PHYSICAL SECURITY PROGRAM

April 9, 2007

Incorporating Change 1,
May 27, 2009

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

(USD(I))

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

APR 9 2007

FOREWORD

This Regulation is issued under the authority of DoD Instruction 5200.08, "Security of DoD Installations and Resources," December 10, 2005. It implements the policies and minimum standards for the physical security of DoD installations and resources.

DoD 5200.08-R, "Physical Security Program," May 1991, is hereby canceled.

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

This Regulation is effective immediately and is mandatory for the DoD Components.

Send recommended changes to this Regulation to the following address:

Director of Security
Deputy Under Secretary of Defense (CI&S)
Office of the Under Secretary of Defense for Intelligence
Room 3A666, Pentagon
5000 Defense Pentagon
Washington, D.C. 20301-5000

The DoD Components, other Federal agencies, and the public may download this Regulation from the Washington Headquarters Services Directives web page at http://www.dtic.mil/whs/directives. Approved for public release; distribution unlimited.

Robert Andrews
Acting Under Secretary of Defense for Intelligence

TABLE OF CONTENTS

REFERENCES

(a) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” as amended
(b) DoD Instruction 5200.08, "Security of DoD Installations and Resources," December 10, 2005
(c) DoD 5200.1-R, "DoD Information Security Program," January 1997
(d) Director, Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," November 18, 2002
(e) DoD Directive O-5210.41, "Security Policy for Protecting Nuclear Weapons," November 1, 2004
(f) DoD Instruction 5210.65, "Minimum Security Standards for Safeguarding Chemical Agents," March 12, 2007
(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 and Explosives," August 12, 2000
(i) DoD Directive 5205.07, "Special Access Program (SAP) Policy," January 5, 2006
(j) DoD Instruction 5210.84, “Security of DoD Personnel at U.S. Missions Abroad,” October 15, 1996
(k) Chapter 169, Section 2859, Title 10, United States Code
(l) DoD Directive 3224.3, "Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment and Support," February 17, 1989
(m) DoD Instruction 2000.16, “DoD Antiterrorism (AT) Standards,” October 02, 2006
(n) DoD Directive 2000.12, "DoD Anti-Terrorism (AT) Program," August 18, 2003
(o) UFC 4-010-01, Unified Facilities Criteria, “DoD Minimum Antiterrorism Standards for Buildings,” October 8, 2003
(p) Under Secretary of Defense, Acquisition, Technology and Logistics Memorandum, “Department of Defense Unified Facilities Criteria,” dated May 29, 2002
(q) Military Standard-3007F, "Standard Practice for Unified Facilities Criteria and Unified Facilities Guide Specification,” December 13, 2006
(r) Federal Information Processing Standards (FIPS) 201-1, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” March 01, 2006
(s) Homeland Security Presidential Directive-12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004
(t) DoD Directive 1000.25, “DoD Personnel Identity Protection (PIP) Program,” July 19, 2004
(u) DoD 4500.9R-Part II, “Defense Transportation Regulation,” November 2004
(v) DoD Directive 3020.40, “Defense Critical Infrastructure Program (DCIP),” August 19, 2005
(w) Title 21, Code of Federal Regulation, Parts 1301.71 through 1301.76
(x) Public Law 91-513, "Comprehensive Drug Abuse Prevention and Control Act of 1970"
(y) Military Standard-1388-2A, "DoD Requirement for a Logistic Support Analysis Record," March 17, 1981

(z) DoD Regulation 4145.19-R-1, "Storage and Materials Handling," September 15, 1979

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

DL1. DEFINITIONS

For the purposes of this Regulation, terms are defined below and in Joint Publication 1-02 (Reference (a)).

DL1.1. Antiterrorism. See Reference (a).

DL1.2. Capability. Facilitating method to implement a course of action. (A capability may or may not be accompanied by an intention).

DL1.3. Controlled Area. A controlled space extending upward and outward from a specified point. This area is typically designated by a commander or director, wherein sensitive information or operations occur and requires limitations of access.

DL1.4. Critical Communications Facility. A communications facility that is essential to the continuity of operations of the President or Secretary of Defense during national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

DL1.5. Counterintelligence. See Reference (a).

DL1.6. Electronic Security Systems (ESS). That part of 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.

DL1.7. Installations. Real DoD properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor and Government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

DL1.8. National Defense Area (NDA). See Reference (a).

DL1.9. Personnel Identity Management and Protection. A business process that validates, authenticates and secures an individual's identity. The process includes: identity vetting; a binding of the identity to an identity protection and management system through the issuance of a DoD credential; the linkage of the Personal Identity Verification (PIV) credential to the individual through the use of uniquely identifying characteristics and a personal identification number; and digital authentication of the identification credential linkage to the individual.

DL1.10. Physical Security. See Reference (a)

DL1.11. Resources. Personnel and/or materials provided as a means of support (does not refer to monetary source for purposes of this guidance).

DL1.12. Restricted Area. An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. 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/director, properly posted, and shall employ physical security measures. Additionally, Controlled Areas may be established adjacent to Restricted Areas for verification and authentication of personnel.

DL1.13. Risk. A measure of consequence of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).

DL1.14. Risk Assessment. A defined process used to fuse the procedures of analyzing threat, risks, and vulnerabilities, into a cohesive, actionable product.

DL1.15. Risk Management. Process and resultant risk of systematically identifying, assessing and controlling risks. Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements.

DL1.16. 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.

DL1.17. Security-in-Depth. A determination by the senior agency official that a facility's security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. Examples include the use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard patrols throughout the facility during non-working and working hours, and closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

DL1.18. Threat. The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.

DL1.19. Threat Analysis. The continual process of compiling and examining all available information concerning the capability, activity, and intention of potential aggressors, which supports the deployment and degree of countermeasure requirements to address the perceived threat.

DL1.20. Threat Assessment. A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity.

DL 1.21. Vulnerability. A situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources.

DL1.22. Vulnerability Assessment. The comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and /or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management.

C1. CHAPTER 1

GENERAL INFORMATION

C1.1. PURPOSE

In accordance with the requirements of DoD Instruction 5200.08, (Reference (b)), this Regulation implements DoD policies and minimum standards for the physical protection of DoD personnel, installations, operations, and related resources.

C1.2. APPLICABILITY AND SCOPE

C1.2.1. This Regulation addresses the physical security of personnel, installations, facilities, operations, and related resources of DoD Components. In overseas areas, Combatant Commanders (COCOMs) may deviate from the policies in this Regulation where local conditions, treaties, agreements, and other arrangements with foreign governments and allied forces require.

C1.2.2. This Regulation provides minimum standards for the protection of resources normally found on installations and unique resources on the installation. Separate guidance shall be referred to for:

C1.2.2.1. Classified Information; DoD 5200.1-R, (Reference (c)).

C1.2.2.2. Sensitive Compartmented Information Facilities; DCID 6/9, (Reference (d)).

C1.2.2.3. Security Policy for Protecting Nuclear Weapons; DoD Directive 5210.41, (Reference (e)).

C1.2.2.4. Security of DoD Chemical Agents; DoD Instruction 5210.65, (Reference (f)).

C1.2.2.5. Nuclear Reactors and Materials; DoD Directive 5210.63, (Reference (g)).

C1.2.2.6. Physical Security Arms, Ammunition and Explosives; DoD Manual 5100.76-M, (Reference (h)).

C1.2.2.7. Special Access Program; DoD Directive 5205.07, (Reference (i)).

C1.2.2.8. Security of DoD Personnel assigned to U.S. Missions Abroad; DoD Instruction 5210.84, (Reference (j)).

C1.2.3. During transition to war and following commencement of hostilities, COCOMs may prescribe procedures that modify specific provisions of this Regulation as local threat and risk conditions require. However, security operations and procedures must ensure the effective protection of Government assets. Under these conditions, COCOMs may delegate that authority to unit or installation commanders.

C1.2.4. Nothing in this Regulation abrogates the authority or responsibility of commanders to apply more stringent security standards required by other DoD Issuances during emergencies, increased threat level or high risk determinations, or as the commander/director deems necessary.

C1.3. OBJECTIVES

The objectives of this Regulation are to:

C1.3.1. Implement general policy for the security of personnel, installations, military operations, and certain additional assets.

C1.3.2. Provide security guidance and general procedures that are realistic, harmonized with other security disciplines, and provide the necessary flexibility for commanders to protect personnel, installations, projects, operations, and related resources against capable threats from terrorists, criminal activity, and other subversive or illegal activity.

C1.3.3. Reduce the loss, theft, diversion of, or damage to DoD assets through the use of advanced technologies; thereby enhancing overall security, while ensuring that warfighting capability is maintained.

C1.3.4. Standardize personal identification and authentication to DoD installations and facilities, including interoperability with other Federal entities, utilizing the DoD PIV credential (Common Access Card (CAC)) as the universal authority of individual authenticity*, consistent with applicable law*. The DoD PIV credential will provide the HSPD-12 mandated level of identity assurance and government-wide recognition.

C2. CHAPTER 2

POLICY OBJECTIVES

C2.1. PHYSICAL SECURITY PROGRAM

C2.1.1. The physical security program is that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. Physical security is a primary command responsibility.

C2.1.2. Physical security programs are designed for prevention and provide the means to counter threats when preventive measures are ignored or bypassed. Physical security threats include, but are not limited to:

C2.1.2.1. Foreign intelligence services.

C2.1.2.2. Foreign military and paramilitary forces.

C2.1.2.3. Terrorists and saboteurs.

C2.1.2.4. Criminals.

C2.1.2.5. Protest groups.

C2.1.2.6. Disaffected persons.

C2.1.3. Physical security planning includes:

C2.1.3.1. Using biometric, electronic and/or mechanical technological security systems to mitigate both vulnerability to the threat and reduce reliance on fixed security forces.

C2.1.3.2. Implementing physical security programs to form the basis of integrated defense plans, which builds physical security into contingency, mobilization, antiterrorism, and wartime plans, and tests of physical security procedures and measures during the exercise of these plans.

C2.1.3.3. Coordinating physical security with operations security, law enforcement, information security, personnel security, communications security, automated information security, counterintelligence and antiterrorism programs to provide an integrated and coherent effort. This effort consists of understanding the threat, reviewing the vulnerabilities, and identifying priorities. Risks can therefore be managed as to their criticality to the mission and physical security program requirements confidently submitted to the Plans, Programming, Budgeting, and Execution System (PPBES) process.

C2.1.3.4. Training security forces and owner or user personnel at facilities or sites in defense against, and response to, unauthorized penetrations.

C2.1.3.5. Creating and sustaining physical security awareness training for all personnel.

C2.1.4. Physical security employs physical protective and security procedural measures in combination with active or passive systems, technologies, devices, and security personnel used to protect assets from possible threats. These measures include:

C2.1.4.1. Security forces and owner or user personnel.

C2.1.4.2. Military working dogs.

C2.1.4.3. Physical barriers, facility hardening, and active delay or denial systems.

C2.1.4.4. Secure locking systems, containers, and vaults.

C2.1.4.5. Electronic security systems (e.g., IDS, radio frequency detectors, electronic emissions detectors).

C2.1.4.6. Assessment or surveillance systems (e.g., closed-circuit television, thermal imagers, millimeter wave, radar).

C2.1.4.7. Protective lighting (e.g., visible, IR).

C2.1.4.8. Credential technologies, access control devices, biometrics, materiel or asset tagging systems, and contraband detection equipment.

C2.2. RESPONSIBILITIES

The Heads of the DoD Components shall designate a program manager to oversee the physical security program. The oversight function includes:

C2.2.1. Developing standard policies and procedures to supplement the provisions of this Regulation to meet specific needs, including joint supplementation, when possible.

C2.2.2. Maintaining liaison with the antiterrorism, counterintelligence, and law enforcement entities to coordinate and integrate seamless awareness, reporting, and First Responder programs to provide practical, expedient and credible flow of critical information.

C2.2.3. Formalizing security procedures for joint response to adverse or terrorist incidents.

C2.2.4. Conducting specific physical security threat assessments and update them annually or as needed (see Chapter 169, section 2859, title 10, United States Code (Reference (k))).

C2.2.5. Establishing and coordinating requirements for the acquisition of physical security equipment and establish procedures to identify requirements for related research as described in DoD Directive 3224.3, (Reference (l)).

C2.2.6. Developing training, qualification, and suitability requirements for dedicated security forces (including contract security forces where employed, security technicians, and physical security specialists).

C2.3. SECURITY SYSTEM PERFORMANCE GOAL

C2.3.1. The goal of the security system for an installation, area, facility, or asset is to employ Security-in-Depth: 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 deter, detect, identify, track, assess, record, communicate, delay, and respond to unauthorized access activities.

C2.3.2. Each security system component has a function and related measures that provide an integrated capability for:

C2.3.2.1. Deterrence as an immediate indication of deliberate attempts, security probing, and warning for inadvertent or mistaken intention;

C2.3.2.2. Detect, identify and track, through human, animal, or electronic means, and alert security personnel to possible threats and attempts at unauthorized entry at or shortly after time of occurrence;

C2.3.2.3. 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;

C2.3.2.4. Communications, secure and diverse, used for command and control, that provide countermeasures that contribute to prevention and containment of sabotage, theft, or other criminal activity;

C2.3.2.5. Delay, through the use of active and passive security measures, including a full range of barriers, impeding intruders in their efforts to reach their objective; and

C2.3.2.6. Response will provide the use of designated, trained and properly equipped security forces. The responsive forces must also have assessed the situational requirements through the detection and delay, accounting for sufficient warning and protection to the asset, until the response force can be expected to arrive at the scene.

C2.4. PHYSICAL SECURITY/ANTITERRORISM INTEGRATION

Threat level guidance and Force Protection Conditions are designed to enhance the baseline physical security requirements at DoD installations and facilities, due to heightened terrorist threat or action. The antiterrorism security measures are employed as a whole, or in part (as directed by the commander/director), at installations and facilities. These procedures are found in DoD Instruction 2000.16, (Reference (m)) and DoD Directive 2000.12, (Reference (n)).

C2.5. PHYSICAL SECURITY PLANNING, SYSTEM ACQUISITION, CONSTRUCTION, AND LEASING STANDARDS

C2.5.1. Heads of the DoD Components shall establish procedures for physical security planning, construction, and acquisition of facilities or buildings as appropriate and in accordance with UFC 4-010-01, Unified Facilities Criteria, (Reference (o)). Unified Facilities Criteria (UFC) instruction provides protective design planning, construction, sustainment, restoration, and modernization criteria for installations and leased facilities, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with Undersecretary of Defense, Acquisition, Transportation and Logistics Memorandum dated May 29, 2002, (Reference (p)). UFC instructions are distributed only in electronic media and are effective upon issuance. The UFC system is found on the world-wide web. The UFC system is prescribed by Military Standard 3007F, (Reference (q)).

C2.5.2. Federal Information Processing Standards (FIPS) 201-1, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” March 01, 2006, (Reference (r)) provides guidance for the acquisition of Federal PIV credentials and supporting equipment, when fulfilling the requirements for Federal standards of identity and access control. Further information directing the acquisition of a Federal credential is found in Chapter 3.

C2.5.3. DoD Components securing existing access doors with high security padlocks and hasps may continue their use, in accordance with Reference (h). However, new construction or planned upgrades to access doors for Category I and II Arms, Ammunition & Explosives (AA&E) areas shall require the installation of the Internal Locking Device, see Reference (h).

C3. CHAPTER 3

INSTALLATION ACCESS AND EMERGENCY PLANNING

C3.1. GENERAL

This chapter implements general procedures that meet minimum Federal standards for controlling entry onto and exiting from military installations and the facilities within military installations. Access control is an integral and interoperable part of DoD installation physical security programs. Each installation commander/facility director must clearly define, consistent with DoD policy, the access control measures (tailored to local conditions) required to safeguard personnel, facilities, protect capabilities, and accomplish the mission.

C3.2. PROCEDURES

DoD Components shall develop, establish and maintain uniform policies that support interoperable procedures to control access to installations and facilities, including:

C3.2.1. Implementing DoD Antiterrorism Standards and DoD Antiterrorism Program (References (m) and (n)), which provide the definitive guidance to the COCOMs and subordinate commanders as to implementation of specific security measures (e.g., inspecting persons, property and/or vehicles) based upon the level of threat. Employment of the measures demonstrates Security-in-Depth through a layered security effort to identify, diminish, and/or eliminate the threat.

C3.2.2. Developing appropriate operational concepts or security standards to meet the performance goal of section C2.3. of this publication. Therefore, where appropriate, security system levels shall be included in security planning documents to assure minimum security standards.

C3.2.3. Using random antiterrorism measures within existing security operations to reduce patterns, change schedules, and visibly increase the security profile of an installation. This enhances the possible detection of violation(s) and reduces the effectiveness of pre-operational surveillance by hostile elements and/or unauthorized personnel.

C3.2.4. Designating restricted or controlled areas to safeguard property or resources for which the commander is responsible (area designations such as restricted and controlled shall be directed appropriately by the responsible commander to safeguard mission essential property or material).

C3.2.5. Enforcing the removal of, or denying access to, persons who threaten security, order, and the discipline of the installation.

C3.2.6. Reviewing all access control procedures (such as inspecting an individual and their possessions while on the installation) for legal sufficiency by the appropriate General Counsel or Legal Advisor to the DoD Component prior to issuance.

C3.3. INSTALLATION ACCESS

C3.3.1. Homeland Security Presidential Directive-12 (HSPD-12), (Reference (s)), mandates policy for a common identification standard for all Federal employees and contractors. The Federal Information Processing Standard 201-1 (FIPS 201-1), (Reference (r)), provides standards for the identity verification, issuance, and use of the common identity standard. The DoD Federal PIV credential, the CAC, will provide a level of identity assurance and a method of authentication. *Consistent with applicable law,* ~~T~~the CAC shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. The credential will provide for a consistent, government-wide, identification and authentication approach to facility and information security, and increase confidence in the overall security posture. The CAC, upon presentation at perimeter security locations, shall be accepted for perimeter screening purposes. Specific implementation standards directed by HSPD-12/FIPS 201-1 are:

C3.3.1.1. The development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification, shall be issued to Federal employees and contractors as identified in DoD Directive 1000.25, (Reference (t)).

C3.3.1.2. A National Agency Check with Inquiries (NACI) or equivalent national security clearance (e.g. National Agency Check with Local Agency Checks including Credit Check (NACLC)) is required for permanent issuance of the credential. The credential may be issued upon favorable return of the FBI fingerprint check, pending final favorable completion of the NACI/equivalent, based on a commander/director risk management decision. An individual holding a valid national security clearance shall not require an additional submission of the NACI/equivalent.

C3.3.1.3. Credentials issued to individuals without a completed NACI/equivalent will be electronically distinguishable from those credentials revealing a completed NACI/equivalent.

C3.3.1.4. Occasional visitors to Federal facilities will continue using a locally established, temporary issue, visitor identification system.

~~C3.3.2. The Defense Biometric Identification System (DBIDS) card shall be issued and authorized for routine, physical access, to a single DoD installation or facility. The DBIDS card renders a source of identity and verification of affiliation with the Department of Defense, and is a proven physical access system in accordance with Reference (r). The DBIDS card, while not an interagency PIV credential, shall have a standard vetting requirement. A National Agency Check (NAC) or equivalent national security clearance is required for permanent issuance of the DBIDS credential. The credential may be issued upon favorable return of the FBI fingerprint check, pending final favorable completion of the NAC, based on a commander/director risk~~

~~management decision. An individual holding a valid national security clearance shall not require an additional submission of the NAC.~~

C3.3.~~3~~2. ~~Upon full implementation of the CAC, the standard DoD PIV access control credential and the DBIDS credential, eliminate all other non-FIPS 201-1 compliant badges and associated equipment used for physical access (see Reference (r)).~~ Existing legacy Physical Access Systems (PAS) will continue to operate until upgraded or replaced with compliant systems. Operating maintenance costs to existing PAS must be balanced and justified against use of such funds toward transition to HSPD-12/FIPS 201-1 compliant systems. While the granting of access privileges remains a local business operation decision, it must function in concert with the Federal PIV policy and procedures. The CAC, as a controlled item, shall not be utilized in temporary badge issuance exchanges. Use of a badge (such as an intelligence community badge) as an identifying badge vice an access credential, is not prohibited in restricted areas by FIPS 201-1 or this regulation.

C3.4. EMERGENCY PLANNING

C3.4.1. The DoD Components shall require commanders to plan for increasing vigilance and restricting access at installations during:

C3.4.1.1. National emergencies.

C3.4.1.2. Disasters.

C3.4.1.3. Terrorist threat conditions or increased Force Protection Conditions (see Reference (m) for further information).

C3.4.1.4. Significant criminal activities.

C3.4.1.5. Civil disturbances.

C3.4.1.6. Other contingencies that would seriously affect the ability of installation personnel to perform their mission.

C3.4.2. Planning should include:

C3.4.2.1. Establishing an installation/facility force protection working group that defines coordination and procedures for installation/facility emergency planning;

C3.4.2.2. Coordinating with local, state, Federal, or host-country officials to maintain integrity of restricted access to the installation and reduce the effect on surrounding civilian communities;

C3.4.2.3. Establishing of a system for positive identification of personnel and equipment authorized to enter and exit the installation;

C3.4.2.4. Maintaining adequate physical barriers that will be installed to control access to the installation;

C3.4.2.5. Pre-designating personnel, equipment, and other resources to enforce restricted access and respond to incidents; and

C3.4.2.6. Exercising contingency plans to validate their effectiveness.

C4. CHAPTER 4

SECURITY OF WEAPON SYSTEMS AND PLATFORMS

C4.1. GENERAL

This chapter establishes procedures and responsibilities for security of weapon systems, including platforms, such as armored fighting vehicles, fixed- and rotary-wing aircraft, and ships in port.

C4.2. PROCEDURES

C4.2.1. 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.

C4.2.2. Each DoD Component Head shall issue instructions governing the security of its weapon systems. The priority for security placed on similar systems or platforms within each DoD Component's inventory may vary due to differences in:

C4.2.2.1. Mission.

C4.2.2.2. Location and vulnerability.

C4.2.2.3. Operational readiness.

C4.2.2.4. Value, classification, and replacement costs.

C4.2.3. Before operations, the cognizant 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 resorting to external support from the cognizant DoD Component. The cognizant 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.

C4.2.4. Security considerations for transportation and storage of AA&E (weapons systems) are described in DoD 4500.9R-Part II (Reference (u)). Requirements for securing devices (such as locks and seals) used in transit of AA&E are described in Reference (h).

C5. CHAPTER 5

PROTECTION OF BULK PETROLEUM PRODUCTS

C5.1. GENERAL

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

C5.2. PROCEDURES

C5.2.1. Commanders or Directors of GOGO and GOCO fuel support points, pipeline pumping stations, and piers shall designate and post these facilities as Controlled Areas.

C5.2.2. When this entity is designated as part of the Defense Critical Infrastructure Program, security planning and protection shall be done in accordance with DoD Directive 3020.40 (Reference (v)).

C5.2.3. Access to Controlled Area 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 credentials) based on the considerations in Chapter 3.

C5.2.4. 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.

C5.3. SECURITY PLANNING AND LIAISON

Commanders shall protect their fuel facilities by:

C5.3.1. Establishing liaison and coordinate and exercise 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.

C5.3.2. Establishing liaison with supporting local, State, and Federal law enforcement agencies and host-nation officials; and support agreements, if appropriate.

C6. CHAPTER 6

SECURITY OF COMMUNICATIONS SYSTEMS

C6.1. GENERAL

C6.1.1. 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.

C6.1.2. 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.

C6.2. PROCEDURES

C6.2.1. The protection provided to DoD communication facilities and systems shall be sufficient to maintain 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 that processes, transmits, or receives, telecommunications traffic is deemed as a defense critical infrastructure capability or crucial by the President.

C6.2.2. 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.

C6.2.3. The DoD Component must review the host installation's implementation of physical security measures during inspections, oversight, and staff visits.

C6.2.4. Access shall be controlled at all communications facilities and only authorized personnel shall be allowed to enter. Facilities should be designated and posted as a minimum, a Controlled Area, as directed.

C6.2.5. Depending on regional conditions, commanders should consider locating enough weapons and ammunition at communications facilities to arm designated, on-site personnel. If arms are stored at the facilities, appropriate security measures and procedures shall be employed in accordance with Reference (h).

C6.2.6. Existing essential structures should be hardened against attacks in accordance with the guidance provided in paragraph C.2.5. This includes large antenna support legs, antenna

horns, operations buildings and cable trays. Future construction programs for communications facilities should include appropriate hardening of essential structures.

C6.2.7. When this entity is designated as part of the Defense Critical Infrastructure Program, security planning and concerns shall be done in accordance with Reference (v).

C6.3. RESPONSIBILITIES

C6.3.1. The Heads of the DoD Components shall coordinate with each COCOM to identify critical communications facilities and mobile systems. Communications capabilities deemed as defense critical infrastructure shall be coordinated with the Office of the Assistant Secretary of Defense for Homeland Defense/America's Security Affairs..

C6.3.2. DoD Components shall direct that each designated subordinate commander or facility director develop a security plan for each communications facility and mobile system under their command. The plan shall include emergency security actions and procedures for emergency destruction of sensitive equipment and classified information (Reference (c)). 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.

C6.3.3. 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 inter-Service support agreement. Whether the facilities or mobile systems are located on or off the installation, installation commanders are responsible for security of these assets as part of the host support.

C6.3.4. Operations, maintenance, and communications personnel at the facility or mobile system are the most important factor in security. DoD Components shall implement a training program so 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:

C6.3.4.1. Security procedures and personal protection skills for assigned personnel.

C6.3.4.2. The use of weapons and communications equipment for protecting the facility or mobile system.

C6.3.4.3. Awareness of local threats, postulated threats and Force Protection Conditions.

C6.3.5. Components may issue additional instructions governing security of the communications facilities.

C6.4. MOBILE COMMUNICATIONS SYSTEMS

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

C7. CHAPTER 7

SECURITY OF CONTROLLED INVENTORY ITEMS

C7.1. GENERAL

C7.1.1. This chapter implements security policy and procedures for safeguarding controlled inventory items, including prescribed drugs and controlled substances, as identified in Title 21, Code of Federal Regulation, Parts 1301.71 through 1301.76, (Reference (w)), Public Law 91-513, (Reference (x)) and precious metals.

C7.1.2. DoD materiel assigned a code indicating the security classification and/or security risk or pilferage controls for storage and transportation pursuant to Military Standard 1388-2A, (Reference (y)) shall be afforded special attention, as in DoD Regulation 4145.19-R-1, (Reference (z)). Controlled Inventory Item Codes (CIIC) are found in DLA Joint Regulation 4145.11, (Reference (aa)).

C7.2. PROCEDURES

C7.2.1. 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 maintain their protection and integrity.

C7.2.2. 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.

C7.2.3. 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.

C7.3. RESPONSIBILITIES

C7.3.1. The Heads of the DoD Components shall:

C7.3.1.1. Establish physical security measures to protect inventory items at depot, base, and installation level.

C7.3.1.2. Monitor the effective implementation of security requirements through scheduled inspections of and staff or oversight visits to affected activities.

C7.3.1.3. Provide that adequate safety and health considerations are incorporated into the construction of a security area for controlled inventory items.

C7.3.2. Establish functioning security measures to reduce the incentive and opportunity for theft.

C7.4. CONTROLLED ITEMS SECURITY

C7.4.1. Commanders will provide storage facilities and procedures for operations to adequately safeguard controlled inventory items.

C7.4.2. Security requirements for inventory items in storage:

C7.4.2.1. General security requirements for classified, sensitive, and pilferable items are found in Reference (x).

C7.4.2.2. Specialized storage requirements for arms, ammunition, and explosives are found in Reference (h).

C7.4.2.3. Additional guidance for the secure storage of sensitive inventory items, controlled substances, and pilferable items are found in Reference (aa).