Assistant Secretary of Defense for
Command, Control, Communications, and
Intelligence (703) 697-5568

DOD 5200.8-R

DEPARTMENT OF DEFENSE

PHYSICAL SECURITY PROGRAM

MAY 1991

UNDER SECRETARY OF DEFENSE FOR POLICY

50272-101

REPORT DOCUMENTATION PAGE	1. REPORT NO. DoD 5200.8-R	2.	3. Recipient's Accession No.
4. Title and Subtitle Physical Security Program			5. Report Date May 1991
			6.
7. Author(s) D. Cavileer			8. Performing Organization Rept. No.
9. Performing Organization Name and Address Under Secretary of Defense for Policy Washington, DC 20301			10. Project/Task/Work Unit No.
			11. Contract(C) or Grant(G) No. (C) (G)
12. Sponsoring Organization Name and Address			13. Type of Report & Period Covered Regulation
			14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

This Regulation describes the DoD Physical Security Program including threat statements, asset priorities, installation requirements, and guidance for the physical security of weapons systems, POL, communication facilities and sensitive materiel.

17. Document Analysis
- a. Descriptors
- b. Identifiers/Open-Ended Terms
- c. COSATI Field/Group

18. Availability Statement	19. Security Class (This Report)	21. No. of Pages
Release unlimited for sale by the National Technical Information Service (NTIS)	UNCLASSIFIED	
	20. Security Class (This Page) UNCLASSIFIED	22. Price

(See ANSI-239.18) *See Instructions on Reverse*

OPTIONAL FORM 272 (4-77)
(Formerly NTIS-35)
Department of Commerce

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D. C. 20301-2000

POLICY

May 13, 1991

FOREWORD

This Regulation is issued under the authority of DoD Directive 5200.8, "Security of DoD Installations and Resources" (April 25, 1991). It prescribes standards and policy relating to the physical protection of military installations and assets of the Department of Defense.

This Regulation applies to the Office of the Secretary of Defense (OSD); the Military Departments (including their National Guard and Reserve components); the Chairman, Joint Chiefs of Staff and Joint Staff; the Unified and Specified Commands; the Inspector General of the Department of Defense (IG, DoD); and the Defense Agencies (hereafter referred to collectively as "DoD Components").

This Regulation is effective immediately. Implementation within 180 days from date of issuance is mandatory for all DoD Components.

It is understood that the review of existing physical security plans and operational concepts will take 1 year, with security upgrades extending through the fiscal year Defense plan in accordance with the methods in Chapter 2 of this Regulation.

Send recommended changes to this Regulation through channels to:

Director, Security Plans and Programs
Office of the Deputy Under Secretary
of Defense (Security Policy)
Room 3C278, The Pentagon
Washington, DC 20301-2200

DoD Components may obtain copies of this Regulation through their own publications channels. Other Federal agencies and the public may obtain copies from the Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

Paul Wolfowitz

PAUL WOLFOWITZ

TABLE OF CONTENTS

CHAPTER 6-SECURITY OF COMMUNICATIONS SYSTEMS

CHAPTER 7-SECURITY OF MATERIEL

FIGURES

REFERENCES

(a) DoD Directive 5200.8, "Security of DoD Installations and Resources" April 25, 1991

(b) DoD Regulation 5200.1-R, "DoD Information Security Program," June 1, 1986, authorized by DoD Directive 5200.1, June 9,1982

(c) Director, Central Intelligence Directive 1/21, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," September 1, 1987

(d) Defense Intelligence Agency Manual 50-3, "Manual for Physical Security Standards for Sensitive Compartmented Information Facilities," February 28, 1990

(e) DoD Manual O-5210.41-M, "Nuclear Weapon Security Manual(U)," September 1987, authorized by DoD Directive 5210.41, September 23, 1988

(f) DoD Directive 5210.65, "Chemical Agent Security Program," October 15, 1986

(g) DoD Directive 5210.63, "Security of Nuclear Reactors and Special Nuclear Materials," April 6, 1990

(h) DoD Manual 5100.76-M, "Physical Security of Sensitive Conventional Arms, Ammunition & Explosives," December 28, 1988, authorized by DoD Directive 5100.76, February 10, 1981

(i) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," 4 January, 1989

(j) DoD Directive 3224.3, "Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment and Support," February 17, 1989

(k) MIL-HNBK-1013/1, "Design Guidelines for Physical Security of Fixed Land-Based Facilities," October 1987

(l) MIL-STD-1785, "System Security Engineering Program Management Requirements," September 1, 1989

(m) DoD Directive O-2000.12, "DoD Combatting Terrorism Program", August 27, 1990

(n) Title 21, Code of Federal Regulations, Parts 1301.71 through 1301.76

(o) Public Law 91-513, "Comprehensive Drug Abuse Prevention and Control Act of 1970"

(p) MIL-STD-1388-2A, "DoD Requirement for a Logistic Support Analysis Record," March 17, 1981

(q) DoD Regulation 4145.19-R-1, "Storage and Materials Handling," September 15, 1979, authorized by DoD Directive 4145.19, August 13, 1975

(r) DoD Manual 4100.39-M, "Defense Integrated Data Systems (DIDS) Procedures Manual," Volume 10, Table 61, September 11, 1980, authorized by DoD Directive 4100.39. September 11, 1980

(s) DLA Joint Regulation 4145.11, "Safeguarding of DLA Sensitive Inventory Items, Controlled Substances, and Pilferable Items of Supply," February 1, 1990

DEFINITIONS

1. Critical Communications Facility. A communications facility that is essential to the continuity of operations of the National Command Authority (NCA) during national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

2. Electronic Security Systems (ESS). That part or physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, intrusion detection systems (IDS), automated entry control systems (AECS), and video assessment systems.

3. Installations. Real DoD properties including bases, stations, forts, depots, arsenals, plants (both contractor and Government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

4. National Defense Area (NDA). An area established on non-Federal lands located within the United States, its possessions or territories, for safeguarding classified information, or protecting DoD equipment and/or materiel. Establishment of a NDA temporarily places such non-Federal lands under effective control of the Department of Defense and results only from an emergency event. The senior DoD representative at the scene shall define the boundary, mark all avenues of approach with a physical barrier, and post warning signs if authorized by the appropriate military commander. The land owner's consent and cooperation should be obtained whenever possible; however, military necessity shall dictate the final decision on location, shape, and size of the NDA.

5. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage and theft.

6. Restricted Area. An area to which entry is subject to special restrictions or control for security reasons, or to safeguard property or materiel. This does not include those designated areas restricting or prohibiting overflight by aircraft. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander, properly posted, and shall employ physical security measures.

7. Survivability. The ability to withstand or repel attack, or other hostile action, to the extent that essential functions can continue or be resumed after onset of hostile action.

8. Systems Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. SSE uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats.

CHAPTER 1

GENERAL INFORMATION

A. PURPOSE

In accordance with the requirements of DoD Directive 5200.8 (reference (a)), this Regulation prescribes DoD policies and minimum standards for the physical protection of DoD personnel, installations, operations, and assets.

B. APPLICABILITY AND SCOPE

1. This Regulation addresses the physical security of personnel, installations, operations, and assets of DoD Components. In overseas areas, combatant commanders may deviate from the policies in this regulation where local conditions, treaties, agreements, and other arrangements with foreign governments and allied forces require.

2. This regulation is intended to provide general minimum requirements which are supplemented by specific asset or unique program-related physical security policies. Detailed and separate instructions are provided for the following assets that are normally found on military installations:

a. Classified Information. See DoD 5200.1-R (reference (b)).

b. Sensitive Compartmented Information Facilities. See DCID 1/21 and DIAM 50-3 (reference (c) and reference (d)).

c. Nuclear Weapons and Nuclear Weapon Systems. See DoD C-5210.41-M (reference (e)).

d. Chemical Agents. See DoD Directive 5210.65 (reference (f)).

e. Nuclear Reactors and Special Nuclear Materials. See DoD Directive 5210.63 (reference (g)).

f. Conventional Arms, Ammunition and Explosives. See DoD 5100.76-M (reference (h)).

g. Special Access Programs. See DoD Directive 0-5205.7 (reference (i)).

3. During transition to war and following commencement of hostilities, Commanders of Unified and Specified Commands may prescribe procedures that modify specific provisions of this Regulation as local conditions and regional threats require. However, security operations and procedures must ensure the maximum protection of Government personnel and property. Under these conditions, these commanders may delegate that authority to unit or installation commanders.

4. This Regulation neither abrogates nor abridges the authority or responsibility of commands to apply more stringent security standards required by other DoD Directives, during emergencies, or at any time required to meet the regional threat.

C. OBJECTIVES

The objectives of this Regulation are to do the following:

1. Establish general policy for the security of personnel and installations, military operations, and certain assets.

2. Provide realistic guidance, general procedures, and the necessary flexibility for commanders to protect personnel, installations, operations, and assets from typical threats.

3. Reduce the loss, theft, or diversion of, and damage to, DoD assets, thereby ensuring that warfighting capability is maintained.

CHAPTER 2

POLICY

A. PHYSICAL SECURITY PROGRAM

1. The physical security program is defined as that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, materiel and documents, and to safeguard them against espionage, sabotage, damage, and theft. Physical security is a primary command responsibility.

2. Physical security programs provide the means to counter threats during peacetime, transition to war, and in wartime. Physical security threats include the following:

a. Foreign intelligence services.

b. Paramilitary forces.

c. Terrorists and saboteurs.

d. Criminals.

e. Protest groups.

f. Disaffected persons.

3. Physical security planning includes the following:

a. Using electronic security systems to reduce both vulnerability to the threat and reliance on fixed security forces.

b. Integration of physical security into contingency, mobilization, and wartime plans, and testing of physical security procedures and measures during the exercise of these plans.

c. Coordinating with installation operations security, crime prevention, information security, personnel security, communications security, automated information security and physical security programs to provide an integrated and coherent effort.

d. Training security forces at facilities or sites in tactical defense against, and response to, attempted penetrations.

e. Creating and sustaining physical security awareness.

f. Identifying resource requirements to apply adequate measures.

4. Physical security measures are a combination of active or passive systems, devices, and security personnel used to protect a security interest from possible threats. These measures include:

a. Security forces and owner or user personnel.

b. Military working dogs.

c. Physical barriers, facility hardening and active delay or denial systems.

d. Secure locking systems, containers, and vaults.

e. Intrusion detection systems.

f. Assessment or surveillance systems (i.e., closed-circuit television or thermal imagers).

g. Protective lighting.

h. Badging systems, access control devices, materiel or asset tagging systems, and contraband detection equipment.

B. RESPONSIBILITIES

The DoD Component shall designate a point of contact to oversee the physical security program. The oversight function includes the following:

1. Develop necessary standard policies and procedures to supplement the provisions of this regulation to meet specific needs, including joint supplementation, when possible.

2. Coordinate and maintain liaison with the other Departments and Agencies on physical security matters.

3. Establish procedures for sharing threat information expeditiously through law enforcement and intelligence channels.

4. Formalize security procedures for joint response to terrorist incidents.

5. Develop specific physical security threat assessments and update them annually or as needed.

6. Coordinate the acquisition of physical security equipment and establish procedures to identify requirements for related research as described in DoD Directive 3224.3 (reference (j)).

7. Develop training, qualification, and suitability requirements for dedicated security forces (including contract

security forces where not prohibited), security technicians and physical security specialists.

C. SECURITY SYSTEM PERFORMANCE GOAL

1. The goal of the security system for an asset or facility is to deploy security resources so as to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage or other criminal activity. To achieve this goal a security system provides the capability to detect, assess, communicate, delay and respond to an unauthorized attempt at entry.

2. The components of a security system each have a function and related measures which provide an integrated capability for the following:

a. Detection, accomplished through human, animal or electronic means, alerts security personnel to possible threats and attempts at unauthorized entry at or shortly after time of occurrence;

b. Assessment, through use of video subsystems, patrols or fixed posts, assists in localizing and determining the size and intention of an unauthorized intrusion or activity;

c. Command and control, through diverse and secure communications to ensure that all countermeasures contribute to preventing or containing sabotage, theft or other criminal activity;

d. Delay, through the use of active and passive security measures, including barriers, impedes intruders in their efforts to reach their objective;

e. Response, through the use of designated, trained and properly equipped security forces. Detection, and delay must provide sufficient warning and protection to the asset until the response force can be expected to arrive at the scene.

D. PHYSICAL SECURITY THREAT MATRIX

At Figure 2-1 is a description of the DoD generic threat types developed for the physical security program. Using these threat types as a guide, commanders shall develop program, system, command or installation threat statements which assess potential security threats to critical assets. Using both law enforcement and intelligence information, these assessments should categorize opportunity (when possible) and capabilities of potential adversaries. Physical security threat statements will be used for the development of security systems tailored to the protection of assets and items of security interest.

THREAT TYPE	THREAT DESCRIPTION	THREAT EXAMPLE
MAXIMUM	INDIVIDUALS IN ORGANIZED AND TRAINED GROUPS ALONE OR WITH ASSISTANCE FROM AN INSIDER; SKILLED ARMED AND EQUIPPED INTRUDERS WITH PENETRATION AIDS	TERRORISTS AND SPECIAL PURPOSE FORCES; HIGHLY TRAINED INTELLIGENCE AGENTS
ADVANCED	INDIVIDUAL(S) WORKING ALONE OR IN COLLUSION WITH AN INSIDER; SKILLED OR SEMISKILLED WITHOUT PENETRATION AIDS	HIGHLY ORGANIZED CRIMINAL ELEMENTS; TERRORISTS OR PARAMILITARY FORCES; FOREIGN INTELLIGENCE AGENTS WITH ACCESS
INTERMEDIATE	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE OR IN SMALL GROUPS; SOME KNOWLEDGE OR FAMILIARITY OF SECURITY SYSTEM	CAREER CRIMINALS;ORGANIZED CRIME;WHITE COLLAR CRIMINALS; ACTIVE DEMONSTRATORS; COVERT INTELLIGENCE COLLECTORS; SOME TERRORIST GROUPS
LOW	INDIVIDUAL(S) OR INSIDER(S) WORKING ALONE OR IN A SMALL GROUP	CASUAL INTRUDERS; PILFERERS AND THIEVES; OVERT INTELLIGENCE COLLECTORS; PASSIVE DEMONSTRATORS

Figure 2-1. Physical Security Threat Matrix

E. PRIORITIZATION OF ASSETS

At Figure 2-2 is a description of the DoD resource and asset prioritization scheme with examples of typical assets, a criticality definition, and an example of a typical security system for each level. DoD Components shall develop appropriate operational concepts or security standards to meet the performance goal of paragraph C against the type of threats defined in paragraph D for critical assets designated by the Component under each security system level. Security system levels are assigned to critical assets or major systems in security planning documents to ensure that minimum security standards are met. Commanders are responsible for higher levels of security afforded personnel, equipment and assets within the command depending on regional threat.

F. PHYSICAL SECURITY PLANNING AND SYSTEM ACQUISITION

DoD Components shall establish procedures to ensure that physical security planning for the acquisition of major systems is appropriate, and in accordance with paragraph E above. One management solution is provided by MIL-STD-1785 (reference (l)).

G. PROTECTIVE DESIGN AND MILITARY CONSTRUCTION

DoD Components shall establish procedures to ensure that all military construction projects are reviewed at the conceptual stage and throughout the process so that appropriate physical security, antiterrorist or protective design features are incorporated into the design. Use MIL-HNBK-1013/1 (reference (k)) or other approved security engineering guidance for information.

H. SECURITY OF LEASED FACILITIES

DoD Components shall establish procedures to ensure that leases for DoD activities resident within commercial facilities include provisions for positive physical security of DoD occupied areas.

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
A INTEGRATED ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, ACCESS DELAY AND DENIAL SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED IMMEDIATE RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE WILL RESULT IN GREAT HARM TO THE STRATEGIC CAPABILITY OF THE UNITED STATES	NUCLEAR AND CHEMICAL WEAPONS AND ALERT/MATED DELIVERY SYSTEMS CRITICAL COMMAND, CONTROL AND COMMUNICATIONS FACILITIES AND SYSTEMS CRITICAL INTELLIGENCE GATHERING FACILITIES AND SYSTEMS PRESIDENTIAL TRANSPORT SYSTEMS NUCLEAR REACTORS AND CATEGORY I AND II SPECIAL NUCLEAR MATERIALS RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
B ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIER SYSTEMS, DEDICATED SECURITY FORCES, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD BE EXPECTED TO GRAVELY HARM THE OPERATIONAL CAPABILITY OF THE UNITED STATES	ALERT SYSTEMS, FORCES, AND FACILITIES ESSENTIAL COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY I ARMS, AMMUNITION, AND EXPLOSIVES RESEARCH, DEVELOPMENT AND TEST ASSETS

Figure 2-2. Resource and Asset Priorities

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
C ELECTRONIC SECURITY SYSTEMS, ENTRY AND CIRCULATION CONTROL, BARRIERS, SECURITY PATROLS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD IMPACT UPON THE TACTICAL CAPABILITY OF THE UNITED STATES	NONALERT RESOURCES AND ASSETS PRECISION GUIDED MUNITIONS COMMAND, CONTROL, AND COMMUNICATIONS FACILITIES AND SYSTEMS CATEGORY II ARMS, AMMUNITION AND EXPLOSIVES POL/POWER/ WATER /SUPPLY STORAGE FACILITIES RESEARCH, DEVELOPMENT AND TEST ASSETS

SECURITY SYSTEM LEVEL	ASSET DEFINITION	ASSET EXAMPLE
D ELECTRONIC SECURITY SYSTEMS, ACCESS CONTROLS, BARRIERS, DESIGNATED RESPONSE FORCES	THE LOSS, THEFT, DESTRUCTION OR MISUSE OF THIS RESOURCE COULD COMPROMISE THE DEFENSE INFRASTRUCTURE OF THE UNITED STATES	ARMS, AMMUNITION, AND EXPLOSIVES EXCHANGES AND COMMISSARIES, FUND ACTIVITIES CONTROLLED DRUGS AND PRECIOUS METALS TRAINING ASSETS RESEARCH, DEVELOPMENT AND TEST ASSETS

CHAPTER 3

INSTALLATION ACCESS AND CIRCULATION CONTROL

A. GENERAL

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 commander must clearly define the access control measures (tailored to local conditions) required to safeguard facilities and ensure accomplishment of the mission.

B. POLICY

It is DoD policy that DoD Components shall develop, establish, and maintain policies and procedures to control access to installations, including the following:

1. Using a defense-in-depth concept to provide gradated levels of protection from the installation perimeter to critical assets.

2. Determining the degree of control required over personnel and equipment entering or leaving the installation.

3. Prescribing procedures for inspecting persons, their property and vehicles at entry and exit points of installations or at designated secure areas within an installation, and for search of persons and their possessions while on the installation.

(a) This shall include determination of whether searches or inspections are randomly conducted or mandatory for all. See DoD Regulation 5200.1-R, Chapter 5, Section 3 (reference (b)) prescribing inspection procedures for the safeguarding of classified information.

(b) Examinations of individuals and their possessions while on the installation for the primary purpose of obtaining evidence is classified as a "search" under the Fourth Amendment and separate guidance regarding the conduct of these searches will be issued.

(c) All procedures shall be reviewed for legal sufficiency by the appropriate General Counsel or Legal Advisor to the DoD Component prior to issuance. The procedures shall require Commanders to consult with their servicing Judge Advocate or other legal advisor before authorizing gate inspections.

4. Enforcing the removal of, or denying access to, persons who are a threat to order, security and the discipline of the installation.

5. Designating Restricted Areas to safeguard property or materiel for which the commander is responsible.

6. Using randomized antiterrorism measures within existing security operations to reduce patterns, change schedules and visibly enhance the security profile of an installation. This reduces the effectiveness of preoperational surveillance by hostile elements.

C. INSTALLATION ACCESS

DoD Components shall:

1. Determine necessary access controls based on the considerations in Chapter 2 of this Regulation. This will include the evaluation of automated entry control systems or access devices, where necessary.

2. Allocate resources necessary to enforce the established controls. These controls will be monitored and evaluated to ensure adequate protection is maintained.

D. EMERGENCY PLANNING

1. DoD Components shall require commanders to plan for increasing vigilance and restricting access at installations under the following situations:

a. National emergency.

b. Disaster.

c. Terrorist threat conditions (See DoD Directive 2000.12 (reference (m)) for further information).

d. Significant criminal activity.

e. Civil disturbance.

f. Other contingencies that would seriously affect the ability of installation personnel to perform their mission.

2. Planning should include the following:

a. Coordination with local, state, federal, or host country officials to ensure integrity of restricted access to the installation and reduce the effect on surrounding civilian communities;

b. Establishment of a system for positive identification of personnel and equipment authorized to enter and exit the installation;

c. Maintenance of adequate physical barriers that will be installed to control access to the installation;

d. Predesignation of personnel, equipment, and other resources to enforce restricted access and respond to incidents;

e. Exercising contingency plans to validate their effectiveness.

CHAPTER 4

SECURITY OF WEAPON SYSTEMS AND PLATFORMS

A. GENERAL

This Chapter establishes policy and responsibility for security of weapon systems, including platforms, such as armored fighting vehicles, fixed and rotary wing aircraft, and ships in port. DoD Components have a responsibility to protect weapon systems, particularly those in operational roles during a conflict, regardless of location.

B. POLICY

1. Commanders are responsible for the security of assigned, or transient weapon systems while these systems are resident on their installations. Commanders shall develop security plans to meet this responsibility.

2. Each DoD Component shall issue instructions governing the security of its weapon systems and describing the security concept for each class of platform, in accordance with Chapter 2 of this Regulation. The priority for security placed on similar systems or platforms within each DoD Component inventory may vary due to differences in the following:

a. Mission;

b. Location and vulnerability;

c. Operational readiness;

d. Value, classification, and replacement costs.

3. Before operations, the owning DoD Component should request special security support from the host installation, if necessary, as far in advance as possible. Economic and logistical considerations dictate that every reasonable effort be made by the host installation to provide the necessary security without resort to external support from the owning DoD Component. The owning DoD Component should provide materiel and personnel for extraordinary security measures (extraordinary security measures are those that require heavy expenditures of funds, equipment, or manpower; or unique or unusual technology) to the host installation.

CHAPTER 5

PROTECTION OF BULK PETROLEUM PRODUCTS

A. GENERAL

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.

B. POLICY

It is DoD policy that:

1. Commanders of GOGO and GOCO fuel support points, pipeline pumping stations, and piers shall designate and post these installations as Restricted Areas.

2. Access to these facilities shall be controlled and only authorized personnel shall be permitted to enter. Commanders shall determine the means required to enforce access control (i.e., security forces, barriers, lighting, and security badges) based on the considerations in Chapter 3 of this Regulation.

3. Security force personnel shall be equipped with a primary and an alternate means of communications to alert other military or civilian law enforcement agencies, as appropriate, in event of an intrusion, fire, or other emergency.

C. SECURITY PLANNING AND LIAISON

Commanders shall take the following actions to protect their fuel facilities:

1. Establish liaison and coordinate contingency plans and inspection requirements with the nearest U.S. military installation to provide manpower and equipment resources to the facility in the event of emergencies and increased threat conditions.

2. Establish liaison with supporting, local, State, and Federal law enforcement agencies and host nation officials; and support agreements, if appropriate.

CHAPTER 6

SECURITY OF COMMUNICATIONS SYSTEMS

A. GENERAL

1. This Chapter describes concepts for physical security of communications facilities located on and off military installations, to include mobile systems. Specific security support for facilities that require special security measures shall be coordinated between the concerned Components.

2. Because of the difference in location, physical layout and equipment, security considerations must be thoroughly assessed for each communications system. The physical security program shall be tailored to that particular facility or system.

B. POLICY

1. It is DoD policy that the protection provided to DoD communication facilities and systems shall be sufficient to ensure continuity of operations of critical users and the facilities they support. These include nuclear weapon delivery units and storage facilities, main operating bases (for allied air forces), and primary command and control elements. The determinations on strategic importance, both to the United States and its allies, shall be based upon whether or not each mobile system or facility processes, transmits, or receives, telecommunications traffic considered crucial by the National Command Authorities (NCA), the Chairman, Joint Chiefs of Staff, or the Commanders in Chief of the Unified and Specified Commands.

2. Communications systems play a major role in support of each DoD Component's mission, providing operational communications in both peacetime and wartime. These are attractive targets due to limited staffing, isolated location and mission. Therefore, security for these systems must be an important part of each command's physical security program.

3. The DoD Component must review the host installation's implementation of physical security measures during inspections, oversight, and staff visits.

4. Access shall be controlled at all communications facilities; only authorized personnel shall be allowed to enter. Facilities should be designated and posted as Restricted Areas.

5. Depending on regional conditions, commanders should consider locating enough weapons and ammunition at communications facilities to arm designated onsite personnel. If arms are stored at the facilities, appropriate security measures and procedures shall be employed in accordance with DoD 5100.76-M (reference (h)).

6. Existing essential structures should be hardened against attacks. This includes large antenna support legs, antenna horns, operations building and cable trays. Future construction programs for communications facilities should include appropriate hardening of essential structures.

C. RESPONSIBILITIES

1. DoD Components shall have each major command identify critical communications facilities and mobile systems.

2. DoD Components shall have each commander of a major command ensure that a security plan is developed for each communications facility and mobile system under his or her command. The plan shall include emergency security actions and procedures for emergency destruction of sensitive equipment and classified information. The plan may be an annex to an existing host installation security plan; only the applicable parts of the total plan shall be distributed to personnel at the facility or mobile system.

3. The owning DoD Component shall arrange for security of off-installation facilities and mobile systems with the closest U.S. military installation. This includes contingency plans for manpower and equipment resources during emergencies. These arrangements can be made by establishing a formal agreement, such as an interservice support agreement. Whether the facilities are located on or off the installation, or mobile, installation commanders are responsible for security of communications facilities for which they provide host support.

4. Operations, maintenance, and communications personnel at the facility or mobile system are the most important factor in security. DoD Components shall have each commander of a major command ensure implementation of a training program to ensure that 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 shall include the following:

a. Security procedures and personal protection skills for assigned personnel.

b. The use of weapons and communications equipment for protecting the facility or mobile system.

c. Awareness of local terrorist threats and other activity in the area.

5. DoD Components may issue additional instructions governing security of the communications facilities.

D. MOBILE COMMUNICATIONS SYSTEMS

In accordance with Chapter 2 of this Regulation, a security operational concept or standards shall be developed for mobile systems to describe the minimum level of security for the system in the expected operational environment.

CHAPTER 7

SECURITY OF MATERIEL

A. GENERAL

1. This Chapter provides security policy and procedures for safeguarding controlled inventory items, including drugs, drug abuse items, as identified under 21 CFR 1301.71 through 1301.76 and P.L. 91-513 (references (n) and (o)), and precious metals .

2. DoD materiel assigned a code indicating the security classification and/or security risk or pilferage controls for storage and transportation in accordance with MIL-STD-1388-2A, (reference (p)) shall be afforded special attention, as in DoD 4145.19-R-1 (reference (q)). Controlled Inventory Item Codes (CIIC) are in DoD 4100.39-M (reference (r)).

B. POLICY

1. The security of controlled inventory items is of special concern to The Department of Defense. Consequently, these items shall have characteristics so that they can be identified, accounted for, secured or segregated to ensure their protection and integrity.

2. DoD Components shall pay special attention to the safeguarding of inventory items by judiciously implementing and monitoring physical security measures. This shall include analysis of loss rates through inventories, reports of surveys, and criminal incident reports, to establish whether repetitive losses indicate criminal or negligent activity.

3. These requirements apply to stocks at depot, base, and installation supply level. Small unit or individual supplies below the base or installation level shall be afforded protection, as determined by the commander.

C. RESPONSIBILITIES

1. DoD Components shall:

a. Establish physical security measures to protect inventory items at depot, base and installation level.

b. Monitor the effective implementation of security requirements through scheduled inspections of and staff or oversight visits to affected activities.

c. Ensure that adequate safety and health considerations are incorporated into the construction of a security area for controlled inventory items.

2. Commanders shall ensure that security measures are established and are functioning to reduce the incentive and opportunity for theft.

D. PROCEDURES

1. Commanders will ensure that storage facilities and procedures for operation adequately safeguard controlled inventory items.

2. Security requirements for inventory items in storage are as follows:

a. General security requirements for classified, sensitive, and pilferable items are in DoD 4145.19-R-1, (reference (q)).

b. Specialized storage requirements for arms, ammunition and explosives are in DoD 5100.76-M, (reference (h)).

c. Additional guidance for the secure storage of sensitive inventory items, controlled substances and pilferable items is in DLAR 4145.11 (reference (s)).