

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!



Department of Defense DIRECTIVE

August 27, 1990
NUMBER O-2000.12

ASD(SO/LIC)

SUBJECT: DoD Combatting Terrorism Program

- References:**
- (a) DoD Directive 2000.12, "Protection of DoD Personnel and Resources Against Terrorist Acts," July 16, 1986 (hereby canceled)
 - (b) U.S. Government Printing Office Number 040-000-00494-7, "Public Report of the Vice President's Task Force on Combatting Terrorism," February 1986
 - (c) Public Law 99-399, "Diplomatic Security and Antiterrorism Act of 1986," August 27, 1986
 - (d) DoD Directive 1300.7, "Training and Education Measures Necessary to Support the Code of Conduct," December 23, 1988
 - (e) through (m), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive:

1. Reissues reference (a) to update DoD policies and responsibilities for implementing the DoD Combatting Terrorism Program, pursuant to reference (b).
2. Assigns responsibilities for the protection of DoD personnel and their families, facilities, and other material resources from terrorist acts.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD); the Military Departments; the Chairman, Joint Chiefs of Staff and Joint Staff; the Unified and Specified Commands; the Office of the Inspector General of the Department of Defense (OIG, DoD); the Defense Agencies; and the DoD Field Activities (hereafter referred to collectively as "DoD Components").
2. This Directive also applies to all DoD personnel and their families, facilities, and other material resources for reducing vulnerability to terrorism; however, Defense attache and security assistance organizations overseas and under the U.S. diplomatic mission shall coordinate their Antiterrorism (AT) programs with the Chief of Mission and comply with Department of State (DoS) standards, in accordance with P.L. 99-399 (reference (c)).
3. Sensitive and compartmented programs of counterterrorism are addressed in relevant National Security Decision Directives (NSDDs), National Security Directives (NSDs), contingency plans, and other relevant classified documents.

#100
FOR OFFICIAL USE ONLY

UNCLASSIFIED WHEN
SEPARATED FROM
ENCLOSURE 5

4. Policy and guidance on the conduct of DoD personnel and their families if seized by terrorists is contained in DoD Directive 1300.7 (reference (d)).

5. Nothing in this Directive shall detract from, nor be construed to conflict with, the authorities and responsibilities of the U.S. Combatant Commanders, or the inherent responsibility of designated military commanders to protect military installations, equipment, and personnel under their command, as in DoD Directive 5200.8 (reference (e)).

C. DEFINITIONS

The terms used in this Directive are defined in enclosure 2.

D. POLICY

It is DoD Policy:

1. To protect DoD personnel and their families, facilities, and other material resources from terrorists acts. Attention shall be given to:

a. Protecting high-risk targets.

b. Elevating the awareness of DoD personnel and their families to the general terrorist threat by advising DoD personnel, through AT Awareness programs, of the terrorist threat in their assigned areas (to include temporary duty (TDY) and/or temporary active duty (TAD) and leave areas); such programs minimally should address the general terrorist threat and personal protection measures that can reduce personal vulnerability, and should be made available to the families of DoD personnel. Awareness programs may be fulfilled by any number of multi-media vehicles, including briefings, films, tapes, sound-on-slide, pamphlets, Armed Forces radio and television networks, etc.

c. Informing DoD personnel and their family members traveling to, or through, DoD-designated high- or potential physical threat countries of the DoD travel security policy (enclosure 3); and to disseminate Federal Aviation Administration (FAA) terrorist threat information as widely as U.S. Government policies permit.

d. Providing appropriate public affairs guidance on DoD Combatting Terrorism efforts in applicable DoD Component directives.

e. Making AT Resident training available to high-risk and other personnel, as identified by appropriate authority (e.g., the Commander in Chief (CINC), the Defense Intelligence Agency (DIA), Service, etc.), who are assessed to be acutely vulnerable to terrorist attack or require specialized instructions in support of their duty assignment (i.e., unit AT program coordinators, AT staff officers, etc.). Resident training is intended to provide more intensive, specialized instruction than that offered in general AT Awareness programs. Resident training requirements, based on the terrorists threat, shall be recommended by appropriate authority to the Services.

2. To facilitate inter-Service coordination and support of U.S. Government antiterrorist activities. The U.S. Government's structure for establishing policy and facilitating efforts to combat terrorism is provided at enclosure 4.

DoD procedures for assessing the terrorist threat, determining terrorist threat levels and conditions, and selecting appropriate antiterrorist security measures are contained in enclosure 5.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SO/LIC)) shall:

a. Monitor, with other DoD Components, the programs to reduce the vulnerability of DoD personnel and their families, facilities, and other material resources to terrorist attack.

b. Provide the OSD representative to the Policy Coordinating Committee on Counter-Terrorism (PCC/CT), and an observer to the Overseas Security Policy Group (OSPG).

c. Provide a chairperson for the DoD AT Coordinating Committee, and membership to subcommittees, as required.

d. Provide policy oversight and guidance to DoD Components in support of respective AT efforts.

e. Develop, publish, and maintain DoD O-2000.12-H (reference (f)), consistent with DoD 5025.1-M (reference (g)), to provide guidance on protective measures that serve to reduce the vulnerability of DoD personnel and their families to terrorist acts.

f. Identify DoD-designated high- and potential physical threat countries, in support of DoD travel security policy, through issuance of the "Travel Security Advisory (TSA)" message, in coordination with the Assistant Secretary of Defense (International Security Affairs) (ASD(ISA)), the Assistant Secretary of Defense (International Security Policy) (ASD(ISP)), and the Principal Deputy Under Secretary of Defense (Strategy and Resources) (PDUSD(S&R)), as appropriate.

g. Conduct the Worldwide AT Conference, as required.

h. Act as point of contact within the Department of Defense for matters relating to the sharing of data and information on AT and the threat posed by domestic and foreign terrorists to the Department of Defense.

i. Coordinate DoD Combatting Terrorism Program issues before the DoD Physical Security Review Board, the DoD Physical Security Equipment Steering Group, and other relevant security boards and committees.

2. The Under Secretary of Defense for Acquisition (USD(A)) shall provide a member to the DoD AT Coordinating Committee (and subcommittees as required), and a representative to the DoD worldwide AT Conference.

3. The Under Secretary of Defense for Policy (USD(P)) shall:

a. Provide counterintelligence, physical security, program, and budget policy support to the DoD Combatting Terrorism and DoD Foreign Counterintelligence Programs.

b. Ensure that the DUSD(Security Policy) provides an observer to the OSPG.

c. Provide appropriate members to the DoD AT Coordinating Committee (and subcommittees as required), and to the DoD Worldwide AT Conference.

d. Establish policy governing incorporation of AT protective features in DoD construction projects.

e. Ensure that the ASD(SO/LIC) is supported in issuing the TSA message.

4. The Assistant Secretary of Defense for Force Management and Personnel (ASD(FM&P)) shall:

a. Establish an AT program for the Department of Defense Dependents Schools System.

b. Provide a member to the DoD AT Coordinating Committee (and subcommittees as required), and a representative to the DoD Worldwide AT conference.

5. The Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) shall review the intelligence and counterintelligence support provided under this Directive for compliance with DoD Directive 5240.1 and DoD 5240.1-R (references (h) and (i)).

6. The Secretaries of the Military Departments shall:

a. Institute Combatting Terrorism programs, and support them with adequate programming, planning, and funding.

b. Institute AT Awareness programs designed to raise the awareness of DoD personnel and their family members to the general terrorist threat, and to measures that can be taken to reduce personal vulnerability.

c. Provide resident training to personnel assigned to high-risk billets and others, as appropriate.

d. Ensure that overseas DoD installations and activities develop, maintain, and implement AT Awareness programs for assigned and official visiting personnel, and their families. Such programs shall be designed to familiarize personnel with DoD AT procedures, guidance, and instructions that:

(1) Are appropriate to the nature and severity of the local terrorist threat, the mission of the DoD installation or activity, and other local conditions; and,

(2) Address respective DoD personnel, residential, vehicular, and office security; i.e., particularly in response to threats of bombings, kidnappings, and assassinations.

e. Ensure that DoD personnel and their families are informed of and understand DoD travel security policy and required actions for travelers enroute to, or through, DoD-designated high- or potential physical threat countries.

f. Establish military construction programming policies to ensure that AT protective features for facilities and installations are included in the planning and design of military and minor construction projects.

g. Ensure existing physical security, base defense, and law enforcement programs address terrorism as a potential threat to DoD personnel and their families, facilities, and material resources.

h. Provide a Military Service representative as a member to the DoD AT Coordinating Committee (and subcommittees as required), and a representative to the DoD Worldwide AT Conference.

i. Provide funding and programming support for physical security equipment issues, as they relate to the Combatting Terrorism program.

j. 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.

7. The Chairman, Joint Chiefs of Staff (CJCS), shall:

a. Ensure that Unified and Specified Command policies and programs are established for protection of DoD personnel and their families, facilities, and other material resources from terrorist acts.

b. Implement the Terrorist Threat Condition (THREATCON) System consistent with this Directive.

c. Provide membership to the PCC/CT, the DoD AT Coordinating Committee meeting and subcommittees, as required, and a representative to the DoD Worldwide AT Conference.

8. The Commanders of the Unified and Specified Commands with territorial responsibilities shall:

a. Establish command policies and programs for the protection of DoD personnel and their families, facilities, and other material resources from terrorist acts.

b. Assess the terrorist threat for the theater according to this Directive, and provide a copy of the threat assessment to the Military Services. On the basis of the threat assessment, identify and recommend to appropriate authority those incumbents of high-risk billets and spouses requiring resident training.

c. Keep subordinate commanders and chiefs of mission informed of the nature and degree of the local threat, and ensure that commanders are prepared to respond to threat changes.

d. Assist subordinate commanders and DoD Agencies, within their geographic regions, in implementing programs developed under this Directive.

e. Ensure that THREATCONs are uniformly implemented and disseminated as specified by this Directive and by guidance in supporting Directives.

f. Serve as the DoD point of contact with U.S. embassies and host-nation officials on matters involving AT policies and measures.

g. Provide a representative to the DoD AT Coordinating Committee and subcommittees, as required, and to the DoD Worldwide AT Conference.

9. The Director, Defense Intelligence Agency (DIA), shall:

a. Provide prompt dissemination of intelligence information on terrorist threats, including specific warning of threats against DoD personnel and their family members, facilities, and other material resources, in accordance with DoD Directive 5240.1, DoD 5240.1-R, and DoD Directive 5240.6 (references (h), (i), and (j)).

b. Provide a member to the DoD AT Coordinating Committee and subcommittees, as required, and a representative to the DoD Worldwide AT Conference.

c. Provide the DoD member to the OSPG.

d. Institute and resource an AT program designed to raise the awareness of overseas DIA personnel and their families to the terrorist threat and measures to reduce personal vulnerability.

e. Ensure that overseas DIA activities develop, maintain, and implement AT programs for assigned and official visiting personnel that are designed to familiarize personnel with AT procedures, guidance, and instructions that:

(1) Are appropriate to the nature and severity of the local terrorist threat, the mission of the activity, and other local conditions.

(2) Address respective DIA personnel and residential, vehicular, and office security, particularly in response to threats of bombings, kidnappings, and assassinations.

f. Ensure that DIA personnel are aware of DoD travel security policy and required actions for traveler enroute to, or through, DoD-designated high-or potential physical threat countries.

g. Provide resident training to personnel assigned to high-risk billets and to others, as recommended by appropriate authority to the Military Services.

10. The Heads of other Defense Agencies shall:

a. Institute an AT Awareness program to orient all DoD personnel on the general terrorist threat and the personal protection measures that could reduce their individual vulnerability to acts of terrorism. The program should also inform DoD travelers who are enroute to, or traveling through, DoD-

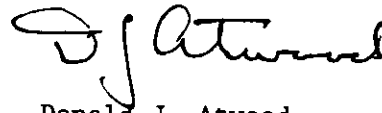
Aug 27, 1990
O-2000.12

designated high- or potential security threat countries of the provisions and requirements of the DoD travel security policy.

b. Provide a member to the DoD AT Coordinating Committee (and subcommittees as required), and a representative to the DoD Worldwide AT Conference.

F. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Assistant Secretary of Defense (Special Operations and Low Intensity Conflict) within 120 days.



Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 5

1. References
2. Definitions
3. U.S. Government Antiterrorism Management Structure
4. DoD Travel Security Policy
5. Terrorist Threat Condition System (THREATCON)

REFERENCES, continued

- (e) DoD Directive 5200.8, "Security of Military Installations and Resources," July 29, 1980
- (f) DoD O-2000.12-H, "Protection of DoD Personnel Against Terrorist Acts," April 1983, authorized by this Directive
- (g) DoD 5025.1-M, "Department of Defense Directives System Procedures," April 1981, authorized by DoD Directive 5025.1, December 23, 1988
- (h) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988
- (i) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, April 25, 1988
- (j) DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program," February 26, 1986
- (k) Title 10, United States Code, Section 1072(2)
- (l) Volume 57, Decision of the Comptroller General of the United States, Pages 519 and 522(1978)
- (m) Joint Federal Travel Regulations, Volume 1; and Joint Travel Regulations, Volume 2 (current editions)

DEFINITIONS

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 forces.
2. AT Awareness. Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorist acts.
3. AT Resident Training. Formal classroom instruction in designated DoD courses that provide specialized instruction on specific combatting terrorism topics; i.e., personal protection, terrorism analysis, regional interest, and AT planning.
4. Combatting Terrorism. Actions, including AT and CT, taken to oppose terrorism throughout the entire threat spectrum.
5. Counterterrorism (CT). Offensive measures taken to prevent, deter, and respond to terrorism.
6. DoD-Designated High-Physical Threat Countries. Geographic areas determined to be of significant terrorist threat to DoD travelers, as designated by the ASD(SO/LIC) in coordination with the ASD(ISA), the ASD(ISP), and the DUSD(S&R).
7. DoD-Designated Potential Physical Threat Countries. Geographic areas determined to be of potential terrorist threat to DoD travelers, as designated by the ASD(SO/LIC) in coordination with the ASD(ISA), the ASD(ISP), and the DUSD(S&R).
8. Domestic Terrorism. Terrorism perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.
9. Family Member. That definition used for "dependent" found in 10 U.S.C. (reference (k)) (spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild (under 21, incapable of self support or under 23 and enrolled in a full-time institution) and others listed in reference (k)).
10. 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.
11. High-Risk Personnel. U.S. personnel and their family members whose grade, assignment, travel itinerary, or symbolic value may make them an especially attractive or accessible terrorist target.
12. High-Risk Target. U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value may be an especially attractive or accessible terrorist target.

13. International (or Transnational) Terrorism. Terrorism in which planning and execution of the terrorist act transcends national boundaries. In defining international terrorism, the purpose of the act, the nationalities of the victims, or the resolution of the incident are considered. Those acts are usually planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists.

14. Military Services. Includes the Army, Navy, Air Force, Marine Corps, and the Coast Guard, under agreement with the Department of Transportation when it is not operating as a Military Service in the Navy.

15. Non-State Supported Terrorism. Terrorist groups that operate autonomously, receiving no significant support from any government.

16. State-Directed Terrorism. Terrorist groups that operate as agents of a government, receiving substantial intelligence, logistical, and operational support from the sponsoring government.

17. State-Supported Terrorism. Terrorist groups that generally operate independently, but receive support from one or more governments.

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

19. Terrorist Threat Condition (THREATCON) System. (See enclosure 5.)

U.S. GOVERNMENT ANTITERRORISM MANAGEMENT STRUCTURE

A. The management of the U.S. Government response to terrorists incidents against U.S. citizens, facilities, and/or interests is in several classified NSDDs and NSDs. A lead Agency is designated for coordinating U.S. Government actions to resolve a terrorists incident. Specifically, those "lead" designations are, as follows:

1. The DoS, for terrorist incidents outside U.S. territory.
2. The Department of Justice (DoJ) for terrorist incidents within U.S. territory. Unless otherwise specified by the Attorney General, the Federal Bureau of Investigation (FBI) shall be the lead Agency within the DoJ for operational response to such incidents.
3. The FAA for aircraft piracy within the special jurisdiction of the United States. The Federal Aviation Administration (FAA) is responsible for the communication of terrorist threat information to commercial air carriers and their passengers.

B. Several groups have been formed for establishing policy and facilitating U.S. Government efforts for combatting terrorism.

1. The Policy Coordinating Committee on Counter-Terrorism (PCC/CT) is the principal organization responsible for developing and overseeing U.S. Government policy on terrorism issues. The PCC/CT, chaired by the DoS, meets frequently for dealing with terrorism issues such as research and development (R&D), legislation, public diplomacy, training programs, and inter-Departmental exercises. The Department of Defense is jointly represented by the Office of the ASD(SO/LIC) (OASD(SO/LIC)) and the Chairman, Joint Chiefs of Staff (CJCS), with attendance by other DoD Agencies on as as-needed basis.

2. The Overseas Security Policy Group (OSPG) is an inter-agency group chaired by the DoS and attended by all U.S. Government Agencies having personnel assigned to diplomatic facilities abroad. The OSPG charter and purpose is to coordinate security policy for such facilities. The Department of Defense is represented by the DIA, with attendance by other DoD Components on as as-needed basis.

3. The Department of Defense has established the DoD AT Coordinating Committee. That committee meets periodically and provides a forum for exchanging ideas and developing policy recommendations on efforts to protect DoD personnel and their family members and DoD resources. That group forms and tasks subcommittees to address specific issues. An Executive Council, chaired by the OASD(SO/LIC), shall convene, as needed. Its membership shall consist of the Services and the CJCS representatives of the DoD AT Coordinating Committee. The Executive Council serves as a steering group for policy and post-incident issues.

- a. The DoD AT Training Subcommittee serves as the principal forum at the action officer (AO) level to identify, implement, and coordinate AT training and education programs. Its additional function is to review AT training courses throughout the Department of Defense for potential consolidation and DoD-wide application. Its membership shall be drawn from

DOD TRAVEL SECURITY POLICY

The Department of Defense's worldwide presence increases its vulnerability to terrorist acts and as a result various commands have developed guidance to enhance the travel security of DoD personnel. To establish consistency within the Department of Defense, the following standard guidance has been developed for use by all DoD Components:

A. When official business requires travel to, or through, DoD-designated high- or potential physical threat countries, DoD personnel and their dependents maximally shall travel by military air or Military Airlift Command (MAC) charter. The Military Services shall identify international airlift requirements to MAC. MAC maximally shall support those requirements with priority of support for travel to high-physical threat countries. Theater commanders shall also identify intratheater airlift requirements to MAC through their Air Force Service Components.

B. Members of the Uniformed Services and DoD civilian employees are authorized to use foreign flag airlines and/or indirect routings to avoid DoD-designated high- or potential physical threat countries. Transportation officers, who arrange travel through an indirect routing or on a foreign flag air carrier to avoid such areas should cite 57 Comp. Gen. 519 and 522 (reference (l)), as the justification for using a foreign flag carrier. The use of that citation must be documented in each case and attached to each travel voucher. That citation is not authority to disregard totally the requirement in the JFTR, volume 1, paragraph U3125C; and the JFTR volume 2, paragraph C2204-2 (reference (m)), to use U.S. air carriers where available. Travelers hereby authorized to avoid specific areas must disembark at the nearest interchange from point of origin and continue the journey on American flag carrier service.

C. Blanket approval and reimbursement for the use of regular-fee passports is not authorized. The passport policy for DoD personnel and their family members traveling on official orders to and or from non-high- or potential physical threat countries remains unchanged. DoD personnel shall travel on no-fee official (red) passports or on official orders with I.D. Cards, as required by the country visited. Command-sponsored family members shall continue to use the no-fee regular (blue) passports with an official endorsement. DoD personnel and their families traveling on official orders to and/or from high- or potential physical threat countries by commercial air are authorized, but not required, to obtain and use the regular-fee passport for security reasons. Travelers electing to exercise that option are responsible for obtaining the regular-fee passport and all required visas. Reimbursement for passports and visas obtained under those conditions is authorized by the JFTR (reference (m)), and payment shall be made on submission of appropriate documentation. Some countries have strict rules as to type of passport or visa required for entry. Information on the restrictions on use of regular-fee passports can be obtained from local personnel offices before travel. Individuals traveling solely by military air or MAC charter shall not be reimbursed for regular-fee passports, unless U.S. Government transportation became available on short notice (i.e., after commercial travel arrangements had been made and passport purchased), or priority of travel was sufficiently high to require backup travel

arrangements. Reimbursement for regular-fee passports for personal travel is not authorized.

D. Commercial airline tickets shall not be annotated to show any affiliation of the traveler to the U.S. Government.

E. Travel itineraries of high-risk personnel (to include flag and/or general officers or civilian equivalents) minimally shall be marked "FOR OFFICIAL USE ONLY," and handled in accordance with command directives, when their travel takes them to, or through, DoD-designated high-physical threat countries or DoD-designated potential physical threat countries, as defined by the DoD travel security policy.

TERRORIST THREAT CONDITION SYSTEM

A. GENERAL. Procedures for terrorism analysts to assess the terrorist threat and for commanders to determine threat conditions and appropriate AT security measures are contained in B. and C. below. The terrorist Threat Condition (THREATCON) system shall be implemented by all DoD Components; it provides a common framework to facilitate inter-Service coordination, support U.S. military AT activities, and enhance overall DoD implementation of U.S. Government antiterrorist policy. A commander, Agency, or organization director determines which THREATCON level is to be designated and which security measures are appropriate. Actions should be based on all appropriate sources of information, to include intelligence, law enforcement information, and command liaison, as tempered by best judgment and knowledge of the local situation.

B. THREAT ASSESSMENTS AND LEVELS FOR USE BY TERRORISM ANALYSTS

1. Threat assessments shall be used to determine threat levels, to implement security decisions, and to establish awareness and resident training requirements. Threat assessments shall be based on the standardized joint-Service criteria promulgated by the CJCS.

2. Threat levels are determined by an assessment of the situation using the following six terrorist threat factors:

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

b. Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

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

d. History. Demonstrated terrorist activity over time.

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

f. Security Environment. The internal policy and security considerations that impact on the capability of terrorist elements to implement their intentions.

3. The following terminology shall be used to describe the various threat levels to ensure uniformity throughout the Department of Defense:

a. Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

b. High. Factors of existence, capability, history, and intentions must be present.

c. Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

d. Low. Existence and capability must be present. History may or may not be present.

e. Negligible. Existence and/or capability may or may not be present.

C. THREATCONS. Terrorist threat conditions, and their associated suggested security measures, are established as follows: The decision to arrive at a particular THREATCON should be based on multiple factors that may include threat, target vulnerability, criticality of assets, security resource availability, operational and morale impact, damage control, recovery procedures, international relations, and planned U.S. Government actions that could trigger a terrorist response.

1. THREATCON NORMAL. Applies when a general threat of possible terrorist activity exists, but warrants only a routine security posture.

2. THREATCON ALPHA. Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONS resulting from intelligence received or as a deterrent. The measures in that THREATCON must be capable of being maintained indefinitely.

a. Measure 1. Remind all personnel at regular intervals, including family members, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; alert for unidentified vehicles on, or in the vicinity of, U.S. installations, units, or facilities; and alert for abandoned parcels or suitcases or any unusual activity.

b. Measure 2. Keep available at all times the duty officer or other appointed personnel who have access to plans for evacuating or sealing off buildings and/or areas in use or where an explosion or attack has occurred. Keep key personnel who may be needed to implement security plans on call.

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

d. Measure 4. Increase security spot checks of vehicles and persons entering installations and nonclassified areas under the jurisdiction of the U.S. command or Agency.

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

f. Measure 6. As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly:

(1) Secure and regularly inspect all buildings, rooms, and storage areas not in use.

(2) At the beginning and end of each workday and at regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages or activity.

(3) Check all deliveries to messes, clubs, etc. (advise family members to check all home deliveries).

(4) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and family members.

g. Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of a higher THREATCON.

h. Measure 8. As appropriate, review and implement security measures for high-risk personnel; e.g., direct use of inconspicuous body armor.

i. Measure 9. As appropriate, consult local authorities on the threat and mutual AT measures.

j. Measure 10. Spare.

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

a. Measure 11. Repeat measure 1 in paragraph C.2.a., above, and warn personnel of any other terrorist form of attack.

b. Measure 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.

c. Measure 13. Check plans for implementation of the measures in the next higher THREATCON.

d. Measure 14. Where possible, cars and objects such as crates, trash containers, etc., are to be moved at least 25 meters from buildings, particularly those buildings of sensitive or prestigious nature. Consider the application of centralized parking.

e. Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

f. Measure 16. At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use of suspicious packages.

g. Measure 17. Examine all mail for letter or parcel bombs.

h. Measure 18. Check all deliveries to messes, clubs, etc.

- i. Measure 19. As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets.
 - j. Measure 20. Make staff and dependents aware of the general situation in order to stop rumors and to prevent unnecessary alarm.
 - k. Measure 21. At an early stage, inform members of local security committees of any action being taken and why.
 - l. Measure 22. On entry of visitors to the unit, physically inspect them and a percentage of their suitcases, parcels, and other containers.
 - m. Measure 23. Wherever possible, operate random patrols to check vehicles, people, and buildings.
 - n. Measure 24. Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a car.
 - o. Measure 25. Implement additional security measures for high-risk personnel, as appropriate.
 - p. Measure 26. Brief personnel, who may augment guard force, on use of deadly force and/or rules of engagement.
 - q. Measure 27. As appropriate, consult local authorities on the threat and mutual AT measures.
 - r. Measure 28 through 29. Spare.
4. THREATCON CHARLIE. Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations is imminent. Implementation of this measure for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.
- a. Measure 30. Continue all THREATCON BRAVO measures or introduce those outstanding.
 - b. Measure 31. Keep available at their places of duty all personnel who are responsible for implementing antiterrorist plans.
 - c. Measure 32. Limit access points to absolute minimum.
 - d. Measure 33. Strictly enforce control of entry and search a percentage of vehicles.
 - e. Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.
 - f. Measure 35. Issue weapons to guards (local orders should include specific orders on issue of ammunition).

- g. Measure 36. Introduce increased patrolling of the installation.
 - h. Measure 37. Protect all designated vulnerable points (VPS) and give special attention to VPS outside military establishments.
 - i. Measure 38. Erect barriers and obstacles to control traffic flow.
 - j. Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attacks.
 - k. Measure 40. Spare.
5. THREATCON DELTA. Implementation applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, that THREATCON is declared as a localized warning.
- a. Measure 41. Continue or introduce all measures listed for THREATCON BRAVO and CHARLIE.
 - b. Measure 42. Augment guards, as necessary.
 - c. Measure 43. Identify all vehicles already on the installation within operations or mission support areas.
 - d. Measure 44. Search all vehicles entering the complex or installation as well as vehicles' contents.
 - e. Measure 45. Control access and implement positive identification of all personnel.
 - f. Measure 46. Search all suitcases, briefcases, packages, etc., brought into the complex or installation.
 - g. Measure 47. Take measures to control access to all areas under the jurisdiction of the U.S. command or Agency concerned.
 - h. Measure 48. Make frequent checks of the exterior of buildings and of parking areas.
 - i. Measure 49. Minimize all administrative journeys and visits.
 - j. Measure 50. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attacks.
 - k. Measure 51. Spare.

those Service activities responsible for combatting terrorism training and education.

b. The DoD Nontactical Vehicle Armoring Subcommittee serves as the principal forum at the AO level to review and coordinate the armoring of nontactical vehicles. Its membership consists of those DoD Components responsible for the armoring or use of such vehicles. That subcommittee shall provide for the exchange of information on the latest armoring techniques and applicable armoring contracts. Information obtained from the inter-Agency Armor and Protective Systems Working Group shall be disseminated to the Department of Defense through that subcommittee.

c. The DoD Intelligence Support Subcommittee serves as the principal forum at the AO level to identify and define terrorism-related intelligence issues within the Department of Defense and the national intelligence community. It recommends to the Secretary of Defense positions to be presented to the national executive agencies relating to national intelligence community issues. Its membership shall be drawn from DoD intelligence, operations, and security organizations, and invited representatives of national law enforcement and intelligence Agencies.

d. The Diplomatic AT and Security Subcommittee serves as the principal forum at the AO level to review those issues unique to DoD Components found under direct cognizance of an ambassador of a U.S. Mission abroad; e.g., attaches and Security Assistance Organizations (SAOs).

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY