY FORCE IS ASSIGNED? |
| | | f. MEANS/AVENUES BY WHICH THE WATERFRONT FACILITY MAY BE ACCESSED FROM WATERSIDE AND LANDSIDE? |
| | | g. TYPES OF CARGO OPERATIONS, ON THE FACILITY AND ON A VESSEL MOORED TO THE FACILITY, THAT ARE TO BE EXPECTED? |
| | | h. GENERAL SECURITY TOPICS? |
| | | I. ARE LOCAL LAW ENFORCEMENT AGENCIES ASKED TO ACTIVELY PARTICIPATE IN PERTINENT PORTIONS OF THE PROGRAM? |
| 127. COMMENTS ON THE EMPLOYEE SECURITY EDUCATION PROGRAM | | |

DD Form 2638, JAN 93

_____ WHEN FILLED IN

Page 8 of _____ Pages

WHEN FILLED IN

| PART M - ADDITIONAL INFORMATION | | | | |
|---|---|---|---|---|
| *Use this section to add pertinent information for your particular installation or activity. Attach additional copies of this continuation page, as necessary.* | | | | |
| 1. TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA, ETC. | 2. PROJECT OFFICE/OFFICER | 3. DATE *(YYMMDD)* | | |
| NO. | ITEM *(Assign a number to each item.)* | | | |
| | | | | |

DD Form 2638, JAN 93

WHEN FILLED IN

Page 9 of _____ Pages

# AP18. APPENDIX 18
# SPECIFIC CONSTRUCTION PROTECTIVE MEASURES

## AP18.1. SPECIFIC CONSTRUCTION PROTECTIVE MEASURES.

This Appendix discusses general construction protective measures. DoD AT Minimum Construction Standards are available at reference (aw) . Mandatory DoD minimum antiterrorism standards for new and existing inhabited buildings are contained in Appendix B of reference (aw). Additional recommended measures for new and existing inhabited buildings are included in Appendix C of reference (aw). Mandatory DoD minimum antiterrorism standards for expeditionary and temporary structures are contained in Appendix D of reference (aw). Combatant Commanders, Service and/or local commands provide specific guidance for unique/site-specific standards. While there are many ways to organize the variety of possible construction protective measures available to specific installations, one way to do so generally aligns with the seven previously discussed construction design strategies. Specific measures and other construction considerations generally fall within the four groupings of site planning, structural design, architectural design, and electrical and mechanical design. Other construction terms such as landscape design, parking security, interior design, fire protection engineering, and electronic security are generally addressed within these four groupings. Specific measures and other construction considerations are provided below.

## AP18.2. SITE PLANNING

Operational, logistics, and security requirements should be integrated in the overall design of buildings, equipment, landscaping, parking, roads, and other features. If implemented, the following additional measures, as well as related creative solutions developed during this phase, can significantly enhance site security with little increase in cost and should be considered for all inhabited buildings.

### AP18.2.1. Building Location Considerations.

AP18.2.1.1. Standoff and Building Separation Distances. Maximize where practical, meeting the DoD AT minimum standoff distances (reference (ax)) and specific combatant command guidance at locations without specific threat, but mitigate possible blast effects when required standoff distances cannot be met or higher threats exist than the structure is capable of protecting occupants. Other key concepts relating to standoff and building separation distances are controlled perimeter, parking and roadways, family housing, and trash receptacles.

AP18.2.1.2. Vantage Points. Vantage points are natural or man-made positions from which potential aggressors can observe and target people or other assets in and around a building. Identify vantage points outside the control of personnel in the targeted building and either eliminate them or provide means to avoid exposure to them. Means to avoid exposure may include actions such as reorienting the building or shielding people or assets in and around the building using such measures as reflective glazing, walls, privacy fencing, or vegetation.

AP18.2.1.3. Visitor Populations. Activities with large visitor populations provide opportunities for potential aggressors to get near buildings with minimal controls and therefore limit opportunities for early detection. Maximize separation distance between inhabited buildings and areas with large non-DoD visitor populations.

AP18.2.1.4. Commercial Transportation Nodes. Avoid sites for inhabited buildings that are close to railroads, ports, airfields, and major road networks. Where any of these transportation nodes are in the vicinity of existing buildings, provide adequate standoff distances from inhabited buildings required to controlled perimeters. Where those standoff distances are not available and since moving things (such as existing railroads) may be difficult and prohibitively expensive, ensure that there are procedures in place to prohibit trains or other similar transportation vessels from stopping in the vicinity of inhabited structures.

AP18.2.1.5. Unobstructed space. Aggressors will not generally place assets in areas near buildings where their explosive devices could be visually detected by building occupants observing the area around the building. Obstructions within 10 meters (33 feet) of buildings should not be permitted that allow for concealment from observation of explosive devices 150 mm (six inches) or greater in height. This does not preclude the placement of site furnishings or plantings around buildings. It only requires conditions such that any explosive devices placed in that space would be observable by building occupants. Unobstructed space also addresses electrical and mechanical equipment, and equipment enclosures to eliminate opportunities for placement and concealment of explosive devices.

AP18.2.2. Vehicle Considerations.

AP18.2.2.1. Vehicle Access. The first line of defense in limiting opportunities for aggressors to get vehicles close to DoD buildings is at vehicle access points at the controlled perimeter, to parking areas, and at drive-up/drop-off points. Keep the number of access points to the minimum necessary for operational or life safety purposes. That will limit the number of

points at which access may have to be controlled with barriers and/or personnel in increased threat environments or if the threat increases in the future.

AP18.2.2.2. High-Speed Vehicle Approaches. The energy of a moving vehicle increases with the square of its velocity; therefore; minimizing a vehicle's speed allows vehicle barriers to be lighter and less expensive should vehicle barriers ever become necessary. To facilitate reductions in vehicle speeds in the future, ensure there are no unobstructed vehicle approaches perpendicular to perimeters at the required parking and roadway standoff distances.

AP18.2.2.3. Drive-up/drop-Off and Access Roads. Some facilities require access to areas within the required standoff distance for dropping off or picking up people or loading or unloading packages and other objects. Examples that may require drive-up/ drop off include, but are not limited to, medical facilities, exchanges and commissaries, childcare centers, and schools. Here consideration is given to marking, unattended vehicles, access control and location of the drive-up/drop-off and access roads to prevent unauthorized vehicles from being parked and left unattended or located under any inhabited portion of a building. Additionally, locate these points away from large glazed areas of the building to minimize the potential for hazardous flying glass fragments in the event of an explosion. The drive-up/drop-off point should be coordinated with the building geometry to minimize the possibility that explosive blast forces could be increased due to being trapped or otherwise concentrated.

AP18.2.2.4. Parking Beneath Buildings. Parking beneath buildings makes building occupants highly vulnerable and this parking should be eliminated where possible. Where very limited real estate makes parking beneath buildings unavoidable, the following measures should be incorporated into the design for new buildings or mitigating measures should be incorporated into existing buildings to achieve an equivalent level of protection. Ensure that access at personnel and vehicle entrances to parking areas is physically controlled, that the floors beneath inhabited areas will not breach from a detonation in the parking area, and that all structural elements within and adjacent to the parking area will be subject to the progressive collapse provisions.

AP18.2.2.5. Entry Control Points for Family Housing. For new family housing areas, provide space for an entry control point at the perimeter of the housing area so that a controlled perimeter can be established there if the need arises in the future.

AP18.3. STRUCTURAL DESIGN

If adequate standoff distances are achieved, conventional construction provides some protection from a terrorist attack. However, even when standoff distances exist, additional structural measures should be incorporated into building designs in accordance with reference (aw) to ensure that buildings do not sustain damage disproportionate to the original localized damage, collapse, or create hazardous debris.

AP18.3.1. Progressive Collapse Avoidance. Progressive collapse is considered to be significant risk for buildings of three stories (not including basement stories) or more. The superstructure can be designed to sustain local damage with the structural system as a whole remaining stable and not being damaged to an extent disproportionate to the original local damage. An arrangement of the structural elements can provides stability to the entire structural system by transferring loads from any locally damaged region to adjacent regions capable of resisting those loads without collapse. This shall be accomplished by providing sufficient continuity, redundancy, or energy dissipating capacity (ductility), or a combination thereof, in the members and connections of the structure. To verify the design a structure must be analyzed in a number of ways. Additionally, all floors need improved capacity to withstand load reversals (caused by blast effects) by designing them to withstand a net uplift at least equal to the dead load plus one-half the live load. For example, some existing buildings have been outfitted with steel beam systems to reinforce the existing structure to provide an appropriate level of protection.

AP18.3.2. Exterior Walls. A significant number of DoD buildings have un-reinforced masonry exterior walls that would likely crumble with a fairly small explosive without adequate standoff. As a result, with inadequate standoff, un-reinforced masonry walls should be prohibited for the exterior walls of inhabited buildings. Buildings should have adequate reinforcement of at least a minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1200 mm (48 in) or have mitigating measures to provide an equivalent level of protection. There are many available ways to reinforce exterior walls to provide adequate protection for building occupants.

AP18.3.3. Structural Isolation. Where there are areas of buildings that do not meet the criteria for inhabited buildings, design the superstructures of those areas to be structurally independent from the inhabited area. This will minimize the possibility that collapse of the uninhabited areas of the building will affect the stability of the superstructure of the inhabited

portion of the building. Alternatively, verify through analysis that collapse of uninhabited portions of the building will not result in collapse of any portion of the building.

AP18.3.4. Building Overhangs. Avoid building overhangs with inhabited spaces above them where people could gain access to the area underneath the overhang. Where such overhangs must be used, measures should be incorporated into the design for new buildings or mitigating measures should be incorporated into existing buildings to achieve an equivalent level of protection so that roadways and/or parking areas are not under overhangs, that floors beneath inhabited areas will not breach from the detonation underneath the overhang, and that all structural elements within and adjacent to the overhang will not suffer progressive collapse.

AP18.4. ARCHITECTURAL DESIGN

There are many aspects of building layout and other architectural design issues that significantly enhance building occupant' safety and security with little increase in cost and should be fully explored and leveraged for all inhabited buildings.

AP18.4.1. Windows and Glazed Doors. To minimize hazards from flying glass fragments, glazing and window frames are key components for all inhabited buildings. Windows and frames should work as a system to ensure that their hazard mitigation is effective and apply even if adequate standoff distances are met. Specific measures are available to further mitigate glazing and window frames hazards where standoff distances are not met. Additionally, whenever window or door glazing is being replaced in existing inhabited buildings as part of a planned renovation, it should meet the same guidelines.

AP18.4.2. Building Access. The areas outside of installations are commonly not under the direct control of the installations. People entering and exiting the buildings are vulnerable to being fired upon from vantage points (discussed in site planning) outside the installations

AP18.4.2.1. Main Entrance. To mitigate those vulnerabilities in new buildings ensure that the main entrance to the building does not face an installation perimeter or other uncontrolled vantage points with direct lines of sight to the entrance. For existing inhabited buildings where the main entrance faces an installation perimeter either use a different entrance as the main entrance or screen that entrance to limit the ability of potential aggressors to target people entering and leaving the building.

AP18.4.2.2. Exterior Doors. For all new and existing buildings, ensure that all exterior doors into inhabited areas open outwards. By doing so the doors will seat into the doorframes in

response to an explosive blast, increasing the likelihood that the doors will not enter the buildings as hazardous debris.

AP18.4.3. Internal Circulation. Design circulation within buildings to provide visual detection and monitoring of unauthorized personnel approaching controlled areas or occupied spaces.

AP18.4.4. Asset Location. To minimize exposure to visual detection, monitoring, direct blast effects and potential impacts from hazardous glass fragments and other potential debris, consider placement of key personnel, critical assets, to minimize risk.

AP18.4.4.1. Critical assets and mission critical or high-risk personnel. Locate away from the building exterior.

AP18.4.4.2. Visitor control. Controlling visitor access points maximizes the possibility of detecting potential threatening activities. Keep visitor control points in buildings away from sensitive or critical areas, areas where high risk or mission critical personnel are located, or other areas with large population densities of DoD personnel.

AP18.4.4.3. Room layout. In rooms adjacent to the exterior of the building position personnel and critical equipment to minimize exposure to direct blast effects and potential impacts from hazardous glass fragments and other potential debris.

AP18.4.4.4. External hallways. Because doors can become hazardous debris during explosive blast events, because doors designed to resist blast effects are expensive, and because external hallways have large numbers of doors leading into inhabited areas, avoid exterior hallway configurations for inhabited structures.

AP18.4.4.5. Mailrooms. As mail bombs are frequent methods employed by terrorists, protective measures need to address the location of rooms to which mail is delivered or in which mail is handled in inhabited buildings. The measures involve limiting collateral damage and injuries and facilitating future upgrades to enhance protection should they become necessary. By locating the mailroom on the building perimeter there is an opportunity to modify it in the future if a mail bomb threat is identified. Where mailrooms are located in the interior of buildings, few retrofit options are available for mitigating the mail bomb threat. Mailrooms should also be located as far from heavily populated areas of the building and critical infrastructure as possible. This measure will go far toward minimizing injuries and damage if a mail bomb detonates in the mailroom where the mailroom is not specifically designed to resist that threat.

AP18.4.5. Roof access. For all inhabited buildings, control access to roofs to minimize the possibility of aggressors placing explosives or chemical, biological, or radiological agents there or otherwise threatening building occupants or critical infrastructure. For new buildings eliminate all external roof access by providing access from internal stairways or ladders, such as in mechanical rooms. For existing buildings eliminate external access where possible, or secure external ladders or stairways with locked cages or similar mechanisms.

AP18.4.6. Overhead mounted architectural features. For all buildings, ensure that all suspended ceiling systems and other overhead mounted architectural features are mounted to minimize the likelihood that they will fall and injure building occupants. For example, in the DoD AT construction standards, all such systems will be mounted such that they resist forces of 0.5 times the component weight in any direction and 1.5 times the component weight in the downward direction. But this standard does not preclude the need to design architectural feature mountings for forces required by other criteria such as seismic standards.

AP18.4.7. Minimize secondary debris. Eliminate un-revetted concrete barriers and site furnishings in the vicinity of inhabited structures that are accessible to vehicle traffic. Revet exposed concrete surfaces with 1 meter (3 feet) of soil to prevent fragmentation hazards in the event of an explosion.

AP18.5. ELECTRICAL AND MECHANICAL DESIGN

Electrical and mechanical design standards address limiting damage to critical infrastructure, protecting building occupants against chemical, biological, and radiological threats, and notification of building occupants of threats or hazards.

AP18.5.1. HVAC.

AP18.5.1.1. Air intakes. Air intakes to HVAC systems that are designed to move air throughout a building that are at ground level provide an opportunity for aggressors to easily place contaminants that could be drawn into the building. For all new inhabited buildings locate all air intakes at least 3 meters (10-ft) above the ground and is recommended for existing inhabited buildings.

AP18.5.1.2. Emergency air distribution shutoff. All buildings should provide an emergency shutoff switch in the HVAC control system that can immediately shut down air distribution throughout the building. The switch (or switches) should be located to be easily accessible by building occupants. Providing such a capability will allow building occupants to limit the distribution of airborne contaminants that may be introduced into the building.

AP18.5.2. Utility distribution and installation. Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical to safely evacuating personnel from the building or their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. Where possible, route critical or fragile utilities such that they are not on exterior walls or on walls shared with mailrooms to minimize the possibility of the above hazards. Where redundant utilities are required in accordance with other requirements or criteria, ensure that the redundant utilities are not collocated or do not run in the same chases. This minimizes the possibility that both sets of utilities will be adversely affected by a single event.

AP18.5.3. Equipment bracing. Mount all overhead utilities and other fixtures to minimize the likelihood that they will fall and injure building occupants. For example, DoD AT construction standards require all equipment mountings to be designed to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. But they do not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards.

AP18.5.4. Under building access. To limit opportunities for aggressors placing explosives underneath buildings ensure that access to crawl spaces, utility tunnels, and other means of under building access is controlled.

AP18.5.5. Mass notification. All inhabited buildings should have a timely means to notify occupants of threats and instruct them what to do in response to those threats. The capability enables real-time information to be provided to building occupants or personnel in the immediate vicinity of the building during emergency situations. The information relayed should be specific enough to discriminate appropriate response actions. Any system, procedure, or combination thereof that provides this capability will be acceptable.

# AP19. APPENDIX 19
# MAIL HANDLING SUSPICIOUS PACKAGES

## AP19.1. INTRODUCTION

AP19.1.1. This Appendix offers information to assist personnel in identifying suspicious envelopes and packages and actions to take in the event hazardous or explosive content is detected. Although thorough, the list below identifies typical indicators and personnel should remain vigilant for not-so-typical indicators. If a suspicious envelope or parcel is located, personnel should perform the actions listed at the end of this Appendix.

## AP19.2. INDICATORS OF SUSPICIOUS ENVELOPES AND PARCELS

AP19.2.1. The following are typical indicators that highlight suspicious envelopes and parcels.

AP19.2.1.1. Unknown or strange postmark. The mail may be postmarked from a strange or unknown place, usually outside your normal channels of correspondence.

AP19.2.1.2. Lack of return address. This may be an attempt by the terrorist to reduce the amount of evidence on an envelope or to avoid suspicion by using what could be determined to be an erroneous address.

AP19.2.1.3. Excessive amount of postage. It is risky to ask a mail clerk to weigh a letter bomb for the exact amount of postage. Postal personnel normally know what to look for and may be able to determine that the package contains a bomb. Therefore, it is safer for the terrorist to add additional postage rather than risk being caught with the bomb.

AP19.2.1.4. Abnormal or unusual size or shape. The envelope or package may be of an abnormal, excessive, or unusual size because of the construction of the firing device and other bomb parts inside.

AP19.2.1.5. Protruding strings, aluminum foil, or wires. Strings or wires may protrude from or be attached to the item. The bomb maker may have constructed the device in a sloppy manner, causing unsecured wires to work loose. The more likely reason for an exposed wire is that it is an arming wire that the courier did not remove, fearing it would detonate instantaneously.

AP19.2.1.6. Misspelled words. Misspelling on the envelope or package could occur because the writer is simply not familiar with military ranks or unit designations.

AP19.2.1.7. Inconsistency between the return address and the postmark. The return address and the postmark may be different; e.g., the return address may indicate the item was mailed from Oregon, whereas the postmark may indicate Frankfurt, Germany.

AP19.2.1.8. Handwritten labels, foreign handwriting, or poorly typed addresses. Handwriting that appears to be foreign may indicate that the bomber, or whoever addressed the item, is from another country.

AP19.2.1.9. Unusual odor. The item may exhibit an unusual odor, such as shoe polish, almonds, or marzipan (a sweet almond paste used predominately in Germany for candies). Heavily perfumed packages or envelopes may also indicate a device is present. NOTE: Intentionally smelling an envelope or package to determine existence of an unusual odor is not advised. Deliberate smelling of envelopes and packages may expose personnel to chemical or biological agents. The intent of this indicator is that unusual odors may be detected under normal operating conditions and without close scrutiny.

AP19.2.1.10. Unusual weight. The item may be unusually heavy or light for its size. A normal envelope weighs 1 to 2 ounces, compared to a letter bomb, measuring one-fourth to one-half inch thick. It may appear to contain a small report or pamphlet rather than a few sheets of paper. A package may be unusually light if it contains only the firing device, power source, and explosive, rather than whatever is listed on the exterior of the package, such as books or other materials.

AP19.2.1.11. Unbalanced weight. The balance of the item may be uneven because of the way the explosives are placed or because they have shifted to one side.

AP19.2.1.12. Springiness in the top, bottoms, or sides. This may result from the bomb having a pressure-release-type switch. Also, the wires used to construct the device may cause the springiness.

AP19.2.1.13. Inflexibility. The envelope may be inflexible if the firing device and other contents have been mounted on material to prevent shifting around while traveling through the mail system. If the internal components have simply been glued or mounted to the sheet explosive, the envelope may stay in a flexed or semi-flexed position when bent.

AP19.2.1.14. Crease marks, discoloration, or stains. Crease marks or stains, such as those from potato chips or French fries, may show on the outside. This happens because many explosives sweat or exude the oil used in their manufacture, such as motor (Semtex-H) or vegetable (C-4) oil.

AP19.2.1.15. Incorrect titles or title but no name. Often, suspect envelopes or packages are addressed to figureheads, such as "Commander" or "Director" and not "Colonel Jones" or "Mr. Smith."

AP19.2.1.16. Excessive security material, such as masking tape, string, etc. To prevent inadvertent compromise of package contents, excessive security material is used to ensure package integrity during transit.

AP19.2.1.17. Ticking, beeping, or other sounds. Seldom used, analog timers are still a possibility. Digital timers may emit faint beeps or other sounds.

AP19.2.1.18. Marked with restrictive endorsements, such as "Personal," "Rush, Do Not Delay," or "Confidential." Restrictive endorsements ensure suspect envelope or package is opened only by the target individual.

AP19.2.1.19. Evidence of powder or other contaminants. Chemical or biological contaminants can escape through envelope or package seams.

AP19.3. PREVENTATIVE MEASURES

AP19.3.1. To minimize exposure to chemical or biological-laden envelopes and packages, mail handlers should use gloves when handling mail and have several large sealable bags nearby for isolating suspicious mail and discarding all clothing worn when in contact with a suspicious parcel. Surgical masks or protective masks and a change of clothing should also be kept in mailrooms. Powder coated gloves should be avoided as the powder may be associated with a chemical or biological contamination from the mail.

AP19.3.2. Commanders should be aware that individual protective masks are commercially available which provide a significant level of protection against inhalation of certain biological agents. High Efficiency Particulate Air filter masks are relatively inexpensive, available, and effective. Discretionary use is advisable to mitigate risk of exposure.

AP19.3.3. Personnel should be instructed on the location, security procedures, and process for disabling building ventilation systems.

AP19.4. ACTIONS TO TAKE UPON ENCOUNTERING A SUSPICIOUS ENVELOPE OR PACKAGE

AP19.4.1. Personnel, upon encountering a suspicious envelope or package, should follow these suggested actions:

AP19.4.1.1. DO NOT PANIC.

AP19.4.1.2. For a suspicious unopened envelope or package, perhaps marked with a threatening message:

AP19.4.1.2.1. Do not open the envelope or package.

AP19.4.1.2.2. Do not shake or empty the contents of any suspicious envelope or package.

AP19.4.1.2.3. Place the envelope or package in a plastic bag or some other type of container to prevent leakage of contents. If you do not have any container, cover the envelope/package using clothing, paper, a trashcan, etc., and do not disturb this cover.

AP19.4.1.2.4. Evacuate the room, close the door, and secure the area to prevent further access.

AP19.4.1.2.5. If handling envelopes or packages suspected of containing chemical or biological contaminants, wash hands with soap and water to prevent potential of spreading any powder or contaminant.

AP19.4.1.2.6. If at home, dial the local emergency number, such as "9-1-1," and report the incident to local police. If at work, report the incident to local police, chain of command personnel, and the building security manager. If warranted, contact the local FBI field office.

AP19.4.1.2.7. Make a list of all people who were in the room or area when the suspicious envelope or package was recognized. Public health authorities and law enforcement officials may need this information for follow-up advice and investigations.

AP19.4.1.3. For an envelope or package containing powder or other contaminant that spills out onto a surface:

AP19.4.1.3.1. Avoid inhalation of the contaminant. Don respiratory protection if available.

AP19.4.1.3.2. Do not try to clean up the contaminant. Immediately and carefully cover the envelope or package and spilled contents using clothing, paper, a trashcan, etc., and do not disturb this cover.

AP19.4.1.3.3. Evacuate the room, close the door, and secure area to prevent further access.

AP19.4.1.3.4. Wash your hands with soap and water to prevent potential of spreading contaminant.

AP19.4.1.3.5. If at home, dial the local emergency number, such as "9-1-1," and report the incident to local police. If at work, report the incident to local police, chain of command personnel, and the building security manager. If warranted, contact the local FBI field office.

AP19.4.1.3.6. Remove contaminated clothing as soon as possible and place in a plastic bag or other container capable of being sealed. The sealed clothing should be given to emergency responders for proper handling.

AP19.4.1.3.7. Shower with soap and water as soon as possible. Do not use bleach or other disinfectant on skin. The intent is to flush the contaminant from the skin; excess scrubbing or brushing may cause abrasions allowing the contaminant to penetrate the skin.

AP19.4.1.3.8. Make a list of all people who were in the room or area when the suspicious envelope or package was recognized, especially those who had actual contact with the contents. Public health authorities and law enforcement officials may need this information for follow-up advice and investigations.

AP19.4.1.4. If there is a question of room or air handling system contamination by aerosolized agents:

AP19.4.1.4.1. If possible, disable ventilation unit(s) fans in the local area.

AP19.4.1.4.2. Evacuate the area immediately, close the door, and secure area to prevent further access.

AP19.4.1.4.3. If at home, dial the local emergency number, such as "9-1-1," and report the incident to local police. If at work, report the incident to local police, chain of command personnel, and the building security manager. If warranted, contact the local FBI field office.

AP19.4.1.4.4. Shut down air handling system if possible.

AP19.4.1.4.5. Make a list of all people who were in the room or area. Public health authorities and law enforcement officials may need this information for follow-up advice and investigations.