

Army Regulation 190-16
OPNAVINST 5530.15A
AFR 207-4
MCO 5500.13A
DLAR 5710.4

Military Police

Physical Security

This printing is a reprint action which adds the Navy's publication number, authentication, and distribution requirements.



0 5 7 9 L D 0 5 6 9 1 1 0

Headquarters
Department of the Army
Washington, DC
31 May 1991

SUMMARY of CHANGE

AR 190-16/OPNAVINST 5530.15A
AFR 207-4/MCO 5500.13A/DLAR 5710.4
Physical Security

This revision--

- o Mandates that major command or second echelon commanders develop local security threat statements (chap 1).
- o Suggests that intrusion detection systems be considered to augment other physical security procedures, devices, and equipment for aircraft security planning (chap 3).
- o Prescribes security force equipment and security procedures for the protection of aircraft (chap 3).
- o Incorporates a nonalert aircraft security requirements matrix (chap 3).
- o Clarifies security procedures for critical communications facilities both on and off military installations (chap 5).
- o Incorporates DOD-approved progressive levels of terrorist threat to U.S. military facilities and personnel (app B).

Departments of the Army, the Navy,
the Air Force, and the Defense
Logistics Agency
Washington, DC
31 May 1991

*Army Regulation 190-16
*OPNAVINST 5530.15A
*Air Force Regulation 207-4
*Marine Corps Order 5500.13A
*DLA Regulation 5710.4
Effective 28 June 1991

Military Police

Physical Security

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:



MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

By Order of the Secretary of the Navy:

F. B. KELSO, II
Admiral, United States Navy
Chief of Naval Operations

Official:

F. J. HERRON
Captain, United States Navy
Assistant Vice Chief of Naval
Operations

W. G. CARSON
Lieutenant General, United States Marine
Corps
Deputy Chief of Staff for Installations
and Logistics

By Order of the Secretary of the Air Force:

MERRILL A. McPEAK
General, United States Air Force
Chief of Staff

Official:

EDWARD P. PARDINI
Colonel, United States Air Force
Director of Information Management

By Order of the Director, Defense Logistics
Agency:

GARY C. TUCKER
Colonel, United States Army
Staff Director, Administration, DLA

History. This UPDATE printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation establishes standard policies on physical security systems planning, threat statements, control of access to installations, security of aircraft, bulk petroleum assets, and critical communications facilities. The Joint Chiefs of Staff-approved terminology, terms, definitions, and prescribed security measures are intended to facilitate inter-Service coordination and support of U.S. military terrorism counteraction activities.

Applicability. This regulation applies to the Active Army, the Air Force, the Navy, the Marine Corps, and the Defense Logistics Agency. It applies to the personnel of the U.S. Army Reserve when located on installations owned, leased, or otherwise under the jurisdiction of the military departments or the Defense Logistics Agency. It also applies to personnel of the Army National Guard, the Air National Guard, the Air Force Reserve, the U.S. Navy Reserve, and the U.S. Marine Corps Reserve when in the service of the United States or located on installations owned, leased, or otherwise under the jurisdiction of the military departments or the Defense Logistics Agency.

Internal control systems. This regulation is subject to the requirements of AR 11-2. It contains internal control provisions but does not contain checklists for conducting internal control reviews. These checklists are contained in DA Circular 11-89-2.

Supplementation. Army supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (DAMO-ODL), WASH DC 20310-0440. Air Force, Navy, Marine Corps, and DLA supplementation of this regulation is permitted, but is not required. If supplements are issued, major or second echelon commands will furnish one copy of each supplement to their headquarters. Air Force, to Air Force Office of Security Police, ATTN: SPOS, Kirtland Air Force Base, NM 87117-6001; Navy, to Chief of Naval Operations (OP-09N), Navy Department, Washington, DC 20388-5400; Marine Corps, furnish one copy to Commandant of the Marine Corps (Code POS-40), Headquarters, U.S. Marine Corps, Washington, DC 20380-0001; and Defense Logistics Agency, furnish one copy to Staff Director, Office of Command Security, Defense Logistics Agency, ATTN: DLA-1.Cameron Station, Alexandria, VA 22304-6100.

Interim changes. Army interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant

to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. The proponent agency of this regulation is the Office of the Deputy Chief of Staff for Operations and Plans. Users are invited to send comments and suggested improvements through appropriate command channels to HQDA (DAMO-ODL) WASH DC 20310-0440.

Distribution. Distribution of this publication is made in accordance with DA Form 12-09-E, block number 3184, intended for command level D for Active Army, Army National Guard, and U.S. Army Reserve.

Navy: SNDL Part 2; Stocked: Naval Aviation Supply Office, Physical Distribution Division, Code 103, 5801 Tabor Avenue, Philadelphia, PA 19120-5099 (500 copies).

Air Force: F

Marine Corps: MARCORPS PCN 10208415400.

Defense Logistics Agency: 3;52A;72;81.

Contents (Listed by paragraph number)

Chapter 1 Introduction

Purpose • 1-1
References • 1-2
Explanation of abbreviations and terms • 1-3
Responsibilities • 1-4
Policy • 1-5

Concept of physical security programs • 1-6
Threat assessments • 1-7
Physical security council • 1-8
Serious security incident reports • 1-9
Terrorist threat conditions
(THREATCONS) • 1-10

Chapter 2 Installation Access Control

Controlled entry and exit • 2-1
Policy • 2-2
Installation access • 2-3
Restricted access plan • 2-4

Chapter 3 Standards for Aircraft Security

Aircraft security • 3-1
Policy • 3-2

*This regulation supersedes AR 190-16, OPNAVINST 5530.15A, AFR 207-4, MCO 5500.13, and DLAR 5710.4. 15 March 1984.

Aircraft security planning • 3-3
Transient or deployed aircraft • 3-4
Security force equipment • 3-5
Security procedures • 3-6
Emergency situations • 3-7

Chapter 4

Security of Bulk Petroleum Assets

Introduction • 4-1
Policy • 4-2
Security planning and liaison • 4-3
Physical security inspections • 4-4

Chapter 5

Security of Critical Communications Facilities

Introduction • 5-1
Policy • 5-2
Service directives • 5-3
Physical security equipment • 5-4
Security force requirements • 5-5
Security measures to improve survivability • 5-6
Off-installation facility staffed full-time • 5-7
Off-installation facility staffed part-time • 5-8

Appendixes

A. Related Publications
B. Terrorist Threat Conditions (THREATCONS)

Glossary

Index

Chapter 1 Introduction

1-1. Purpose

a. This regulation provides realistic guidance and prescribes uniform physical security policies and procedures for installation access control, aircraft, bulk petroleum assets, and critical communication facilities on Department of Defense (DOD) installations and equipment used by the military services and the Defense Logistics Agency (DLA). In overseas areas, commanders or officers in charge may deviate from the policies in this regulation if local conditions, treaties, agreements, and other arrangements with foreign governments and allied forces require.

b. Upon the declaration of war, installation, division, and separate brigade commanders may prescribe procedures that suspend specific provisions of this regulation if local conditions require; however, the procedures must ensure the maximum practical security for Government personnel and property. These commanders may delegate this authority to commanders or activity chiefs in the grade of lieutenant colonel, civilian equivalent, or above.

1-2. References

Related publications are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities

a. *Military services and DLA headquarters.* The following officials will exercise staff supervision over policy programs for physical security of their Services or agencies: for the Army, the Deputy Chief of Staff for Operations and Plans; for the Air Force, The Inspector General; for the Navy, the Special Assistant for Naval Investigative Matters and Security; for the Marine Corps, the Director, Operations Division, Headquarters, U.S. Marine Corps (HQMC); and for the DLA, the Staff Director, Office of Command Security. They will—

- (1) Develop necessary standard policies and procedures.
- (2) Supplement the provisions of this regulation to meet specific Service or DLA needs.
- (3) Coordinate and maintain liaison with the other Services or agencies on physical security matters, including taking part in working groups and committees.
- (4) Set up procedures for sharing threat information in a timely manner through law enforcement, security, or intelligence channels.
- (5) Formalize security procedures for joint response to contingencies.
- (6) Develop or request from their own Service or agency specific physical security threat assessments and update them annually or as needed.

b. *Major command or second echelon command.* Commanders at this level (Army, Air Force, Navy, Marine Corps, and DLA) will—

- (1) Develop a local security threat statement in coordination with local intelligence support elements and forward to subordinate installations and activities.
- (2) Coordinate regional sharing of threat information.
- (3) Supplement Service or DLA threat assessments based on the threat in the commander's area of responsibility and forward the assessments to installations. (Note: For the Air Force only, threat assessments will be supplemented as prescribed by the Air Force Office of Special Investigations (AFOSI) or the Inspector General. For the Navy and Marine Corps, the threat assessment will be provided by the Naval Investigative Service Command (NISCOM), Anti-Terrorist Alert Center (ATAC).)

(4) Encourage establishment of agreements between installations for mutual support against terrorist incidents (that is, sharing intelligence and coordinating terrorist threat conditions (THREATCONS)).

c. *Installation or activity heads.*

- (1) Commanders, directors, supervisors, and officers in charge at this level (Army, Navy, Air Force, Marine Corps, and DLA) will protect personnel and property in their commands against trespass, terrorism, sabotage, theft, arson, and other illegal acts. Commanders

will provide the level of security required based on a thorough assessment of the following considerations:

(a) The types of activity areas or resources and their criticality to the installation's missions.

(b) Current threats to the installation or activity area, including trespassing, terrorism, sabotage, theft, arson, and other illegal acts. (See chaps 3 and 5 for specific security program responsibilities.)

(c) The vulnerability of the installation, including construction and physical layout of the installation or activity area, geographical location, social and political environment, and attractiveness of installation assets to current threats.

(2) Commanders at this level (Army, Air Force, Navy, Marine Corps, and DLA) will—

(a) Develop plans to ensure the protection of DOD resources against trespass, terrorism, sabotage, theft, arson, and other illegal acts during peacetime, mobilization, and war, and share them with other commands located in close proximity.

(b) Develop an installation security threat assessment and share it with other commands and Services within the geographic area.

(c) Establish procedures for providing support to, and requesting support from, other local Service or DLA installations in the event of a terrorist incident.

(d) Exchange current threat information with other Service or DLA installations in the area.

1-5. Policy

a. Physical security is the responsibility of commanders, directors, supervisors, and officers in charge, whether military or civilian.

b. Physical security programs will provide the means to counter threat entities during peacetime, mobilization, and wartime. These include—

- (1) Hostile intelligence services.
- (2) Paramilitary forces.
- (3) Terrorists or saboteurs.
- (4) Criminal elements.
- (5) Protest groups.
- (6) Disaffected persons.

c. Physical security procedures include, but are not limited to—

- (1) Using physical security equipment or measures to reduce vulnerability to a threat.
- (2) Integrating physical security into contingency, mobilization, and wartime plans, and testing physical security procedures and measures during the exercise of these plans.
- (3) Coordinating installation operations security (OPSEC), crime prevention, and physical security programs to protect against the total criminal element.
- (4) Training guards at sensitive or other storage sites in tactical defense against, and response to, attempted penetrations.
- (5) Creating physical security awareness.

d. Physical security measures are physical security equipment, procedures, or devices used to protect security interests from possible threats. They include, but are not limited to—

- (1) Security guards.
- (2) Military working dogs.
- (3) Physical barriers.
- (4) Badging systems.
- (5) Secure containers.
- (6) Locking devices.
- (7) Intrusion detection systems (IDS).
- (8) Security lighting.
- (9) Assessment or surveillance systems (such as closed-circuit television (CCTV)).
- (10) Access control devices.
- (11) Facility hardening.

1-6. Concept of physical security programs

Security of property, equipment, facilities, and personnel is the responsibility of each military and civilian employee of DOD. Investigative and law enforcement agencies may assist in meeting these responsibilities. (These agencies include the U.S. Army and Marine Corps Military Police, the U.S. Air Force Office of Security Police, the AFOSI, the U.S. Army Criminal Investigation Command (USACIDC), the NISCOM, and the DOD, Inspector General.)

1-7. Threat assessments

a. Monitoring. Each Service and DLA must constantly monitor current and potential threats due to their diverse missions, the dispersal of forces, and various states of unit readiness. Threat information is normally passed through intelligence summaries, serious incident reports, law enforcement, and security incidents reports.

b. Analysis. Installations will develop a local threat statement based on local area analysis and information provided by Service intelligence and investigative organizations.

c. Security resources. The threat statement is a key tool for the commander to use to determine the commitment of physical security resources. It is an integral part of the installation physical security or resource protection plan.

1-8. Physical security council

a. The physical security council (PSC) is a means by which an installation commander can gain full community involvement in program design and implementation. Military services and DLA should consider the establishment of such councils at each installation.

b. A PSC should be chaired by a member of the installation command element. The senior law enforcement or security officer is to serve as the coordinator. Membership should include major subordinate activity representatives and key members of the installation staff (such as the comptroller, operations security, intelligence, logistics, and facilities engineer).

c. The PSC can perform any or all of the following functions:

- (1) Provide guidance for the development and distribution of the installation threat assessment.
- (2) Develop the installation physical security plan.
- (3) Evaluate the effectiveness of the installation security program and ensure regulatory compliance.
- (4) Recommend priorities for the commitment of security resources to the commander.
- (5) Evaluate the results of security-related inspections, surveys, and exercises, and recommend corrective actions.
- (6) Review installation entry- and visitor-control procedures.
- (7) Evaluate crime prevention programs and levy specific tasks in support of these programs upon commanders or officers in charge and heads of staff agencies.
- (8) Evaluate reports of significant losses or thefts and corrective actions taken.
- (9) Develop security education requirements.
- (10) Review existing regulations, directives, and plans to ensure that the installation can support a terrorism counteraction program suited to the local situation. (Note: Marine Corps installations will establish a PSC per the guidance herein and as required by OPNAVINST 5530.14 series. As a minimum, Air Force installations should follow established guidance in AFR 207-1 in developing a Base Security Plan.)

1-9. Serious security incident reports

Each Service and DLA will set up a management information system (NORTH-) reporting by subordinate commands of serious security incidents. This system must also require proper follow-up reports that identify the deficiencies that contributed to each incident, and that describe the actions taken to correct those deficiencies. Reports of interest to other Services or DLA will be distributed to them at the Service or DLA headquarters level.

1-10. Terrorist threat conditions (THREATCONS)

a. The THREATCONS in appendix B have been established to describe progressive levels of terrorist threats to U.S. military facilities and personnel. These THREATCONS will be used by the military services and DLA. They should improve coordination and mutual support of the Services and DLA in terrorism counteraction activities.

b. The commander with jurisdiction or control over threatened facilities or personnel is responsible for choosing the proper response to terrorist threats. Declaring a specific THREATCON to exist does not imply any mandatory reports (unless otherwise required), nor does it require that the recommended actions listed in appendix B be taken, except to report rationale to the next higher headquarters.

c. Marine Corps commanders should refer to the current edition of MCO 3302.1 for additional guidance regarding THREATCONS. The Department of the Army requires positive THREATCON reporting from major Army commands (MACOMs). U.S. Air Force commanders should follow AFR 207-1 for guidance regarding THREATCONS. MACOMs will implement a reporting system within their respective commands.

Chapter 2 Installation Access Control

2-1. Controlled entry and exit

This chapter prescribes general policies for controlling entry into and exit from military installations. Access control is an integral part of the installation physical security program. Each installation must clearly define the access control measures (tailored to local conditions) required to safeguard the installation and ensure accomplishment of its mission.

2-2. Policy

Installation commanders will develop, set up, and maintain policies and procedures to control installation access. They will—

- a.* Determine the degree of control required over personnel and equipment entering or leaving the installation.
- b.* Prescribe and distribute procedures for the search of persons (and their possessions) on the installation. These procedures will cover searches conducted as persons enter the installation, while they are on the installation, and as they leave the installation.
- c.* Enforce the removal of, or deny access to, persons who threaten order, security, or discipline of the installation.
- d.* Designate restricted areas to protect classified defense information or safeguard property or material for which they are responsible.

2-3. Installation access

- a.* Installation commanders will determine necessary access controls per paragraph 1-4c.
- b.* Installation commanders will allocate resources necessary to enforce the controls established. The considerations in paragraph 1-5c will be monitored constantly and evaluated to ensure adequate protection is maintained.

2-4. Restricted access plan

a. Each installation commander will develop a plan for increasing vigilance and restricting installation access as events require. This plan will be activated upon the occurrence of the following situations:

- (1) National emergency.
- (2) Disaster.
- (3) Terrorist or hostile threat.
- (4) Significant criminal action.
- (5) Civil disturbance.
- (6) Other contingencies that would seriously affect the ability of the installation to perform its mission.

b. The plan should include actions to counter various stages of each threat.

c. The plan will include—

- (1) Coordination with local, State, and Federal or host country officials to ensure integrity of restricted access to the installation and reduce the effect on surrounding civilian communities.
- (2) Establishment of a system for positive identification of personnel and equipment authorized to enter and exit the installation.
- (3) Maintenance of adequate physical barriers that could be installed to deter access to the installation.
- (4) Predesignation of personnel, equipment, and other resources to enforce restricted access and react to incidents.
- d.* Each commander will review and update the plan as required. All personnel should be informed of the plan and their personal responsibilities under the plan. The plan shall be included as an annex to the host Installation Physical Security Plan.

Chapter 3 Standards for Aircraft Security

3-1. Aircraft security

This chapter describes policy and procedures for security of aircraft in transient or deployed. Aircraft have historically been a frequent target of terrorists, saboteurs, and malcontents. The Services have a joint responsibility to protect aircraft, particularly those in operational roles during a conflict, regardless of location or owning Service. Aircraft security must be an important part of every airfield's installation physical security program.

3-2. Policy

a. Installation commanders are responsible for the security of aircraft assigned to, or transient on, their installations. They will develop security plans to meet this responsibility.

b. Each Service will issue proper directives governing security of its aircraft. The priority for security placed on like aircraft systems within each Service's inventory may vary because of differences in the following:

- (1) Mission of aircraft.
- (2) Location of aircraft.
- (3) Operational readiness of aircraft.

c. The owning Service should request special security support from the host airfield of another Service as far in advance as possible.

3-3. Aircraft security planning

In general planning for aircraft security, a commander should consider the degree to which the installation provides a secure environment. Commanders should consider at least the following factors:

- a. Whether the installation is open or closed to the public.
- b. Whether the flightline or aircraft parking area is adequately fenced, lighted, and posted with signs.
- c. Whether a controlled access policy or limited entry restriction is in effect at the flightline or aircraft parking area.
- d. Whether, and to what degree, the flightline or aircraft parking area has security or law enforcement patrol coverage or surveillance provided by personnel working within or around the area.
- e. IDS should be considered to augment other physical security procedures, devices, and equipment.

3-4. Transient or deployed aircraft

a. The installation commander will always provide a secure area for transient aircraft on the installation.

b. For administrative aircraft, this requirement may be met by parking aircraft in an area where normal troop activity provides a reasonable degree of deterrence.

c. More critical aircraft require additional security measures as listed below. The host installation should make every reasonable effort to provide the same degree of security that the owning Service would provide under the same (transient or deployed) circumstances.

(1) Park the aircraft in a permanent restricted area with an IDS when possible.

(2) If parking the aircraft in an established restricted area with IDS is not possible, put it in a hangar or encircle it with an elevated barrier, such as rope and stanchions. When a hangar is used, the walls constitute the restricted area boundary.

(3) Provide area lighting of sufficient intensity to allow the security force to detect and track intruders.

(4) Display restricted area signs so that personnel approaching the aircraft can see the signs.

(5) Provide circulation control. Entry must be limited to only those persons who have a need to enter.

(6) Require the senior security supervisor to give the aircraft commander a local threat assessment for the duration of ground time.

3-5. Security force equipment

a. Each security force member will be equipped with a helmet, body armor, protective field mask, and a portable mobile radio.

b. Security force members will be armed with an M16 or equivalent weapon and at least half the basic load of ammunition.

3-6. Security procedures

a. Various aircraft assigned to the U.S. Air Force provide tactical support, logistical support, reconnaissance, and refueling capability for worldwide American interests. Many of these aircraft, because of their large size or mission tasking, are an attractive target. This is particularly true at installations where their presence is unusual, they are on display, or are located at civilian or foreign airfields. Refer to the security requirements matrix (table 3-1) to determine the minimum security to be provided for nonalert aircraft. These requirements apply to aircraft on display or located at civilian or foreign air fields. Special or increased requirements for specific operational configuration must be identified in advance (when possible) to host security forces.

b. Security forces in support of aircraft must be notified before a visit to the aircraft is allowed to take place. Any change in security priorities based on operational status must be identified to the host installation.

c. The aircraft commander determines if security is adequate.

3-7. Emergency situations

a. Initial security for aircraft that crash or are forced to land outside a military installation is the responsibility of the nearest military installation. The owning Service will respond and assume on-site security as soon as practical.

b. In the above emergency situations, security must—

- (1) Ensure the safety of civilian sightseers.
- (2) Prevent tampering with or pilfering from the aircraft.
- (3) Preserve the accident scene for later investigation.
- (4) Protect classified cargo or aircraft components.

Table 3-1
Non-alert aircraft security requirements matrix

Aircraft type	Security priority	Entry control responsibility	SRT ¹ team	CBS ²	Motorized patrol
Tactical aircraft (e.g., F-4, F-15, F-16, F-111)	C ³	Aircrew	Yes	—	Yes
Airlift aircraft (e.g., C-5, C-130, C-141, C-23S) ⁴	C	Aircrew	Yes	—	Yes
Strategic bomber aircraft (e.g., B-1, B-52, FB-111)	C	Aircrew	Yes	—	Yes
Air refueling aircraft (e.g., KC-10, KC-135)	C	Aircrew	Yes	—	Yes
Special mission aircraft (e.g., compass call, AWACS, WWABNCP)	B	Security	Yes	Yes	—

Table 3-1
Non-alert aircraft security requirements matrix—continued

Aircraft type	Security priority	Entry control responsibility	SRT ¹ team	CBS ²	Motorized patrol
Strategic reconnaissance ⁵	B	Security	Yes	Yes	—
Advanced technology aircraft (e.g., F-177A, B-2)	B	Pilot carriers detailed information for divert contingencies	—	—	—
Other DOD Aircraft ⁶	C	Aircrew	Yes	—	Yes

Notes:

¹Security Response Team (SRT). A team consisting of two security force members available to respond within 5 minutes. All priority aircraft require SRT support. SRTs may be area patrols not specifically dedicated to the visiting aircraft.

²Close Boundary Sentry (CBS). A security force member posted inside or outside the boundary to keep the boundary of the restricted area under surveillance.

³Priority C aircraft require a motorized patrol in lieu of a CBS.

⁴C-5 aircraft at Clark AB RP will receive security protection commensurate with that provided priority B resources.

⁵U-2C/CT aircraft will be protected as priority C.

⁶Secured IAW this MATRIX or as directed by Service-specific requirements.

Chapter 4 Security of Bulk Petroleum Assets

4-1. Introduction

This chapter prescribes general policies for security of Government-owned, Government-operated (GOGO) and Government-owned, contractor-operated (GOCO) fuel support points, pipeline pumping stations, and piers.

4-2. Policy

a. GOGO and GOCO fuel support points, pipeline pumping stations, and piers will be designated and posted as restricted areas.

b. Access to these facilities will be controlled; only authorized personnel will be permitted to enter. Commanders will determine the means required to enforce access control (such as guards, fences, lighting, and security badges) based on the considerations in paragraph 1-5c.

c. Personnel providing security will be equipped with a primary and an alternate means of communications. These means must enable them to alert military or civilian law enforcement agencies, as appropriate, in the event of an intrusion, fire, or other emergency.

4-3. Security planning and liaison

Commanders of major subordinate commands of the Services and DLA will perform the functions listed below to protect their fuel facilities. They will—

a. Establish liaison with the nearest U.S. military installation.

b. Develop and coordinate contingency plans with the nearest U.S. military installation to provide manpower and equipment resources to the facility in the event of emergencies and increased terrorist or hostile threats.

c. Establish liaison with supporting military, local, State, and Federal law enforcement agencies.

d. Develop all necessary support agreements with the agencies in c. above.

4-4. Physical security inspections

a. The nearest installation of the owning Service will conduct a physical security inspection of each fuel facility at least once every 2 years. Commanders of major commands or major subordinate commanders may require inspections more frequently, at their discretion.

b. Inspections should be formal, recorded assessments of crime prevention measures and other physical security measures, used to protect the facilities from loss, theft, destruction, sabotage, or compromise.

c. Inspection reports will be handled according to applicable directives of the military services or DLA.

Chapter 5 Security of Critical Communications Facilities

5-1. Introduction

a. This chapter establishes policy and concepts for physical security of critical communications facilities located on and off military installations. It includes Defense Communications System (DCS) facilities. Providing adequate security, regardless of the location or owning Service, is a joint-Service responsibility. Specific security support for facilities that require special security measures must be coordinated between the involved Services, as required.

b. Because of the differences in location, physical layout, and equipment, the security considerations in paragraph 1-5c must be thoroughly assessed for each facility; the physical security program of each facility should be tailored to that facility.

c. Sensitive compartmental information facilities (SCIFs) are not covered by this regulation. SCI security management, to include administrative, communications, personnel, and physical security criteria, are covered by other DOD and military service publications.

5-2. Policy

a. Critical communication facilities play a major role in support of each Service's mission, providing operational communications in both peacetime and wartime. These facilities are attractive targets due to limited staffing and isolated locations; therefore, security for these facilities must be an important part of each installation's physical security program.

b. The facility commander's immediate superior or the nearest installation of the owning Service will conduct a physical security inspection of each critical communications facility at least once every 2 years. The owning Service must also review the host installation's physical security measures during inspections and staff visits.

c. Access will be controlled at all critical communication facilities. Only authorized personnel will be allowed to enter. Facilities should be designated as restricted areas.

d. Commanders should consider locating enough weapons and ammunition at critical communications facilities to arm designated on-site personnel. If arms are stored at the facilities, appropriate security measures and procedures will be employed. Weapons will not be located at unmanned facilities.

e. Essential structures should be hardened against attacks; this includes large antenna support legs, operations buildings, and cable trays. Construction programs for critical communications facilities will include appropriate hardening of essential structures.

5-3. Service directives

a. Each Service may issue additional directives governing

security of their critical communications facilities; however, Service directives will not reduce the requirements of this regulation.

b. The owning Services will arrange for security of off-installation facilities with the closest U.S. military installation. This includes contingency plans for manpower and equipment resources during emergencies and normal day-to-day security support, if required. These arrangements can be made between Services by establishing a formal agreement such as an inter-Service support agreement.

c. Each major command will identify critical communications facilities as defined by this directive.

d. Each commander of a major command will ensure that a security plan is developed for each critical communications facility under his or her command. The plan will include emergency security actions and procedures for emergency destruction of sensitive equipment and classified information. This plan may be an annex to an existing host installation security plan. Only the applicable parts of the total plan must be distributed to personnel at the facility.

e. Operations, maintenance, and communications personnel at the facility are the most important factors in security. Each commander of a major command should ensure implementation of a training program for each communications facility. The program will be structured to ensure assigned personnel understand their day-to-day security responsibilities, are familiar with the vulnerabilities of the facility, and are prepared to implement emergency security actions. The training program should cover the following:

(1) Security procedures and personal protection skills for assigned personnel.

(2) The use of weapons for protecting the facility.

(3) Training for appropriate personnel in recognition of jamming, electromagnetic disruption, or interference with the facility's communications, including measures required to maintain communications.

(4) Awareness of local threats and activity in the area.

f. Installation commanders should ensure security of communications facilities for which they provide host support, whether the facilities are on or off the installation.

5-4. Physical security equipment

a. Barriers are normally used to deter or delay unauthorized intruders.

(1) The type of barrier used will depend on the facility's importance to the owning Service's mission and other variables per paragraph 1-4c.

(2) Gates will be constructed and installed to provide protection equal to the barrier. Gates will be locked when not in use.

(3) Barriers, including fencing, used for critical communications facilities, will be at least 6 feet in height, except where greater minimum standards are required by individual Service directives. Fencing will be chain-link style, with 2-inch square mesh of 9-gauge diameter wire according to U.S. Army Corps of Engineers (USACE) drawing 40-16-08 obtainable from the U.S. Army Engineer Division, Huntsville, P.O. Box 1600, Huntsville, AL 35807-4301. (In Europe, fencing may be North Atlantic Treaty Organization (NATO) standard designed fencing. This is chain-link fencing with 76mm grid opening, of 2.5 to 3mm gauge wire, at least 2 meters in height, and with 3.76 meter post separation.)

b. Security lighting is normally used at critical communications facilities. This lighting will be designed to deny an intruder approaching the area the cover of darkness, and enable personnel at the facility to detect unauthorized personnel within the area.

c. IDS may be used with CCTV to observe boundaries and supplemental security procedures.

d. One-way glass, peepholes, electrically operated entry gates, and CCTV should be considered as measures to help on-duty personnel enforce entry control procedures.

5-5. Security force requirements

a. Many communications facilities will require few, if any, full-time security members. Communications personnel at the facility will be trained and equipped to perform security functions per paragraphs 5-2d and 5-3e.

b. An armed entry controller should be provided at all staffed critical facilities located off the installation. If an IDS is in use, the entry controller may also perform alarm monitor functions. An

armed response team drawn from designated on-duty communications personnel should be available at all times to respond to alarms.

c. A response force of military forces or local civilian police will be designated to assist personnel at off-installation critical facilities. Agreements with these forces will be per paragraph 5-3b.

d. Security response support for facilities located on the installation is the responsibility of that installation commander.

5-6. Security measures to improve survivability

The survivability of critical communications facilities can be improved by the use of physical security measures. Use of the following measures should be considered by commanders of MACOMs to protect these facilities, based on the considerations in paragraph 1-4c.

a. Provide a 20-foot clear zone on the inside and outside of the perimeter barrier. All underbrush in the clear zone should be removed and all depressions and raises, leveled.

b. Prohibit personnel from parking vehicles within 30 feet of perimeter.

c. Bury fuel storage tanks and fuel lines for back-up generators underground.

d. Bury power and communications cables underground.

e. Maintain an emergency water supply and store it underground.

f. Elevate air-conditioning systems at least 12 feet above the ground.

g. Paint buildings and essential structures in toned-down colors, such as light green, light brown, and other earth shades.

h. Install hardened defensive fighting positions that cover probable avenues of approach by hostile elements.

5-7. Off-installation facility staffed full-time

When a communication element or site is outside the confines of a support installation and is designated as an operating location where personnel perform duty at all times, the following guidance below will govern.

a. Radio and direct-line telephone communication from the facility to the support installation security or law enforcement control center should be available. If distance or cost prohibit this approach, direct lines connecting the facility with the communications management facility or switchboard located on the support installation should be considered.

b. Entry to critical communications facilities will be controlled.

c. When IDS is installed, alarms should sound at a location that is staffed at all times. Commanders of major commands must ensure each subordinate level of command develops procedures for alarm assessment and security force response.

d. Parking of privately owned vehicles within 30 feet of the perimeter fence will be prohibited.

e. An emergency water supply will be maintained and stored underground.

f. Hardened defensive fighting positions that cover probable avenues of approach will be installed.

g. Radio and direct-line telephone communications to support installation law enforcement or security control centers will be installed.

h. Procedures will be developed for alarm assessment and security response.

i. Security force requirements will be coordinated with local civilian police, host nation military, or security forces for backup and response forces to unmanned sites.

5-8. Off-installation facility staffed part-time

When a communications element or site is outside the confines of a support installation, isolated from the host, and the communications element or site is an operating location where personnel perform duty less than 24 hours a day, the guidance below will govern.

a. The facility will be housed in buildings constructed of solid masonry walls or the equivalent. Compensatory measures will be provided for any existing facility that does not meet this requirement.

b. The installation of IDS is required. The system will, at a minimum, be activated when the facility is unstaffed and will alert

the support installation's security forces, local civil or military police, or the supported installation's management facility.

c. One-way glass, optical viewers, entry control systems, electronically operated gates with two-way voice communications, and CCTV should be considered to help on-duty personnel enforce entry control.

Appendix A Related Publications

For Army users, a related publication is merely a source of additional information. The Army user does not have to read it to understand this regulation.

AFR 125-17

The Air Force Crime Prevention Program

AFR 125-37

The Installation and Resources Protection Program

AFR 207-1

Air Force Physical Security Program

AFR 207-21

Command and Control Communications and Warning Systems

AFR 208-1

US Air Force Antiterrorism Program

AR 190-11

Physical Security of Arms, Ammunition, and Explosives

AR 190-13

The Army Physical Security Program

AR 190-40

Serious Incident Report (Requirements Control Symbol CSGPA-1340 (R1))

AR 190-51

Security of Army Property at Unit and Installation Level

AR 380-5

Department of the Army Information Security Program

DLAM 5710.1

Physical Security Manual

DLAR 5200.8

Protection of Defense Logistics Agency Personnel and Resources Against Terrorist Threats

DLAR 5710.1

Security of DLA Activities and Resources

DOD 5100.76M

Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives

DOD 5200.1R

Information Security Program Regulation

DOD 5200.8

Security of Military Installations and Resources

MCO 1600.6

Crime Prevention Program

MCO 3302.1

Combatting Terrorism at the Installation and Unit Level

MCO 4340.1

Reporting of Missing, Lost, Stolen, and Recovered Government Property

MCO 5640.2

Event/Incident Reports

OPNAVINST 5530.14

Physical Security and Loss Prevention

SECNAV 5511.36

Security of Installations

Appendix B Terrorist Threat Conditions (THREATCONS)

B-1. Overview

The THREATCONS discussed in this appendix describe progressive levels of terrorist threat to U.S. military facilities and personnel. The JCS-approved terminology, definitions, and prescribed security measures are intended to facilitate inter-Service coordination and

support of U.S. military terrorism counteraction activities. Security measures to be implemented under each THREATCON are specified. If a command does not implement all the specific measures under a declared THREATCON, the rationale for those not taken must be reported to the next higher headquarters.

B-2. The four THREATCONS (above normal)

a. THREATCON ALPHA. This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, 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 this THREATCON must be capable of being maintained indefinitely.

b. THREATCON BRAVO. This condition 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, and aggravating relations with local authorities.

c. THREATCON CHARLIE. This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel facilities and is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

d. THREATCON DELTA. This condition 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 likely.

B-3. Declaration of THREATCONS

a. Information and warnings of terrorist activity against installations and personnel of U.S. commands and agencies normally will be received from U.S. security authorities or through the security agencies of the host countries concerned. Information also may come from local police forces, be received directly by a U.S. command or agency as a threat or warning from a terrorist organization, or be in the form of an attack on a U.S. installation or U.S. personnel.

b. The declaration of THREATCONS and implementation of measures may be decreed by a U.S. command or agency or by a local commander or head of an agency following receipt of intelligence through official sources or following an anonymous threat. Lateral as well as vertical reporting is directed by dissemination of THREATCON to potentially affected areas.

c. Specific instructions on issuance of weapons and ammunition will be included in local orders. These orders must comply with the policy of the U.S. command or agency concerned.

d. Detailed measures to be adopted by U.S. headquarters, where they share facilities or jurisdiction with other national or foreign organizations, must be coordinated with these organizations.

B-4. THREATCON measures

a. THREATCON ALPHA.

(1) *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. Be alert for unidentified vehicles on, or in the vicinity of, U.S. installations, units, or facilities. Be alert for abandoned parcels or suitcases or any unusual activity.

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

(3) *Measure 3.* Secure buildings, rooms, and storage areas not in regular use.

(4) *Measure 4.* Conduct security spot checks of vehicles and persons entering installations and nonclassified areas under the jurisdiction of the U.S. commander or agency.

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

(6) *Measure 6.* As appropriate, apply one of the following

measures from THREATCON BRAVO individually and randomly:

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

(b) 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 activity or packages (Measure 5).

(c) Check all deliveries to messes, clubs, and so forth (Measure 17). Advise family members to check all home deliveries.

(d) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and build confidence among staff and family members (Measure 18).

(7) *Measure 7.* Key personnel periodically review and understand all plans, orders, personnel details, and logistical requirements related to the introduction of a higher THREATCON.

(8) *Measure 8.* As appropriate, review and implement security measures for high-risk personnel (for example, direct use of inconspicuous body armor).

(9) *Measure 9.* Spare.

b. THREATCON BRAVO.

(1) *Measure 10.* Repeat Measure 1 and warn personnel of any other terrorist form of attack.

(2) *Measure 11.* Keep on call all personnel involved in implementing anticrime contingency plans.

(3) *Measure 12.* Check plans for implementation of the measures contained in the next higher THREATCON.

(4) *Measure 13.* Where possible, cars and objects such as crates and trash containers are to be moved at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

(5) *Measure 14.* Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

(6) *Measure 15.* At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of regularly used buildings for suspicious packages.

(7) *Measure 16.* Increase examination of all mail for letter or parcel bombs.

(8) *Measure 17.* Check all deliveries to messes, clubs, and so forth. Advise family members to check all home deliveries.

(9) *Measure 18.* As far as resources will allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and build confidence among staff and family members.

(10) *Measure 19.* Make staff and family members aware of the general situation in order to stop rumors and prevent unnecessary alarm.

(11) *Measure 20.* At an early stage, inform members of local security committees of any action being taken and why.

(12) *Measure 21.* Physically inspect visitors and a percentage of their suitcases, parcels, and other containers.

(13) *Measure 22.* Wherever possible, operate random patrols to check vehicles, people, and buildings.

(14) *Measure 23.* Protect off-base military personnel and transport according to prepared plans. Remind drivers to lock parked vehicles and institute a positive system of checking before entering and driving a car.

(15) *Measure 24.* As appropriate, implement additional security measures for high-risk personnel.

(16) *Measure 25.* Brief augmentation guard force personnel on the use of deadly force.

(17) *Measures 26-29.* Spares.

c. THREATCON CHARLIE.

(1) *Measure 30.* Continue all THREATCON BRAVO measures or introduce those not already implemented.

(2) *Measure 31.* Keep all personnel responsible for implementing terrorism counteraction plans available at their places of duty.

(3) *Measure 32.* Limit access points to an absolute minimum.

(4) *Measure 33.* Strictly enforce entry control and search a percentage of vehicles.

(5) *Measure 34.* Enforce centralized parking of vehicles away from sensitive buildings.

(6) *Measure 35.* Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

(7) *Measure 36.* Introduce increased patrolling of the installation.

(8) *Measure 37.* Protect all designated vulnerable points, giving special attention to those outside military establishments.

(9) *Measure 38.* Erect barriers and obstacles to control traffic flow.

(10) *Measure 39.* Spare.

d. THREATCON DELTA.

(1) *Measure 40.* Contains or introduces all measures for THREATCON CHARLIE.

(2) *Measure 41.* Augment guards as necessary.

(3) *Measure 42.* Identify all vehicles already on the installation within operational or mission support areas.

(4) *Measure 43.* Search all vehicles (and their contents) entering the complex or installation.

(5) *Measure 44.* Control all access, and implement positive identification of all personnel.

(6) *Measure 45.* Search all suitcases, briefcases, packages, and so forth, brought into the complex or installation.

(7) *Measure 46.* Take measures to control access to all areas under the jurisdiction of the U.S. command or agency concerned.

(8) *Measure 47.* Make frequent checks of the exterior of buildings and parking areas.

(9) *Measure 48.* Minimize all administrative journeys and visits.

(10) *Measure 49.* Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attack.

(11) *Measure 50.* Spare.

B-5. THREATCON assessment factors

a. Existence. Applies when a terrorist group is present, assessed to be present, or able to gain access to a given country or locale. Group need not have posed a threat to U.S. or DOD interests in the past.

b. Capability. Applies when a terrorist group has acquired, assessed, or demonstrated level of capability to conduct terrorist attacks. This includes resources such as intelligence, mobility, personnel, and equipment (that is, explosives, arms, and ammunition).

c. Intentions. Demonstrated action, or stated intent, to conduct anti-U.S. terrorist activity.

d. History. Demonstrated pattern of terrorist activity over time.

e. Targeting. Applies if there are known plans or confirmed intentions of a terrorist group to target U.S. or DOD interests. Targeting can be either specific or nonspecific. If targeting is not against U.S. or DOD interests, this factor should not be considered.

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

g. Determining levels. Combination of positive answers to questions of applicability of any or all of the above assessment factors, as defined, will produce a threat level of either low, medium, high, or imminent.

(1) *Critical.* Factors of existence, capability, and targeting must be present. History and intentions may not be present.

(2) *High.* Factors of existence, capability, history, and intentions must be present. Targeting may not be present.

(3) *Medium.* Factors of existence, capability, and history must be present. Intentions may or may not be present.

(4) *Low.* Existence and capability must be present. History may or may not be present.

(5) *Negligible.* Existence and/or capability may or may not be present.