Army Regulation 190–13

Military Police

The Army Physical Security Program

Headquarters
Department of the Army
Washington, DC
30 September 1993

Unclassified

SUMMARY of CHANGE

AR 190–13
The Army Physical Security Program

This revision-

- Consolidates AR 190-13 and AR 15-15, Department of the Army Physical Security Review Board (DAPSRB), and incorporates policy on the purpose, function, composition of the DAPSRB (chap 7).

- Addresses command responsibility for a crime prevention program (para 2-2).

- Revises DA Form 4261 and DA Form 4261-1 (Physical Security Inspector Identification Card) (paras 3-1 and 3-2).

- Redesignates site surveys as security engineering surveys. Modifies Physical Security Equipment Management Program objectives (para 2-14).

- Identifies the establishment, purpose, functions, and composition of the Department of the Army (DA) Physical Security Equipment Action Group (PSEAG) (para 4-4).

- Redesignates the Product Manager for Physical Security Equipment (PM-PSE) to the Physical Security Equipment Manager, Physical Security Equipment Management Office (PSEMO) (para 4-5).

- Adds an outline of the establishment and specific functions of the Physical Security Equipment Working Group (para 4-6).

- Addresses intrusion detection systems (IDS) by: revising the priority for installation of IDS based on the level of security needed (para 4-9); discussing planning for IDS (para 4-15); establishing new priorities and priority codes for the IDS (table 4-1).

- Outlines security force procedures, inspections, and security patrol plans (chap 8).

- Authorizes exact replication of any Department of the Army and Department of Defense forms that are prescribed in this regulation and are generated by the automated Military Police Management Information System in place of the official printed version of the forms (app A).

Headquarters
Department of the Army
Washington, DC
30 September 1993

*Army Regulation 190–13

Effective 30 October 1993

Military Police

The Army Physical Security Program

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

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

History. This UPDATE printing publishes a revision of this publication. Because the structure of the entire revised text has been reorganized, no attempt has been made to highlight changes from the earlier regulation dated 20 June 1985.

Summary. This regulation implements DOD 5200.8–R, Physical Security Program, and DODD 3224.3, Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support and consolidates two regulations pertaining to physical security: AR 190–13 and AR 15–5. It prescribes policies, procedures, and guidance to plan and implement the Department of the Army Physical Security Program, to include the functions and membership of the Department of the Army Physical Security Review Board, and the Department of the Army Physical Security Equipment Action Group. It provides general guidance concerning requirements for and use of physical security equipment; the appointment of physical security officers and inspectors; physical security credentials, identification cards and badges; restricted areas; and security forces.

Applicability. This regulation applies to all units of the Active Army, the Army National Guard, the U.S. Army Reserve, and the Reserve Officers' Training Corps when in Federal Service that control, move, store, maintain, or secure Army materiel, equipment, and personal property unless exempted by other regulations. This publication applies during partial and full mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Operations and Plans. The Deputy Chief of Staff for Operations and Plans has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The Deputy Chief of Staff for Operations and Plans may delegate this authority in writing to a division chief within the proponent agency who holds a grade of colonel or the civilian equivalent. The approval authority will coordinate all questions regarding the scope of authority to approve exceptions with HQDA(DAJA–AL), WASH, DC 20310–0200.

Army management control process. This regulation is subject to the requirements of AR 11–2. It contains internal control provisions, but does not contain a checklist for conducting internal control reviews. This checklist is contained in DA Circular 11–89–2.

Supplementation. Supplementation of this regulation and establishment of command and local forms is prohibited without prior approval from HQDA(DAMO–ODL–S), 400 ARMY PENTAGON, WASH, DC 20310–0400.

Interim changes. 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. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA(DAMO–ODL–S), 400 ARMY PENTAGON, WASH, DC 20310–0400.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12–09–E, block 2568, intended for command levels A, B, C, D, and E for the Active Army and Army National Guard and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 15–15, 8 February 1977, and AR 190–13, 20 June 1985.

Unclassified

Chapter 1
General

Section I
Introduction

1–1. Purpose
This regulation prescribes policy and assigns responsibility for developing and maintaining practical, economical, and effective physical security programs.

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the consolidated glossary at the end of this Update.

Section II
Responsibilities

1–4. Assistant Secretary of the Army (Installations, Logistics and Environment) (ASA(I,L&E))
The ASA(I,L&E) is responsible for overall physical security policy based on an analysis of the mission of the Army, and known or anticipated requirements and threats. The Department of the Army Physical Security Review Board (DAPSRB) will report to the ASA(I,L&E) through the Deputy Chief of Staff for Operations (DCSOPS).

1–5. Assistant Secretary of the Army (Research, Development, and Acquisition) (ASA(RDA))
The ASA(RDA) is the Army Acquisition Executive and the Senior Procurement Officer within the Department of the Army responsible for administering Army RDA programs in accordance with policies and guidelines. For physical security equipment (PSE), these responsibilities are delegated to the Army Executive Agent for PSE who will be provided by the Commanding General (CG), U.S. Army Materiel Command (AMC), per paragraph 1–18.

1–6. Deputy Chief of Staff for Operations and Plans (DCSOPS)
The DCSOPS will—

a. Provide overall staff responsibility for the physical security of the Army. Develop and coordinate plans pertaining to force protection that allow military forces to counter threats to Army security.

b. Under the DCSOPS, the Chief, Security, Force Protection, and Law Enforcement Division (DAMO–ODL) will—

(1) Approve physical security policy for DCSOPS.

(2) Develop policies, programs, goals, and objectives for the Army Physical Security Program.

(3) Ensure the integration of physical security into Army Operations Security (OPSEC) Programs per AR 530–1.

(4) Ensure physical security requirements are identified in the developmental stages of new equipment and new construction in coordination with the U.S. Army Training and Doctrine Command (TRADOC), the U.S. Army Corps of Engineers (USACE), and AMC.

(5) Program and budget funds for Other Procurement, Army (OPA), Operations and Maintenance, Army (OMA), Operation and Maintenance, Army Reserve (OMAR) as related to physical security.

(6) Chair the DAPSRB per paragraph 7–3.

(7) Provide one voting member (lieutenant colonel, major, or civilian equivalent) to the Army Physical Security Equipment Action Group (APSEAG) per paragraph 4–5.

(8) Coordinate with the Army Staff (ARSTAF) and major Army commands (MACOMs) to establish policies, procedures, and standards pertaining to physical security.

(9) When funding shortfalls exist, establish priorities for the distribution of funds for the procurement of PSE, such as intrusion detection systems (IDS).

(10) Analyze criminal information developed by staff agencies and MACOMs to determine which crimes should be subjects of special crime prevention initiatives.

(11) Ensure integration of physical security with Combating Terrorism Program.

c. Under the DCSOPS, the Chief, Surety and Management Division (DAMO–SWS) will provide one voting member (lieutenant colonel (LTC), major (MAJ), or civilian equivalent) to the APSEAG per paragraph 4–5.

d. Under the DCSOPS, the Commander, U.S. Army Nuclear and Chemical Agency will provide a nonvoting representative to the DAPSRB per paragraph 7–3.

1–7. Deputy Chief of Staff for Logistics (DCSLOG)
The DCSLOG will—

a. Formulate and announce policy for the integrated logistics support (ILS) program for Army programs (AR 700–127) and multi–service programs (AR 700–129).

b. Provide inventory and accountability procedures input into the physical security program for the administrative control of Army property.

c. Provide copies of the survey and inventory adjustments and reports that indicate actual or possible criminal activities to—

(1) ODCSOPS, HQDA(DAMO–ODL–S).

(2) U.S. Army Criminal Investigation Command (USACIDC).

d. Provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

e. Provide one voting member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

1–8. Deputy Chief of Staff for Personnel (DCSPER)
The DCSPER will provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

1–9. Deputy Chief of Staff for Intelligence (DCSINT)
The DCSINT will—

a. Be responsible for all intelligence and counterintelligence aspects of security programs and planning related to protection of Army personnel, materiel, facilities, and operations from espionage, sabotage, criminal subversion, terrorism, and sedition.

b. By fulfilling intelligence and counterintelligence functions outlined in para 1–9a above, identify threats that may increase physical security requirements.

c. Coordinate with HQUSACE to ensure that threat definition is uniform and sufficiently specified to serve as a basis for design.

d. Provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

1–10. The Inspector General
The Inspector General will provide one nonvoting representative to the DAPSRB per paragraph 7–3.

1–11. The Surgeon General
The Surgeon General will provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

1–12. The Auditor General
The Auditor General will provide one nonvoting representative to the DAPSRB per paragraph 7–3.

1–13. Headquarters, USACE
Headquarters, USACE will—

a. Ensure proper planning, evaluation, application, design, installation, and construction of facility enhancements for all aspects of physical security and anti–terrorism related protective construction.

b. Provide criteria and guidance to ensure the proper design, installation, and acceptance testing of all Army and commercial IDS military construction, Army (MCA) projects.

c. Provide the Physical Security Equipment Management Office (PSEMO) (formerly the Product Manager, Physical Security Equipment) with information copies of all IDS engineering surveys performed by USACE. Inform the PSEMO if site designs require the use of nonstandard equipment.

d. Develop and maintain guidance and criteria documents, and provide training for planning, evaluation, application, design, installation, and construction of projects requiring physical security and anti–terrorism related protective construction and equipment.

e. Develop requirements and execute programs for research and development efforts supporting physical security and anti–terrorism related protective construction, and PSE applications.

f. Identify problem areas that impact on the design and installation of IDS and other PSE.

g. Maintain centers of expertise for protective design and for IDS to provide assistance to all Army elements on a reimbursable basis in physical security and IDS, respectively.

h. Coordinate security engineering surveys with MACOM provost marshals (PMs).

i. Be responsible for additional specific procedural tasks per paragraphs 4–4 and 4–7.

j. Provide one voting member (lieutenant colonel, major, or civilian equivalent) to the APSEAG per paragraph 4–5.

k. Under the HQUSACE—

(1) The Commander, USACE, Omaha District, will provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

(2) The Commander, USACE, Huntsville Division, will provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

1–14. Chief of Engineers (COE)

The COE will—

a. Assure physical security design criteria are considered for proposed MCA projects in compliance with Army military construction policy.

b. Maintain an overview of the physical security design program and activities pertaining thereto.

c. Provide administrative and technical advice and assistance and make recommendations on physical security construction matters to the ASA(I,L&E) and HQDA Staff Agencies.

d. Provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

1–15. The Chief, Army Reserve

The Chief, Army Reserve, will—

a. Provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

b. Provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

1–16. The Chief, National Guard Bureau

The Chief, National Guard Bureau, will—

a. Provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB, per paragraph 7–3.

b. Provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

1–17. The CG, TRADOC

The CG, TRADOC, is principal Army combat developer, doctrine developer, trainer, and user representative. In this capacity, when research and development of PSE is required, the CG, TRADOC, will—

a. Formulate concepts, doctrine, organizational structure, materiel objectives, and requirements to employ U.S. Army forces—

(1) In a theater of operations.

(2) In control of civil disturbances.

(3) To secure garrisons.

(4) To combat terrorism.

b. Develop physical security concepts and determine the actions necessary to implement these concepts (doctrine, training, organization, and materiel). Establish an operational tester for all Army IDS and other PSE.

c. Provide training and doctrine support in developing physical security procedures and measures.

d. Comply with AR 71–9 by ensuring the materiel, training, personnel, logistics, doctrine, tactics, and essential–related system requirements for an item of PSE are, throughout the materiel acquisition process—

(1) Identified.

(2) Integrated early.

(3) Tested.

(4) Refined.

e. Ensure the requirements in para 1–17d above are included in—

(1) Requirements documents.

(2) Development contracts.

(3) Tests.

(4) Evaluations.

(5) Other key actions in the acquisition of materiel systems.

f. Determine future Army user requirements for PSE.

g. Ensure, in conjunction with CG, AMC, and as an integral part of the combat development process, that physical security requirements and related subsystems, measures, and procedures are identified in the developmental process for new materiel systems.

h. Evaluate physical security information (directives, ideas, concepts, requested for assistance) that flow to HQ, TRADOC from many sources, to include HQDA, other services, other commands, and individuals.

i. In conjunction with the user representative for specified physical security requirements—

(1) Develop operational concepts and plans designed to improve the physical security posture of the Army; and, when appropriate, to implement physical security policy as established by HQDA(DAMO–ODL).

(2) Determine PSE research, development, test, and evaluation (RDT&E) requirements designed to correct for deficiencies; implement approved physical security operational concepts and plans.

(3) Coordinate with other MACOMs to identify requirements for PSE; coordinate the preparation and staffing within the Army of requirements documents.

j. Designate a representative (MAJ or higher rank officer or civilian equivalent) to the DOD Joint Requirements Working Group (JRWG).

k. Provide one voting member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

l. Under TRADOC, require the Commandant, U.S. Army Military Police School (USAMPS), to provide one nonvoting representative to the DAPSRB per paragraph 7–3.

1–18. CG, AMC

The CG, AMC, is responsible for providing an Army Executive Agent for PSE who will be the Army single point of contact and central manager for planning, acquisition, deployment, installation, and support of PSE, including conventional, nuclear, and chemical. AMC will require—

a. The Army Executive Agent for PSE to —

(1) Provide DA representation (general officer, or civilian equivalent) to the DOD PSE Steering Group.

(2) Provide one voting member (colonel (COL), LTC, or civilian equivalent) representing DA to the DOD Physical Security Equipment Action Group (PSEAG).

(3) Provide a chairman (COL, LTC, or civilian equivalent) to preside over the APSEAG.

b. The Project Manager for Nuclear Munitions (PM NUC) to provide one voting member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

c. The CG, U.S. Army Armament Research, Development and Engineering Center (ARDEC), to provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

d. The Director, Intelligence Materiel Activity (IMA), to provide

one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

e. The CG, U.S. Army Aviation and Troop Command (ATCOM), as the supplier of Army developed interior IDS components, to—

(1) Function as the materiel developer and readiness activity for physical security requirements as validated by the combat developer.

(2) Provide funding for MACOM–approved requirements for commercial IDS (interior or exterior).

(3) Provide funding for MACOM–approved requests for military standard IDS components.

(4) Provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

f. The PSEMO to—

(1) Practice centralized RDA management of PSE for Army use, and for PSE developed by the Army for joint–Service applications in accordance with the assignment of responsibilities defined in DOD Directive 3224.3. (See appendix B.)

(2) Conduct market investigations and market surveys to assess the ability of commercial products or nondevelopmental items (NDI) to meet Army user requirements for PSE.

(3) Develop and acquire physical security systems in accordance with thresholds and requirements described in applicable or DA documents.

(4) Develop and manage an overall ILS program for all assigned PSE programs and systems.

(5) Ensure manpower and personnel integration is a primary concern in system design development.

(6) Manage research, development, testing and evaluation (RDT&E) projects and assigned tasks, product assurance, procurement appropriations, materiel, readiness management functions, and other programs and tasks as assigned.

(7) Monitor, through testing and field validation, the PSE system reliability, availability, maintainability, and durability to ensure requirements are met and maintained throughout production and field operations.

(8) Ensure hazards associated with the design, production, test, operation, maintenance, servicing, support and disposal of the system are identified and resolved through the application of system safety management and engineering.

(9) Maintain the Proof–of–Principle (6.3), and Production Prove–Out (6.4) budget for PSE items satisfying validated Army and multi–Service requirements.

(10) Manage other program funds (OMA, OPA, and Stock Fund) supplied to the PSEMO to support assigned PSE projects, and manage funds from other Federal agencies, as appropriate.

(11) Assist TRADOC with concept formulation plans as they pertain to PSE: developing cost, schedule, and logistical data, as required, to support Cost and Operational Effectiveness/Abbreviated Analyses.

(12) Serve as the Army PSE RDA focal point under the overall management oversight of the Army Executive Agent for PSE, and as delineated in Directive 3224.3 (see app B), receive and evaluate Navy, Air Force, and other Agency life cycle requirements for inclusion in assigned programs.

(13) Serve as the Army representative to the Joint Service Security Equipment Integration Working Group (SEIWG), and act as an observer to the PSEAG, the Joint Service Requirements Working Group (JRWG), and the Joint Test Advisory Group (JTAG).

(14) Provide one voting member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5 and chair the Physical Security Equipment Working Group (PSEWG).

(15) Provide one voting member (LTC, MAJ, or civilian equivalent) to the DAPSRB per paragraph 7–3.

(16) Be responsible for additional specific procedural tasks per paragraphs 4–4 and 4–7.

(17) Establish a repository of information on system security engineering, and provide assistance to weapon system developers on security enhancement techniques and methodologies.

(18) Establish a PSE technical data base. Publish, update at least annually, and distribute to MACOMs and other PSE users a DA Pamphlet detailing Army standard PSE and their application.

g. Under ATCOM, the Commander, Belvoir Research, Development, and Engineering Center (BRDEC), to provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

1–19. CG, U.S. Army Information Systems Command (USAISC)

The CG, USAISC, upon request, will—

a. Provide support in the design, acquisition, installation, operation, and maintenance of communications to support the Army Physical Security Program on a reimbursable basis.

b. Approve and implement the necessary telecommunications requirement (including telecommunications for the installation of IDS) per AR 10–13 and AR 25–1.

1–20. Directors and supervisors of HQDA Staff agencies, commanders of field operating agencies (FOAs) not on military installations, and commanders of USAR and ARNG facilities

These commanders are responsible for physical security within their activities. Applicable portions of paragraph 1–22 below apply.

1–21. Commanders of major Army commands (MACOMs)

These commanders will—

a. Appoint a command physical security officer who will determine command–wide physical security needs.

b. Establish a Physical Security Program to plan, formulate, and coordinate physical security matters; ensure practical, effective, and common sense measures are used.

c. Identify resource needs for meeting physical security requirements.

d. Review for content and accuracy the threat statements prepared by subordinate installations and activities.

e. Identify PSE performance requirements, and coordinate these requirements with the PSE user representative (TRADOC) and the PSEMO.

f. Ensure engineers and physical security personnel coordinate in the formulation of design criteria for new construction projects, and that physical security personnel review all planning documents, plans, and specifications at every step of the planning, design, and construction process.

g. Ensure Army forces deploying to overseas areas designate personnel to carry out physical security responsibilities to safeguard Government personnel, facilities, equipment, operations, and materiel against hostile intelligence, terrorists, other criminal, dissident, or other disruptive activity.

h. Ensure the procedures outlined in paragraph 4–7 are followed in the issue, purchase, lease, or lease renewal of PSE.

i. Be responsible for additional specific procedural tasks per paragraphs 4–4 and 4–7.

j. Support TRADOC in the preparation and coordination of requirements documents.

k. Provide one advisory member (LTC, MAJ, or civilian equivalent) to the APSEAG per paragraph 4–5.

1–22. The military commander in the chain of command

The commander immediately above installations or activities (see para 1–23 below) will issue regulations and orders pertaining to an installation or activity not headed by a military commander under the authority of the Internal Security Act of 1950. (see app C.)

1–23. Commanders of installation or activities

See AR 310–25 for definition of installation and AR 600–20 for a discussion of the selection of an installation commander.

a. Those commanders who are subject to jurisdiction or administration, or in the custody of Defense agencies or separate operating activities, will issue the necessary regulations to protect and secure personnel, places, and property under their command, per the Internal Security Act of 1950.

b. Commanding officers of designated representations, posts, camps, stations, or installations subject to DA jurisdiction or administration, or in DA custody, will also issue the necessary regulations to protect and secure personnel places and property under their command, per the Internal Security Act of 1950. They will—

(1) Appoint, in writing, an installation physical security officer who will report through channels to the commander or deputy commander on all matters related to physical security.

(2) Develop an installation local security threat statement in coordination with local intelligence and law enforcement support elements, based on DA and MACOM threat statements.

(3) Develop an installation physical security plan.

(4) Ensure physical security is included as part of the OPSEC annex in all applicable orders and plans (see AR 530–1).

(5) Ensure supporting military intelligence elements are given all the data relating to the organization and its activities needed to support the force protection mission.

(6) Ensure the passing of threat information to all military activities on/off the installation.

(7) Designate and approve restricted areas per paragraph 6–3.

(8) Provide physical security support to tenant activities per AR 37–49 and AR 210–10.

(9) Ensure security programs provide for safeguarding of personnel, facilities, equipment, operations, and materiel during mobilization and war.

(10) Designate, in writing, mission essential or vulnerable areas (MEVAs) under their control.

(11) Ensure all MEVAs under their control requiring inspection are inspected per paragraph 2–10.

(12) Ensure risk analyses are performed in accordance with DA Pam 190–51 for all facilities (new and existing) either designated or likely to be designated as MEVAs.

(13) Ensure engineers and physical security personnel coordinate in the formulation of design criteria for new construction projects, and that physical security personnel review all plans and specifications at every step of the planning, design, and construction process.

c. The commander shall consider appointing, in writing, a physical security council, to assist the commander and the security officer in discharging their security duties.

1–24. Commanders of host and tenant activities

These commanders are responsible for physical security within their activities as follows:

a. The tenant commander will—

(1) Request physical security requirements or enhancements beyond his or her means from the host commander.

(2) Inform the host commander of all physical security measures in effect.

(3) Defer to the authority of the installation commander on the issue of supplements to this regulation.

(4) Designate their MEVAs in writing, and forward this listing to the installation commander for inclusion in the installation physical security plan.

(5) Forward a copy of their physical security plan to the installation commander, to be included as an annex to the installation physical security plan.

b. Host commanders will provide support to tenant activities in the areas below, unless otherwise mutually agreed in writing.

(1) Law enforcement patrols and security guards, as required to protect personnel and government assets.

(2) Installation and maintenance of Army IDS and other PSE.

(3) Monitoring and response to electronic security equipment when not within the tenant activity's capability.

(4) Minimum essential physical security support (to include installation of IDS when required) to those nonappropriated fund (NAF) income–producing tenant activities (for example, clubs and post exchanges) per NAF regulations.

(5) Inspections of tenant activities, and providing tenant commanders with copies of the inspection reports.

(6) Support tenant commanders' annual physical security training programs.

1–25. The PM or physical security officer

The PM or physical security officer will—

a. Recommend to the commander those installation activities that require special physical security considerations because of their mission essential or critical status and vulnerability to—

(1) Hostile intelligence activities.

(2) Terrorist acts.

(3) Criminal acts.

(4) Dissidence.

(5) Other disruptive influences.

b. Assess installation physical security needs by conducting physical security surveys and inspections per paragraphs 2–9 and 2–10.

c. Recommend physical security considerations in the preparation of installation engineer construction projects, including the design phase. Ensure security considerations are included in new construction, renovation, modification efforts, or lease acquisition.

d. Serve as the installation's single point of contact (POC) for PSE for units under control of and within the AR 5–9 area of responsibility of the installation commander. Ensure coordination of equipment requirements with user, facility engineer, logistics, and communication personnel.

e. In coordination with local intelligence and law enforcement support elements, develop the installation threat statement.

f. Monitor resource management (dollars and personnel) of the installation physical security program. In coordination with the comptroller, plan and program necessary resources for physical security projects in the program budget cycle.

g. Monitor appropriate funding status of all physical security program resource requirements.

h. Coordinate physical security efforts with the organization OPSEC Officer and terrorism counteraction (TC/A) POC.

i. Coordinate with the installation engineer during the planning, design, and construction of all construction projects to identify physical security and anti–terrorism requirements, and to ensure that such requirements are incorporated into the projects at the inception of the project planning.

j. Review planning documents and construction plans and specifications for construction projects at all stages of their development.

1–26. Installation engineer or master planner

The installation engineer or master planner will—

a. Coordinate with the PM or physical security officer during the planning, design, and construction of all construction projects to ensure that physical security requirements are incorporated into the projects at the inception of the project planning.

b. Coordinate the review of all planning documents and construction plans and specifications at all stages of their development with the PM or physical security officer.

1–27. Exemptions

Physical security requirements for nuclear and certain special intelligence activities, cryptological facilities, and all evidence depositories are included in other regulations and are exempt from this regulation unless otherwise specified in those regulations. Upon declaration of war, commanders may suspend specific provisions of this regulation to account for local conditions, while ensuring maximum security for Government personnel and property. The authority to suspend this regulation is granted to installation, division, and separate brigade commanders, and may be further delegated to commanders in the rank of lieutenant colonel.

Chapter 2
Department of the Army Physical Security Program

2–1. General

The DA Physical Security Program is a component of the force protection program. This chapter—

a. Describes the systematic approach that is the basis for the design of physical security programs to ensure protection of all DA assets on the installations and other locations occupied by DA elements.

b. Includes responsibilities outlined in AR 5–9.

c. Includes the requirements for physical security threat assessments, installation physical security plans, and physical security surveys and inspections.

2–2. Crime prevention

a. Crime prevention is a command responsibility. A successful program needs continuing command emphasis; criminal activity should not be allowed to detract from mission accomplishment.

b. An effective crime prevention program will help maximize the security of a military community in peace and war. Its goals are similar to (and support those of) the installation physical security and operational security (OPSEC) programs. Methods used to identify and analyze crime problems complement each other.

c. A crime prevention program is designed to reduce crime by—

(1) Stimulating appropriate crime prevention attitudes, procedures, and behavior.

(2) Protecting potential victims or property from criminal acts by anticipating crime possibilities and eliminating or reducing opportunities for the acts to occur.

(3) Discouraging potential offenders from committing criminal acts.

2–3. Physical security program design

Installation physical security programs shall be designed to—

a. Ensure effective and efficient use of resources.

b. Meet the needs of the installation during peacetime to protect against the traditional criminal, terrorist, and hostile intelligence operations.

c. Expand to allow for security measures that will include plans for security of the installation to permit the rapid marshaling and deployment of forces and materiel during mobilization, and in times of national emergency or war.

2–4. Physical security program factor assessment

To determine the type and extent of the commitment of resources toward installation physical security programs, commanders must assess those factors that will influence their program. The following should be taken into consideration—

a. The importance of the mission to the Army and installation.

b. The local threat assessment (per paras 2–8 and 2–9).

c. The definition and analysis of the area to be protected including—

(1) The nature and arrangement of the activity.

(2) The number of personnel involved.

(3) The monetary, tactical, or strategic value of materiel located in the protected area.

(4) The storage of classified information and equipment.

(5) Other security considerations, such as existing natural or man–made hazards.

d. When the protected area is designated as a MEVA. MEVAs consist of information, equipment, property, and facilities recommended by the PM and approved by the installation commander as requiring additional protection through application of increased physical security measures, procedures, and equipment.

(1) A facility or area will be designated as a MEVA if it is—

(a) Essential to the accomplishment of the installation or organization mission.

(b) Vulnerable to a threat that is intent on destroying, damaging, or tampering with property or equipment, including terrorism.

(c) Vulnerable to a threat that is intent on removing protected items of equipment or property.

(2) A risk analysis per DA Pam 190–51 will be conducted for each MEVA.

(a) The risk analysis will be conducted by the PM with the assistance of the personnel assigned to the unit or activity.

(b) The PM will rank the MEVAs according to the results of the risk analyses, which include existing physical security measures and procedures.

(3) All MEVAs must be inspected.

(4) Example of activities that should be considered for designation as MEVAs are listed below. The installation commander will approve those to be designated as MEVAs.

(a) Ammunition and explosive storage rooms, facilities, or areas.

(b) Arms storage or manufacturing, rebuilding, or demilitarizing facilities and areas.

(c) Airfields, aircraft parking, or aircraft maintenance areas.

(d) Classified sites or locations.

(e) Command posts (main and alternate).

(f) Communications facilities.

(g) Consolidated supply and storage operations.

(h) Controlled drug narcotic vaults or storage areas.

(i) Major data processing facilities.

(j) Field maintenance shops.

(k) Finance offices.

(l) IDS monitor stations.

(m) Motor pools and maintenance activities.

(n) Petroleum, oil, lubricants (POL) storage and dispensing points.

(o) Power supply transmission facilities (alternate and primary).

(p) Water sources.

(q) Medical (Note R) storage areas.

e. The political, economic, legal, terrain, weather, and threat climate.

f. The cost and availability of resources being protected, including the personnel, materiel, equipment, and funds needed to provide minimum protection.

g. The status of the installation, including the possible expansion, relocation, and other changes in operation, to include mobilization and transition to war.

2–5. Physical security planning considerations

The requirements below will be considered when developing physical security plans.

a. During peacetime, the planning for mobilization and war, as well as for current and contingency operations, must be accomplished. Physical security requirements will be integrated into all plans to ensure conservation of physical security resources and effective protection of personnel, facilities, and equipment within Army responsibility.

b. Peacetime planning considerations will be evaluated to permit adjustments in physical security as the threat changes during mobilization and war. Physical security planning will be tied to the defense readiness condition system and the terrorist threat conditions (see AR 190–16 appendix B and AR 525–13) so that as the threat intensifies and readiness increases, equivalent levels of physical security measures and procedures are added.

c. Tactical defense plans will be developed for each installation or activity, to include support installations and key facilities.

d. A plan to control the access to roads that enter and exit the installation will be established. Road closure and restriction plans will be coordinated with local and state law enforcement agencies. Contingency road closings will be included in the installation physical security plan. The plan will also include restricting movement within specific areas of the installation, as required. (See AR 210–10 for a discussion on the control of installation entry and exit.)

e. During unit training and operations that require security precautions, the application of physical security procedures should be tested to protect against—

(1) Hostile intelligence gathering operations (for example, satellites, offshore monitoring, human intelligence (HUMINT)).

(2) Paramilitary forces.
(3) Terrorists or saboteurs.
(4) Traditional criminal elements.
(5) Protest groups.
(6) Disaffected persons.

f. Installations or organizations that expand upon mobilization must identify buildings and facilities to be assigned to expanded activities (for example, hospital wards, USAR schools, logistics warehouses). Once the mobilization assignment has been made, buildings and facilities should be evaluated for physical security requirements. Within the means of the installations, reasonable efforts should be made to correct identified physical security deficiencies.

2–6. Coordination

a. In developing a security plan, coordination and close liaison should be effected between the military commander and—

(1) Adjacent installations or units.
(2) Federal agencies.
(3) State and local agencies.
(4) Similar host country agencies.

b. To the extent permissible, such interaction should allow for an exchange of intelligence, information on security measures being employed, contingency plans, and any other information to enhance local security.

c. On an installation, the host activity shall assume responsibility for coordinating physical security efforts of all tenants, regardless of the components represented, as outlined in the support agreements and the host activity security plan. Applicable provisions shall be included in, or be an appendix to, the support agreement. A formal agreement will contain definite assignment of physical security responsibility for the items stored. The agreement should address—

(1) Maximum quantities to be stored.
(2) Physical safeguards to be used.
(3) Frequency of, and responsibility for, physical inventories or reconciliation's.
(4) Reporting of losses for investigation.
(5) Lock and key control.
(6) Unit that has overall responsibility for the storage facility.
(7) Procedures for authorization and identification of individuals to receipt for, and physically take custody of, Army property.

d. The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and avoids duplication of effort.

2–7. Contingency plans

In most instances it will be necessary to increase security for arms, ammunition and explosives (AA&E) and other sensitive property, and assets and facilities during periods of natural disasters, natural emergencies, or periods of increased threat from terrorist or criminal elements. Therefore, contingency plans should include provisions for increasing the physical security measures and procedures based on the local commander's assessment of the situation. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.

2–8. Security threat assessment

a. Installations will develop a local threat statement. This statement will identify local threats, and make full use of the investigative resources available in the geographic area to anticipate criminal and intelligence activities that threaten the physical security of Army property and personnel. At a minimum, liaison shall be established with the following agencies:

(1) Local Federal Bureau of Investigation (FBI) field office.
(2) Local law enforcement agencies.
(3) Intelligence and investigative agencies of the uniformed services.
(4) Local Bureau of Alcohol, Tobacco, and Firearms field office.
(5) Host country agencies, where applicable.

b. Installation threat statements will be disseminated to all subordinate and tenant activities. The threat statement will be included in the installation physical security plan (see para 2–9).

2–9. Physical security plan format

The physical security plan per FM 19–30, appendix F, will be used as a guide in developing the installation physical security plan. Annexes to the plan may be separated for operational purposes as required; however, the location of the annexes will be listed in the plan. The physical security plan, including all annexes, shall be exercised at least once every two years in order to evaluate its effectiveness. As a minimum, annexes to the plan will include—

a. An installation threat statement per paragraph 2–8.
b. A terrorism counteraction plan.
c. A bomb threat plan. As a minimum, the bomb threat plan should provide guidance for—

(1) Control of operation.
(2) Evacuation.
(3) Search.
(4) Finding the bomb or suspected bomb.
(5) Disposal.
(6) Detonation and damage control.
(7) Control of publicity.
(8) After–action report.

d. An installation closure plan per paragraph 2–5*d*.
e. A natural disaster plan. This plan will be coordinated with natural disaster plans of local jurisdictions. At a minimum, the natural disaster plan should provide guidance for—

(1) Control of operation.
(2) Evacuation.
(3) Communication.
(4) Control of publicity.
(5) Physical security.
(6) After–action report.

f. A civil disturbance plan. It is the commander's responsibility to formulate a civil disturbance plan based on local threats. (For example, commanders of nuclear facilities should anticipate the need to develop crowd control procedures to handle anti–nuclear demonstrations.)

g. A resource plan to meet minimum essential physical security needs for the installation or activity.

h. A communications plan. This plan is required to establish communications with other federal agencies and local law enforcement agencies to share information about possible threats. The communications plan should address all communication needs for paragraphs b through f above.

i. A list of designated restricted areas in accordance with para 6–3.

j. A list of installation MEVAs.

2–10. DA Form 2806–R (Physical Security Survey Report) (RCSCSGA–1672)

a. DA Form 2806–R (Physical Security Survey Report) is a formal recorded assessment of an installation's physical security program. It should provide the commander an assessment of the overall security posture of the installation, given the threat and mission, and advise the commander on the installation physical security program's strengths and weaknesses. Specific procedures and measures evaluated include—

(1) Threat assessment procedures.
(2) Types of security personnel assigned.
(3) Control of visitors and packages.
(4) Use of PSE.
(5) Identification of critical areas or facilities.

b. Physical security surveys will be conducted—

(1) When an installation is activated.
(2) When no record exists of a prior physical security survey.
(3) Every 3 years.
(4) Exceptions are as follows:

(a) Those installations storing nuclear or chemical munitions will be surveyed every 18 months.

(b) Critically sensitive multiple–customer automated data processing (ADP) service center activities or facilities will be surveyed every 18 months.

(c) Those installations storing conventional AA&E will be surveyed every 24 months.

(d) Highly sensitive, sensitive, or nonsensitive multiple–customer ADP service center activities or facilities will be surveyed every 24 months.

(e) Any facility or activity may be surveyed more frequently at the discretion of MACOM commanders or major subordinate command (MSC) commanders.

c. Physical security surveys should be scheduled early in the fiscal year so that resource requirements can be identified and included in the budget cycle.

d. DA Form 2806–R will be used to record physical security survey findings. DA Form 2806–R may be locally reproduced on 8½ – x 11–inch paper. A copy for reproduction purposes is located at the back of this regulation. Attachments may be added to the form to clarify unique command requirements. Figure 2–1 shows a sample of a completed form.

(1) The survey should—

(a) Provide the commander with an assessment of the security posture of the installation.

(b) State recommended actions for the application of resources in a prioritized manner for the reduction of vulnerabilities.

(c) Include proper exhibits that would assist in clarifying findings and recommendations, and an assessment as to their criticality and vulnerability. Photographs, sketches, graphs, and charts are examples of such exhibits.

(2) The survey, including exhibits, will be forwarded to the installation commander for information and corrective action.

(3) The commander's report of corrective action taken will be retained on file until the next survey is completed.

(4) One copy of the completed installation physical security survey report will be forwarded, through command channels, to the MACOM.

(a) The commander's report of corrective action taken, less exhibits, will be included.

(b) MACOMs will establish follow–up actions to ensure that measures are being taken to correct discrepancies noted in installation survey reports.

(5) In the case of the U.S. Army Europe (USAREUR), the USAREUR MSCs will receive survey reports and oversee follow up actions on those installations under their jurisdiction and control.

e. After completion of the survey, the installation PM or security officer will reassess the installation's physical security posture based on—

(1) A risk analysis per DA Pam 190–51.

(2) Mission.

(3) Potential threat.

(4) Findings of the survey team.

(5) Comparison of findings from previously conducted surveys and inspections.

(6) Areas over or under protected.

f. Using the assessment, a physical security resource plan will be developed recommending the prioritized allocation of resources and the revision of existing measures and procedures, or the development of necessary new measures and procedures. Highest priority will normally be given to activities considered essential or critical to mission accomplishment. This plan will be forwarded to the commander for approval, and will be included in the installation physical security plan.

2–11. DA Form 2806–1–R (Physical Security Inspection Report) (RCSCSGPA–1671)

a. DA Form 2806–1–R (Physical Security Inspection Report) is a formal, recorded assessment of physical security procedures and measures implemented by a unit or activity to protect its assets. Normally, the inspections are limited to those units or activities designated by the commander as MEVAs.

(1) A copy of the evaluation of the resource protection assessment conducted under the provisions of AR 11–2 should be provided to the inspector.

(2) Inspectors shall not engage in illegal or dangerous conduct to demonstrate security deficiencies or weaknesses observed during the inspection.

(3) Inspections may be conducted on an unannounced basis. However, before conducting unannounced inspections, inspectors should review unit training schedules to ensure that inspections do not interfere with training exercises.

b. Physical security inspections will be conducted—

(1) When a MEVA, unit, or activity is activated.

(2) When no record exists of a prior physical security inspection.

(3) When there is a change in the unit or activity that may impact on existing physical security plans, and there is an indication or reported incident of significant or recurring criminal activity.

(4) Every 18 months for nuclear reactor and nuclear and chemical storage units or activities, conventional arms, and ammunition storage activities.

(5) Every 18 months for critically sensitive multiple–customer ADP service center activities or facilities.

(6) Every two years for all other MEVAs.

(7) For other activities, as directed by the local commander.

(8) Every two years for ROTC facilities storing only .22 caliber weapons. The biennial requirement to inspect ROTC facilities storing only .22 caliber weapons is eliminated if facilities are inspected by applicable ROTC region physical security personnel during the annual formal inspection (AFI). ROTC facilities storing only demilitarized weapons do not require an inspection. Demilitarized weapons will be stored and accounted for per AR 710–2.

(9) Every two years for highly sensitive, sensitive, or nonsensitive multiple–customer ADP service center activities or facilities. Inspections of all other ADP activities or facilities, not classified as critically sensitive, will be incorporated into scheduled physical security inspections of the individual activity of facility.

(10) When the commander determines greater frequency is required.

c. Physical security inspectors will be granted access to Army facilities, records, and information on a need–to–know basis, consistent with the inspector's clearance for access to classified defense information and provisions of applicable regulations.

d. DA Form 2806–1–R will be used to prepare all physical security inspections. DA Form 2806–1–R may be locally reproduced on 8 1/2– x 11– inch paper. A copy for reproduction purposes is located at the back of this handbook. Attachments may be added to the form to clarify unique command requirements. Figure 2–2 shows a sample of a completed form.

e. Copies of physical security inspection reports will be provided to the—

(1) Commander of the unit or director of the organization inspected.

(2) Commander or director at the next higher level above the organization inspected.

(3) Installation physical security officer.

f. Findings noted on physical security survey or inspection reports that are beyond the capabilities of the local commander to correct because of a lack of resources, will be reported to the next higher commander with a request for resource assistance.

(1) Findings noted on physical security survey or inspection reports may be used for programming funds and requesting telecommunication work orders.

(2) Submission of work order requests or requests for telecommunications support do not resolve a report finding.

(a) Compensatory measures within available resources will be placed in effect pending completion of work order requests.

(b) Recurring findings will be reported on future physical security inspections until deficiency is corrected.

2–12. Reports of action taken

A report of action taken for both surveys and inspections will be required by the installation commander and attached as an exhibit to

the report. DA Form 2806–1–R will be filed with the survey report. These records will be maintained in the active files of the units or activities inspected, as outlined in 2–11e until the completion of the next physical security inspection, and then destroyed.

2–13. Reports classification

Reports of completed surveys or inspections will be classified and safeguarded per DOD 5200.1–R and AR 380–5, as appropriate.

2–14. Security engineering surveys

A security engineering survey is the process of identifying, by means of an on–site survey, engineering requirements associated with facility enhancements for physical security and anti–terrorism, including IDS installation. Security engineering surveys should be performed when planning any new construction or renovations or upgrades to existing facilities where there are likely to be physical security requirements. Security engineering surveys may also be requested by the PM or equivalent security officer to evaluate existing security.

a. The scope of a security engineering survey is to—

(1) Identify the assets to be protected.

(2) Identify the threats to the assets and the levels of protection to which the assets should be protected against them.

(3) Identify protective measures, including IDS, to reduce the vulnerabilities of the assets to the threats.

(4) Determine the cost of proposed protective measures.

b. As a minimum, the following personnel or their representatives should participate or provide input to the security engineering survey—

(1) Director or Engineering and Housing (DEH) or equivalent installation level engineer, to include the master planner.

(2) PM or equivalent security officer, to include the physical security officer.

(3) Operations officer (G–3/S–3).

(4) Intelligence officer (G–2/S–2).

(5) Facility user.

(6) Logistics officer.

(7) Safety officer.

(8) Communications officer.

c. Security engineering surveys may be performed by the MACOM or by the installation engineer, within local capabilities. Security engineering surveys may also be requested on a reimbursable basis from the USACE (Protective Design and/or Intrusion Detection Systems Mandatory Centers of Expertise) by contacting the Commander, U.S. Army Engineer District, Omaha, ATTN: CEMRO–ED–ST, 215 N. 17th Street, Omaha, NE 68102–4978, in accordance with established MACOM procedures.

M TAB TAB TAB TAB

PHYSICAL SECURITY SURVEY REPORT
For use of this form, see AR 190-13; proponent agency is ODCSOPS

Requirement Control Symbol CSGA-1672

1. REPORT NUMBER
2. DATE(S) OF SURVEY
3. NAME AND LOCATION OF INSTALLATION SURVEYED
4. PREPARING AGENCY
5. NAME AND RANK OF INSTALLATION COMMANDER
6. NAME AND RANK OF PROVOST MARSHAL/SECURITY OFFICER
7. NAME(S) OF SURVEY PERSONNEL *(Grade, Rank, Title, and Organization)*
8. REPORT NUMBER AND DATE OF LAST SURVEY

PART I – INSTALLATION DESCRIPTION

9. INSTALLATION ACREAGE
10. NUMBER OF MILITARY ASSIGNED
11. NUMBER OF CIVILIANS EMPLOYED
12. NUMBER OF TENANT ACTIVITIES
13. NUMBER OF BUILDINGS
14. TYPE INSTALLATION *(Check One)*
____OPEN
____ CLOSED
____LIMITED ACCESS *(Temporary)*
15. INSTALLATION MISSION

16. LIST AREAS CONSIDERED TO BE CRITICAL OR VULNERABLE:

a. CRITICAL OR VULNERABLE AREAS	b. PROTECTION REQUIREMENTS	c. PROJECT IMPLEMENTATION

PART II – PHYSICAL SECURITY PERSONNEL

17. SECTION A – GUARDS

TYPE	AUTH	ASGD
a. MILITARY POLICE		
b. MILITARY (NON-MP)		
c. CONTRACT CIVILIAN GUARDS		
d. DOD CIVILIAN GUARDS		
e. GSA GUARDS		
f. FOREIGN DIRECT HIRE		
g. FOREIGN CONTRACT		
h. OTHER *(Specify)*		
i. TOTAL		

18. SECTION B – PHYSICAL SECURITY INSPECTORS

TYPE	AUTH	ASGD
a. MILITARY		
b. CIVILIAN		

DA FORM 2806-R, Apr 85 EDITION OF MAY 66 IS OBSOLETE

Figure 2-1. Sample of a completed DA Form 2806–R

M TAB TAB TAB

PART III – PHYSICAL SECURITY PLANNING

	YES	NO
19. HAS AN INSTALLATION PHYSICAL SECURITY THREAT STATEMENT BEEN PREPARED?		
20. HAVE SUBORDINATE UNITS OR TENANT ACTIVITIES BEEN PROVIDED A COPY?		
21. IS THERE AN INSTALLATION PHYSICAL SECURITY PLAN?		
a. DOES THE PLAN COVER PHYSICAL SECURITY FOR PEACETIME, MOBILIZATION, AND WARTIME?		
b. DOES THE PLAN INCLUDE ANNEXES FOR COUNTERTERRORISM, BOMB THREATS, ADP PLANS, AND WORK STOPPAGE PLANS AND INSTALLATION CLOSURE?		
22. DOES THE INSTALLATION PHYSICAL SECURITY PROGRAM SUPPORT OPERATIONS SECURITY AND CRIME PREVENTION PROGRAMS?		
23. IS PHYSICAL SECURITY INCLUDED IN INSTALLATION CONTINGENCY AND EXERCISE PLANS?		

24. BRIEFLY EXPLAIN "NO" ANSWERS OF ITEMS 19 THROUGH 23

25. FINDINGS/RECOMMENDATIONS

26. SURVEYING OFFICIAL'S EVALUATION

27. OVERALL EVALUATION OF PHYSICAL SECURITY PROGRAM

____ EXCELLENT ____ GOOD ____ POOR

28a. SURVEY OFFICER *(Name, Grade, Organization)* b. SIGNATURE c. DATE

29a. APPROVING AUTHORITY *(Name, Rank, Title)* b. SIGNATURE d. DATE

30. DISTRIBUTION

31. DATE COMMANDER'S REPORT OF CORRECTIVE ACTION RECEIVED

Page 2, DA Form 2806-R, Apr 85

Figure 2-1. Sample of a completed DA Form 2806–R—Continued

Legend for Figure 2-1:
Completion instructions for DA Form 2806–R

1. Report Number. The command originating the report will develop the report number.

2. Date(s) of survey. Self–explanatory.

3. Name and location of installation surveyed. Self–explanatory.

4. Preparing agency. This entry will include the mailing address of the Commander, Law Enforcement Activity (LEA); Provost Marshal (PM); or security officer preparing the survey.

5. Name of commander. Enter name and rank of installation commander.

6. Name of PM/security officer. Enter name and rank, of commander, LEA; PM, or security officer.

7. Name(s) of survey personnel. Identify those personnel conducting the survey.

8. Report number and date of last survey. Enter only the most recent survey; if unknown, enter the word "unknown."

9. Installation acreage. Self–explanatory.

10. Number of military assigned. Enter the total number of military assigned on the first day of the survey.

11. Number of civilians employed. Enter the total number of civilians employed on the first day of the survey (include U.S. citizens and foreign nationals employed on the installation).

12. Number of tenant activities. Enter those organizations, activities, of units that occupy facilities on the installation, but belong to another command.

13. Number of buildings. Self–explanatory.

14. Type installation. See the consolidated glossary, section II, for definitions of open and closed posts. If the open installation has the capability to temporarily limit access, check that block also.

15. Installation Mission. Enter brief mission statement.

16. Areas considered to be critical or vulnerable. The commander will evaluate these areas based on recommendations from the physical security officer.

a. Critical areas. Identify those areas considered to be critical or vulnerable in order of priority.

b. Protection requirements. Briefly identify those physical security measures needed to adequately secure the areas (for example, IDS, single fence, guards).

c. Project implementation. Identify the programmed date of other descriptive data that shows, when necessary, security improvements projected to be made (for example, FY 93 IDS installation).

17. Guards.

a. Military police (MP). Number of MPs assigned to perform security duties, such as guards at sensitive weapons site.

b. Military (non–MP). Include those unit personnel for interior guard duties.

c. through i. Self–explanatory.

18. Physical security inspectors. Enter the number of personnel who have been issued physical security credentials.

19 through 23. Physical security planning questions. Self–explanatory.

24. If any of the questions in 19—23 are answered NO, briefly explain the reason for the NO answer.

25. Findings and recommendations. Self–explanatory.

a. Those commendable areas, problems, and major deficiencies noted during the survey will be identified.

b. Deficiencies noted from previous surveys that have not been corrected will include the word "recurring" at the end of the deficiency.

c. Deficiencies noted will cite a reference when possible. If no reference is cited, the deficiency will be considered only as an observation.

d. Recommendations should follow each deficiency noted. Recommendations should be realistic and meaningful on what can be done to improve security. They should relate to the reference cited in deficiencies noted, if any.

26. Surveying official's evaluation. Evaluation should include the overall assessment of security on the installation or evaluation should include the overall assessment of security of the unit of activity inspected. Evaluation should also furnish advice needed to improve the physical security measures of the unit/activity to include cost effective measures; for example, requests for exceptions.

27. Overall evaluation of physical security programs. Self–explanatory.

28 through 30. Self–explanatory.

31. Date commander's report of corrective action received. Enter date report received by surveying authority. Report of corrective action taken will be filed with the survey.

M TAB TAB TAB

PHYSICAL SECURITY INSPECTION REPORT
For use of this form, see AR 190-13; proponent agency is ODCSOPS

Requirement Control Symbol
CSGPA-1671

1. REPORT NUMBER

2. DATE OF INSPECTION

3. PREPARING AGENCY

4. UNIT OR ACTIVITY INSPECTED

5. NAME AND RANK OF UNIT/ACTIVITY COMMANDER

6. REPORT NUMBER AND DATE OF PREVIOUS INSPECTION

7. UNIT OR ACTIVITY MISSION

8. TYPE OF AREA INSPECTED

9. TYPE INSPECTION

_____ ANNOUNCED _____ UNANNOUNCED

10. HAS THE UNIT BEEN PROVIDED THE:

	YES	NO	NA
a. INSTALLATION PHYSICAL SECURITY THREAT STATEMENT?			
b. INSTALLATION PHYSICAL SECURITY PLAN?			

11. FINDINGS/RECOMMENDATIONS

12. INSPECTING OFFICIAL'S EVALUATION

13. RATING: THE SECURITY OF THIS UNIT/ACTIVITY IS:

_____ ADEQUATE _____ NOT ADEQUATE

TO PROTECT THE ARMY INTERESTS.

14. EXIT INTERVIEW *(Name, Grade or Rank, and Duty Position)*

15a. INSPECTOR *(Name and Rank)* b. SIGNATURE c. DATE

16a. APPROVING AUTHORITY *(Name, Rank, Title)* b. SIGNATURE c. DATE

17. DISTRIBUTION:

DA FORM 2806-1-R, Apr 85

Figure 2-2. Sample of a completed DA Form 2806–1–R

Legend for Figure 2-2:
Completion instructions for DA Form 2806–1–R

1. Report number. The command originating the report will develop the report number.

2. Date of inspection. Self–explanatory.

3. Preparing agency. This entry will include the mailing address of the Commander, Law Enforcement Activity (LEA); provost marshal (PM); or security officer preparing the survey.

4. Unit or activity inspected. Self–explanatory.

5. Name of unit or activity commander. Enter the name and rank of the commander.

6. Report number and date of previous inspection-. Self–explanatory.

7. Unit or activity mission. Enter a brief mission statement.

8. Type area inspected. State type of activity or activities inspected within the unit (for example, arms rooms, finance offices, or ADP facilities).

9. Type inspection. Self–explanatory.

10. Self–explanatory.

11. Findings and recommendations.

a. Those commendable areas, problems, and major deficiencies noted during the inspection will be identified.

b. Deficiencies noted from the previous inspection that have not been corrected will include the word "recurring" at the end of the deficiency.

c. Deficiencies noted will cite a reference when possible. If no reference is cited, the "deficiency" will be considered only as an observation.

d. Recommendations should follow each deficiency noted. Recommendations should be realistic and meaningful concerning what can be done to improve security and should relate to the reference cited in deficiencies noted, if any.

12. Inspecting official's evaluation. Evaluation should include the overall assessment of security on the installation.

13. Rating. Self–explanatory.

14. Exit interview. Enter name, grade or rank, and duty position of person with whom the exit interview is conducted.

15 through 16. Self–explanatory.

17. Distribution. Self–explanatory.

Chapter 3
Physical Security Personnel and Credentials

3–1. Physical security officers

a. Persons selected as physical security officers will meet one or more of the following requirements:

(1) Demonstrated ability to manage physical security programs through prior experience.

(2) Formal training in military police or physical security operations at least equivalent to the 2–week physical security course offered at USAMPS.

b. Civilians may be appointed as physical security officers per—

(1) AR 690–950.

(2) Civilian Personnel Regulation (CPR) 950–19.

(3) Position Classification Standards for Security Administration Series GS–080–0, published by the U.S. Office of Personnel Management, (OPM), Office of Classification, December 1987.

3–2. Physical security inspectors

Installation physical security inspectors will be selected by the PM; security officer; or Commander, U.S. Disciplinary Barracks (USDB), as appropriate.

a. Military inspectors will be—

(1) Qualified in primary MOS 95B or MOS 95C.

(2) SSG (E6) or above (may be waived to SGT (E5)).

(3) Trained per paragraph 3–2c.

(4) Cleared for access to at least SECRET national defense information.

(5) Free of previous disqualification for reasons per paragraph 3–3b.

(6) Cleared by a favorable Crime Records Center (CRC) name check. The additional skill identifier (ASI) H3 will not be awarded, and physical security inspector credentials will not be issued without a favorable CRC name check. (See para 3–5a for CRC message format.)

(7) In possession of authorized credentials.

b. Civilian employees who are appointed to physical security specialist inspector positions must meet the current OPM GS–080–0 physical security qualification standard for the particular grade assigned to the position. As a minimum, civilians should receive the same or comparable resident training courses specified for military inspectors (see para 3–3c.). These civilians should be cleared for access to SECRET national defense information before being issued physical security inspector credentials, and before conducting physical security inspections and surveys.

c. Military physical security inspectors will complete one of the training requirements below or equivalent. These inspectors must be awarded ASI H3 before being issued physical security inspector credentials per paragraph 3–4. Civilian physical security inspectors will complete one of the training requirements below before receiving physical security inspector credentials.

(1) Successful completion of the physical security course (7H–31D/830–ASI H–3) producing ASI H3, conducted by the USAMPS or through a DOD–approved course of instruction.

(2) Successful completion of a formal course of instruction conducted by a MACOM authorized to award ASI H3, and that meets the standards of the USAMPS course.

3–3. Additional skill identifier for military physical security inspectors

a. An ASI H3 will be awarded only to military police personnel qualified to be physical security inspectors per applicable provisions of AR 611–201 and AR 600–200, as amended, and this regulation. ASI H3 will be awarded only on recommendation of USAMPS; the PM; security officer; or Commander, USDB, concerned.

b. The PM; security officer; or Commander, USDB, will initiate action to withdraw ASI H3, collect credentials, and remove the person concerned from the physical security inspector program on determination that the person is no longer qualified to perform physical security inspector duties. Disqualification or relief from physical security inspector duties may be based on any of the following:

(1) Inefficiency, negligence, delinquency, or misconduct in the performance of duty.

(2) Court–martial, civil convictions of a serious nature, or a pattern of behavior, actions, or breaches of discipline that are reasonably indicative of a contemptuous attitude towards the law or other duly constituted authority.

(3) Any illness or mental condition that, in the opinion of a competent medical authority, may cause significant defect in the judgment or reliability of the person.

(4) Final revocation of a personnel security clearance.

(5) Loss of credentials through neglect.

(6) Failure to achieve a verifying score on the latest Self Development Test (SDT) taken.

(7) Any other conduct that may adversely affect an individual's continued performance of inspection duties.

c. Any inspector will be suspended from physical security inspector duties who—

(1) Is the subject of an unfavorable personnel action.

(2) Has had his or her security clearance suspended.

d. Persons will have the ASI removed from active inventory and placed in an historical file who—

(1) Have not worked in physical security related duties requiring the ASI H3 for a period of 4 years or more.

(2) Have attained the rank of Sergeant Major and will not be assigned to a physical security assignment.

e. Commanders will forward the names of personnel in this category (para d above) to the Commander, PERSCOM, ATTN: DAPC–EPT–F/DAPC–EPL–M, who will remove the ASI and annotate official records. A copy of this action will be furnished to the local military personnel office (MILPO) for inclusion in the soldier's Field 201 File. The local commander may restore ASI H3 to a qualified person at any time in accordance with a above.

3–4. Credentials

a. Overview.

(1) The only authorized credentials for physical security inspectors are DA Form 4261 and DA Form 4261–1 (Physical Security Inspector Identification Card). See figures 3–1 and 3–2 for completed examples of these forms. Reproduction of these credentials or use of locally produced physical security inspector credentials is prohibited.

(2) Physical security inspector credentials are numbered serially with a letter and a 4–digit number. They will be completed with the name, rank or grade, physical description, date of birth, social security number, photograph, and signature of the inspector to whom issued.

(3) DA Form 4261 will be authenticated by the PM; security officer; or Commander, USDB.

(4) After identifying data are entered, credentials will be signed by the inspector, properly authenticated, and then laminated by the issuing authority. Credentials that have not been laminated are not valid.

(5) Credentials will not be altered in any way. Issuing authorities will establish procedures for checking credentials, and will collect and destroy those that have been altered, defaced, or marred.

b. Issue.

(1) Physical security inspector credentials will be issued by serial–numbered lots to major Army commanders. Major Army commanders desiring credentials will submit requirements to HQDA(DAMO–ODL–S), 4401 Ford Avenue, Alexandria, VA 22302–1432.

(2) Major Army commanders will—

(a) Develop accountability procedures for the issue, control, accountability, and destruction of credentials.

(b) Prescribe actions to be taken consistent with this regulation if credentials are lost or misused.

(3) The issuing authority will normally be the PM; security officer; or Commander, USDB.

(4) Credentials will be issued only to physical security inspectors meeting the qualification requirements of paragraph 3–2. Physical security officers may be issued credentials at the discretion of the PM; security officer; or Commander, USDB.

(5) Credentials will be issued for a period not to exceed 48 months from the date of issue. The expiration date will be typed on the line provided on DA Form 4261–1.

c. Withdrawal.

(1) Physical security inspector credentials will be withdrawn for cause per paragraph 3–3b.

(2) An inspector's credentials will be withdrawn upon his/her departure from permanent change of station (PCS), expiration term of service (ETS), or reassignment from physical security programs.

(3) Credentials will be withdrawn temporarily when the inspector is being investigated for criminal or other inappropriate conduct that might result in permanent withdrawal for cause.

(4) Inspectors will turn in credentials to the issuing authority during all authorized absences (for example, leave, hospitalization, or temporary duty (TDY) not associated with inspection duties).

d. Reporting information. Issuing authorities will report the full name, rank, social security number, and credential number of each person to whom physical security inspector credentials are issued or from whom credentials are withdrawn. This information will be reported in writing to the MACOM PM or security officer within 10 days of issue or withdrawal. Withdrawals reported will include a short explanation of the reason for withdrawal.

e. Credentials custodian. A credentials custodian, appointed in writing by PM or Security Officer, will establish and maintain a control log to ensure accountability for the issue, withdrawal, and destruction of credentials.

3–5. Crime Records Center, USACIDC

a. Message format. For the required CRC name check, dispatch an electrical message to DIR USACRC USACIDC BALT MD // CICR–ZA//.

b. Authorization for name check. The installation or activity PM or security officer will authorize the request for a name check.

c. Request. The request will include—

(1) The candidate's full name (to include former names and maiden names if applicable).

(2) Social security number.

(3) Date of birth.

(4) Place of birth.

(5) Primary military occupational specialty or DOD Civil Service job series.

(6) Rank or grade.

(7) General technical aptitude area score (for military).

(8) Expiration term of service (for military).

(9) Security clearance.

(10) Civilian education level.

d. Information addressees. Information addressees will include the applicable MACOM PM or security officer and HQDA (DAPC–EPL–M).

e. Issuance of credentials to military physical security inspector candidates. Physical security inspector candidates will not be issued credentials, programmed to attend a physical security inspector training program, or awarded the additional skill identifier H3 until a favorable name check is received from the CRC.

3–6. Uniforms

a. Military physical security inspectors will wear the duty uniform.

b. The PM or security officer may authorize the wearing of appropriate civilian clothing when official duties require entering a foreign territory where wearing the uniform is prohibited.

c. Civilian clothing allowance is not authorized except when TDY performed exceeds 14 days per AR 700–84.

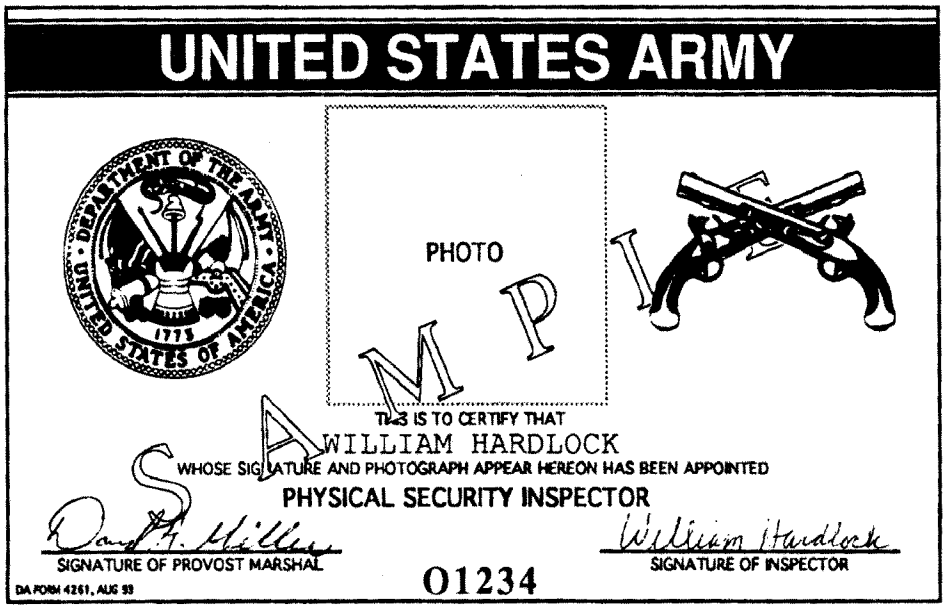

Figure 3-1. Sample of a completed DA Form 4261

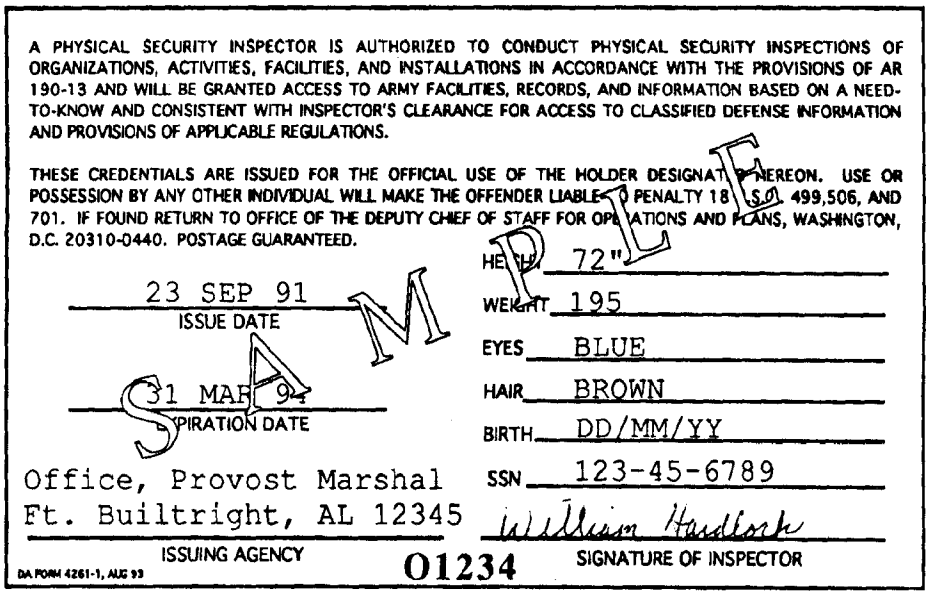

Figure 3-2. Sample of a completed DA Form 4261–1

Chapter 4
Physical Security Equipment

4–1. General
This chapter implements DOD Directive 3224.3 (see appendix B for a reprint of this directive), delineates responsibilities, and provides guidance on the planning, evaluation, approval, and procurement of PSE. This chapter also establishes the APSEAG to accomplish the centralized management of the Army's PSE program.

4–2. DA policy
PSE will be used to ensure protection of DOD resources, including national security information and materiel. MACOMs shall use commercial equipment only if no DOD standardized equipment exists. When there is a need to develop standardized PSE, a statement of need will be forwarded to the TRADOC appointed user representative. Once a component or system is developed by the Army, or adopted from commercial sources, it is considered standardized, and may be adopted by all Services to satisfy joint Service operational requirements.

4–3. Program objectives
The objectives of the PSE program within the Army are to—

a. Comply with the policy guidance set forth in DOD Directive 3224.3, and to fulfill those responsibilities specifically assigned to the Army. These assigned responsibilities include the programming, budgeting, funding, and design and performance criteria development for research and engineering of interior PSE, barriers, lighting systems, interior robotics systems, and command and control systems.

b. Acquire the most effective PSE at reasonable cost.

c. Eliminate duplication of RDT&E efforts among the Services.

d. Initiate research and development projects for PSE only when

there are no DOD standard, evaluated commercial, or NDI products available to satisfy user requirements.

e. Determine the order of priority for research and development, distribution, and installation of IDS and related equipment, in accordance with the Army–wide 5–year master plan.

f. Ensure PSE considerations are incorporated into the planning, development, and support of DOD weapons systems and facilities, as well as new Army materiel systems, per the materiel development process outlined in AR 71–9 and MIL–STD 1785.

g. Incorporate physical security requirements into the design of any system in which security of the system, or of its operating or supporting personnel, is essential to its readiness or survival.

h. Emphasize IDS and PSE are only part of an overall security system, and that they do not stand alone. Proper security depends on a total systems approach which integrates policy, procedures, equipment, protective construction, and awareness.

i. Establish coordination and information exchange between the Army and other DOD agencies to eliminate duplication of effort, and to share information on PSE requirements, test results, technical data, lessons learned, and vulnerabilities in accordance with DOD Directive 3224.3

j. Ensure interoperability, when appropriate, between essential elements of security systems being fielded by the military departments; and the consolidation of testing when possible in accordance with DOD Directive 3224.3.

4–4. Department of the Army Physical Security Equipment Action Group (APSEAG)

a. The APSEAG is established to assist and support the Army Executive Agent for PSE in accomplishing the program objectives listed in paragraph 4–3.

b. The functions of the APSEAG are to—

(1) Provide oversight of Army RDA programs for PSE.

(2) Review and establish priorities for development and procurement of PSE.

(3) Develop, refine, and continually update the Army PSE Master Plan, and provide input to the DOD Physical Security Master Plan.

(4) Ensure the Army PSE development programs and the PSE inventory are continually assessed to assure that they address PSE deficiencies.

(5) Ensure adequate quantities of state–of–the–art PSE are made available through the Army's wholesale supply system to satisfy user requirements.

(6) Influence PSE design, installation, and maintenance policies and procedures to optimize standardization and user satisfaction.

(7) Interface with other Services and DOD concerning PSE matters, and provide representation to the working groups established by DOD Directive 3224.3.

(8) Ensure the Army PSE exploratory development initiatives are incorporated by the Defense Nuclear Agency (DNA) into their PSE exploratory development programs.

(9) Establish a repository of information concerning PSE and system security engineering.

4–5. Composition

The APSEAG will consist of representatives of the following:

a. Chairman: AMC (AMCDE–C). (The Chairman is the Army representative to the DOD PSEAG.)

b. One voting member (lieutenant colonel, major, or civilian equivalent) will be furnished by each of the following:

(1) ODCSOPS (DAMO–OD) or a representative from the Security, Force Protection, and Law Enforcement Division (DAMO–ODL).

(2) ODCSOPS (DAMO–SWS) or a representative from the U.S. Army Nuclear and Chemical Agency.

(3) ODCSLOG (DALO–SMA).

(4) TRADOC (ATCD–SE).

(5) USACE (CEMP–ET).

(6) Project Manager for Nuclear Munitions (AMCPM–NUC–A).

(7) Physical Security Equipment Manager, Physical Security Equipment Management Office (PSEMO), ATCOM (AM–SAT–W–TP).

c. One non–voting, advisory member will be furnished by each of the following:

(1) USACE, Omaha District Center of Expertise for Protective Design.

(2) USACE, Huntsville Center of Expertise for Intrusion Detection Systems (IDS–MCX).

(3) U.S. Army Belvoir Research, Development and Engineering Center (SATBE–JI).

(4) U.S. Army Armament Research, Development and Engineering Center (SMCAR–FSN–M and SMCAR–FSN–T).

(5) USATCOM (AMSAT–I–STG).

(6) Chief, National Guard Bureau (NGB–ARO–OS),

(7) Chief, Army Reserve.

(8) U.S. Army Strategic Defense Command (CSSD–HS–S–P).

(9) Intelligence Materiel Activity (AMXMI–M–D).

(10) PM, U.S. Army Europe and Seventh Army (AEAPM–PS).

(11) PM, AMC (AMCPE–S).

(12) PM, USAISC (ASIS–P).

(13) PM, U.S. Army Intelligence and Security Command (IASEC–FP).

(14) PM, Military Traffic Management Command (MTMC (MTOP–S)).

(15) Commander, USACIDC (CIOP).

(16) PM, Military District of Washington (ANPM–Z).

(17) PM, U.S. Army Health Services Command (HSPM).

(18) PM, Forces Command (FCPM–SM).

(19) PM, TRADOC (ATBO–JP).

(20) PM, U.S. Army Pacific (APPM).

(21) PM, USACE (CEPM–ZB).

(22) PM, U.S. Military Academy (MAPM).

(23) Representatives from other Army Staff agencies or MACOMs who request to attend, or who are invited by the chairman to act as advisors to the APSEAG when items affecting their agencies or commands are to be discussed.

4–6. Physical Security Equipment Working Group (PSEWG)

The PSEWG is established to assist the APSEAG in the accomplishment of its objectives.

a. Specific functions of the PSEWG are to—

(1) Review and continually update the Army 6.2 PSE priority listings.

(2) Review and recommend changes to the Army 6.3/6.4 PSE RDTE&E programs.

(3) Review commercial and government PSE proposals of potential interest to the Army.

(4) Provide input to the Department of the Army Physical Security Master Plan.

(5) Interface with other Services and DOD concerning PSE matters.

(6) Accomplish other PSE related tasks, as directed.

b. The PSE Manager will chair the PSEWG. The membership of the PSEWG will consist of selected representatives of the APSEAG member organizations.

c. The PSEWG Chairman may establish subordinate working or advisory groups to address specific functional areas. The groups will be established by charter and disestablished when the group's function is no longer valid. An example of such a group is the Security Operational Test Site Advisory Group which is established to—

(1) Review and coordinate Security Operational Test Site (SOTS) test schedules.

(2) Propose and plan site improvements.

(3) Encourage multi–Service use.

(4) Establish PSE test certification procedures.

(5) Prevent unnecessary duplication of testing.

(6) Provide an annual report, through the APSEAG, to the DOD PSEAG which includes the SOTS usage, fiscal status, planned improvements and so forth.

4–7. Program Management

a. The Physical Security Equipment Program involves many agencies within DOD and the Army, and is designed to meet the objectives stated in paragraph 4–3.

b. Within DA, responsibilities of HQDA, agencies, MACOMs, and installation commanders are per chapter 1. Specific procedural tasks relating to the Physical Security Equipment Program are discussed in paragraphs c through d below.

c. Executive agent tasks for the management of PSE shall include research and development; commercial NDI assessment and selection; and procurement of PSE. Army–assigned responsibilities for interior PSE include: barriers, lighting systems, command and control systems, and robotic systems in accordance with DODD 3224.3. (See appendix B.)

d. MACOM procedural tasks are outlined below.

(1) MACOMs will identify their physical security requirements through their participation in the Planning, Programming, Budgeting, and Execution System (PPBES). To enable ATCOM to properly forecast PSE procurement needs, MACOMs shall identify their best estimate of procurement and requisition requirements for Joint–Services Intrusion Detection System (J–SIIDS), other military standardized IDS, or commercial PSE, 5 years in advance of desired installation and provide the same to Commander, ATCOM, ATTN: AMSAT–I–STSG, 4300 Goodfellow Boulevard, St. Louis, MO 63120–1790.

(2) MACOMs shall approve all requests for purchase, issue, lease, or lease renewal of nonstandard PSE. Commanders below Army MACOM level are specifically prohibited from approving such requests. This includes commercial IDS, electronic entry control systems, and closed circuit televisions (CCTVs) when they are used for surveillance or assessment purposes. For USAR units, OCAR, (DAAR–CM) will be the approving authority for purchase, lease, or lease renewal of nonstandard PSE. Heads of Army staff agencies and commanders of FOAs obtain their approval for purchase, issue, lease, or lease renewal of nonstandard PSE from HQDA (DAMO–ODL–S), 4401 Ford Avenue, Alexandria, VA 22302–1432.

(3) MACOM commanders and commanders below MACOM level will establish procedures to provide a PSE review in support of request for the installation of PSE, whether these requests be for issue, purchase, lease, or lease renewal.

(a) The PSE review will emphasize a system approach that begins with a review of the current MACOM threat statement and its local supplements.

(b) The PSE review will be based on a security engineering survey which may be performed by supporting security, engineering, and communications representatives, or by qualified contractors. This survey will include an analysis of physical security requirements and costs, and a determination if protection will be significantly improved by installing the desired system or equipment.

(c) MACOMs may request security engineering surveys that are beyond their capability from HQUSACE on a cost reimbursable basis.

(d) The PSE review will also consider what other measures the local commander will implement when installing the proposed system, as well as the impacts on security procedures and security force manpower requirements.

(e) The PSE review will ensure that the requested system meets the threat without any unnecessary expenditure of funds.

(f) The PSE review will include the procedures outlined in paragraphs (5) and (6) below, to ensure that the goal of standardization of PSE within the Army is accomplished.

(4) MACOM commanders and other approving officials shall follow the procedures outlined in paragraphs (5) and (6) below, for their approval process and technical review of requests for purchase, issue, lease, or lease renewal of all PSE. Exempted from these procedures are:

(a) Army standard PSE. This is equipment that is centrally managed or is available through the DOD wholesale supply system. Requests for such equipment should be submitted to the appropriate item manager at the National Inventory Control Point.

(b) PSE acquired for the Army Terrorism Combatting Program. This program is designed to meet a time–sensitive need for organizations to defeat the terrorist threat and to increase the protection of soldiers, family members, DA civilians, key facilities security equipment, training, and intelligence. Access to this source of funding is immediate threat–driven in combination with a direct vulnerability. PSE requirements for this program, both standard and nonstandard, will continue to be submitted directly to HQDA (DAMO–ODL–CBT), 400 ARMY PENTAGON, WASH, DC 20310–0400, for validation, prioritization and funding in accordance with AR 525–13.

(c) Even through PSE acquired in support of the Army Terrorism Combatting program are exempt from the procedures outlined in paragraphs (5) and (6) below, the cost and technical specifications of nonstandard PSE procured as part of this program shall be provided to the PSEMO (AMSTR–PB).

(5) MACOMs, other agencies, and installations shall follow the following detailed step–by–step procedures for the waiver of standard PSE and for approval of nonstandard PSE.

(a) The installation identifies the requirement for PSE through issue, purchase, lease, or lease renewal.

(b) The installation determines the capability of standardized PSE to meet its requirements.

(c) The installation determines standardized equipment will not or cannot meet requirements or is not available.

(d) The installation requests from the MACOM with detailed justification based on (a) through (c).

(e) As specified below, MACOMs will coordinate requests with the appropriate manager of centralized standard PSE to confirm the nonavailability of standard equipment and/or to verify circumstances warranting local procurement of commercial equipment. Coordination is required when approval will result in or otherwise permit a local procurement of an IDS of more that five zones or other PSE valued at more that $25,000 or approval will result in or otherwise permit a local procurement of commercial equipment intended to modify, upgrade, or interface with standardized, type classified IDS of other PSE.

(f) MACOM approval of proposed additions by the installation to an existing IDS, using the same manufacturer's products purchased from the General Services Administration schedule, need not be coordinated beyond the MACOM. However, this need not preclude (but not make mandatory) the consideration of components of a standardized IDS in instances where such components are compatible and available within a time frame to meet installation requirements.

(g) MACOM approvals will reflect the coordination with the centralized manager(s) when required by paragraph (e). A copy of all approvals will be furnished to the PSEMO (AMSAT–W–TP), Fort Belvoir, VA 22060–5606. The PSEMO will advise the APSEAG regarding progress in standardization efforts within the PSE community.

(h) MACOM will also ensure the cost and technical specification of all nonstandard PSE procured as part of the Army Terrorism Counteraction program are provided to the PSEMO (AMSAT–W–TP).

(i) Once approved, the installation proceeds with issue, purchase, lease or lease renewal, or forwards the request to the Commander, ATCOM, ATTN: AMSAT–I–STSG, 4300 Goodfellow Boulevard, St. Louis, MO 63120–1790, to procure or fund as appropriate. Final equipment installation will be reported in accordance with existing reporting channels (and the Security Management Information System, when fielded).

(6) Procedures for technical review shall be as follows:

(a) The MACOM will ensure a review of the installation request is conducted for technical soundness. If such review exceeds the capability of the MACOM, the PSEMO, supported by the USACE, Huntsville Division (USACEHD), Mandatory Center of Expertise for IDS (IDS–MCX) as required, can perform this review for IDS of

6 zones or more. Technical reviews of standardized PSE are not required.

(b) The nature of the review will be established on a case–by–case basis and will depend upon the complexity of the request. A technical review of the design concept is all that is required prior to MACOM approval of the request. The results of the technical review will be included with the MACOM approval. A technical review of the final design can be conducted by the PSEMO and USACEHD (IDS–MCX), if requested, as details are sufficiently developed.

4–8. IDS equipment

A comprehensive physical security system detects aggressors and provides a means to delay them until they can be intercepted by a response force. IDS performs the detection function in the comprehensive system. IDS consists of the following: The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into an area protected by the system. IDS includes both interior and exterior systems, and may also include electronic entry control devices and CCTV for alarm assessment. The system shall be an approved DOD standardized system, or an Army– or MACOM–approved commercial system.

4–9. Priority of distribution and installation of IDS and related equipment

Threat assessment may dictate the responsible commander's reevaluation and reordering of the priority sequence. For example, the threat to key personnel may require that IDS for their quarters be procured and installed before a normally higher priority site. When such changes are required, the MACOM must ensure that ATCOM is aware of this need so that funding can be made available as soon as possible. When completing MACOM submission forms, the priorities and priority codes in table 4–1 shall be used.

Table 4–1
Priorities and priority codes

Category	Code	Type of facility
NA	P1	Nuclear storage site
	P2	Chemical storage site
		Conventional AA&E storage facilities
I	P3	Army National Guard Armories
	P4	U.S. Army Reserve Activities
	P5	Active Army, including ROTC
II	P6	Army National Guard Armories
	P7	U.S. Army Reserve Activities
	P8	Active Army, including ROTC
III	P9	Army National Guard Armories
	P10	U.S. Army Reserve Activities
	P11	Active Army, including ROTC
IV	P12	Army National Guard Armories
	P13	U.S. Army Reserve Activities
	14	Active Army, including ROTC
NA	P15	Classified storage facilities
	P16	Communications storage facilities
	P17	Controlled substance facilities
	P18	Other areas determined by the commander

4–10. IDS installation

a. For Purposes of IDS installation, all Army facilities and activities will be designated as security level A, B, C, or D as indicated in table 4–2 based on risk analysis determined using DA Pamphlet 190–51. Security levels are defined as follows:

Table 4–2
Security levels

Asset type or risk level	Security level
Nuclear/Chemical	A
Risk Level III	B
Risk Level II	C
Risk Level I	C

(1) *Level A (Maximum Level Security).* This level of security is required for an area containing a security interest or defense resource, the compromise or loss of which would have an immediate effect on the defense potential or capability of the United States. Unauthorized access to the area could result in destruction or loss of control of the resources, or disclosure of sensitive information.

(a) The total security effort for the area shall provide the highest possible probability of detection, assessment, and prevention of unauthorized access to the protected items.

(b) The security system shall detect any unauthorized penetration of the boundaries of the protected area, because the mere presence of an intruder in the protected area is unacceptable.

(c) Examples of areas that require Level A security are nuclear and chemical weapons storage facilities and sensitive compartmented information facilities (SCIFs).

(2) *Level B (Advanced Level Security).* This level of security is required for an area containing a security interest or defense resource, the compromise or loss of which would have a near–term effect on the defense potential or capability of the United States.

(a) The total security effort for the area shall provide a high probability of detection, assessment, or prevention of unauthorized penetration, approach, destruction, or removal of the protected item.

(b) The security system shall detect any unauthorized penetration of the boundaries of the protected area that results in introduction of contraband into the protected area, or removal of or damage to sensitive items within the protected area.

(c) Examples of areas which require Level B security are designated limited areas, and AA&E storage areas.

(3) *Level C (Intermediate Level Security).* This level of security is required for an area containing pilferable material or sensitive items that have a monetary value or are attractive for the intruder. This level of security is also required for equipment necessary for the continual functioning of the activity, but not necessarily a part of the immediate or near–term mission or defense capability.

(a) The total security effort for the area shall provide a reasonable probability of detection, assessment, or prevention of unauthorized penetration, approach, destruction, or removal of the protected item.

(b) The security system shall detect any unauthorized penetration of the protected area that results in removal of a protected item.

(c) Examples of areas which require Level C security are ports, critical communications centers, power stations, and critical command posts.

(4) *Level D (Basic Level Security).* This level of security is required for an area established to protect pilferable items, for the principal purpose of providing administrative control, safety, or a buffer for areas of a higher security category. Pilferable items within the area shall require the same physical protection as Level C.

(a) The security system shall detect any unauthorized penetration of the protected area that could result in removal of the protected item.

(b) Examples of areas which require Level D security are warehouses, motor pools, and designated controlled areas.

b. Facilities having IDS will have signs prominently displayed announcing the presence of IDS. They will be affixed at eye level, when possible, on the exterior of each interior wall that contains an entrance to the protected area. They will be affixed on exterior walls

only when the exterior wall contains an entrance to the protected area. Specifications for IDS signs are per appendix E.

4–11. IDS procurement and installation

All IDS projects consisting of six or more zones should be procured using negotiated procurement procedures. Invitation for bids (IFBs) and other low bid procedures should not be used.

4–12. New construction

Commanders and security personnel at all levels will ensure that all possible steps are taken to include IDS requirements in plans for new construction. Funds directly attributed to security should be separately identified by appropriation on construction worksheets using DD Form 1391 (Military Construction Project Data). See paragraph 4–16 for additional funding guidance.

4–13. Maintenance of IDS

The installation commander will maintain IDS per AR 420–43.

a. If systems are Government–owned, IDS maintenance is accomplished under the supervision of the installation Director of Engineering and Housing (DEH), Director of Logistics (DOL), or other designated personnel.

b. Not later than 2 years after acceptance, a post completion evaluation may be performed by the IDS–MCX, on a reimbursement basis, to ensure that the IDS was properly installed and is being maintained at the appropriate level.

c. OMA funds should be set aside for post completion evaluations.

4–14. Coordination

Direct program coordination is authorized between the Army staff, MACOMs, the user representative, and the PSEMO. Coordination with other DOD agencies, or other Government agencies and commercial or industrial activities is authorized, as required, to ensure integration of Army–developed PSE with equipment developed by other Services.

4–15. Planning for IDS

a. IDS shall normally include a central control station where alarms will annunciate, and from which a response force can be dispatched. An audible alarm bell located only at the protected location is not acceptable.

(1) The IDS shall be designed to cause a visual and audible alarm at the central control panel whenever the system is turned off or malfunctions. Some means of voice communication shall be provided between the protected areas and the monitoring area to coordinate status changes. Telephone communication should be considered.

(2) Access and secure switches shall be located at a central control station within the alarmed area.

(3) The IDS shall be placed such that there are sufficient barriers in the facility between the point of detection and the asset to delay the aggressors until a response force can intercept them.

(4) Facilities off military installations, will have a local alarm in addition to monitoring capability.

(5) Alarm circuitry that requires alarm signals to be cleared either by the central control station alarm monitor or by entering the protected area shall be used.

(6) Use of alarm delay switches at Reserve Component (RC) facilities is discouraged.

b. IDS shall include an independent, protected, backup power supply that will meet the backup power requirements identified in the security engineering survey.

c. Where an IDS is used in civilian communities, arrangements shall be made to connect alarms to civil police headquarters, private security companies, or a monitoring service from which immediate response can be directed in case of unauthorized entry.

(1) A commercial answering service is not authorized.

(2) Coordination is required with civil authorities to ensure a response force can be directed to respond immediately.

d. A daily log shall be maintained of all alarms received, and at a minimum shall include:

(1) The nature of the alarm; for example, intrusion system failure or nuisance alarm.

(2) The date and time the alarm was received.

(3) The location, and action taken in response to the alarm.

e. Logs shall be maintained for a minimum of 90 days, and shall be reviewed periodically to identify, monitor, and correct IDS reliability problems.

(1) DA Form 4930–R (Alarm/Intrusion Detection Record), will be used to record alarms received. DA Form 4930–R will be locally reproduced on 8 1/2– X 11–inch paper. A copy for reproduction purposes is located at the back of this handbook.

(2) A computer generated printout of alarms may be used as a substitute, provided all required information has been included or supplemental information is included in a log.

(3) Serios or recurring IDS problem areas will be described in writing and sent through command channels to Commander, ATCOM, ATTN: AMSAT–W–TP, Fort Belvoir, VA 22060–5606.

f. Transmission lines for the alarm circuits shall be electrically supervised and dedicated to minimize undetected tampering. Visible lines shall be inspected on a regular basis. Interior IDS transmission lines outside the protected area shall be installed in rigid conduit as specified in Federal Specification WW–581 or Article 345 of the National Electrical Code. IDS lines terminating in telephone panels will not normally be identified or distinguished from other lines.

g. Following requirements also apply:

(1) IDS will be considered for security classification if it meets the specific classifying criteria per AR 380–5 or other regulatory guidance. If the IDS is classified, personnel security clearances must be obtained for personnel whose duties involve the design, operation, or maintenance of the IDS.

(2) Only authorized personnel should be allowed access to unclassified IDS installation wiring diagrams for a specific facility or location. This also applies to information on known, specific vulnerabilities or counter–measures affecting the IDS.

(3) Personnel whose duties involve the design, operation, or maintenance of unclassified IDS require completion of a favorable National Agency Check (NAC) or NAC with written inquiries prior to appointment to such noncritical, sensitive positions. A local files check will also be conducted by the responsible security office.

(4) A check of the National Crime Information Center for installers and maintainers of unclassified IDS is a command decision. The decision will be based on—

(a) The sensitivity of the area to be protected.

(b) The need for quality control over personnel having access.

(5) All keys associated with IDS components will be safeguarded and controlled per AR 190–51.

(a) System operational checks will be made and logged by unit security personnel to ensure activation of the sensors.

(b) Installation physical security inspectors will include a spot check of various IDS zones during any security inspections to verify the IDS is operating satisfactorily. Checks will also be made of unit log entries and records regarding operation and inspection of IDS.

(6) Before accepting a newly installed IDS system for operation, an inspection will be conducted by qualified technical personnel to ensure the system meets all minimum acceptable standards. The statement of verification will be signed by the installation commander or designated representative, and maintained in the using unit or organization files. DA Form 4604–R (Security Construction Statement) will be used to record the verification. DA Form 4604–R may be locally reproduced on 8 1/2 X 11–inch paper. A copy for reproduction purposes is located at the back of this handbook

(7) Maintenance of IDS will be provided by personnel qualified in installation and repair of IDS. Such maintenance will be performed consistent with operational requirements to ensure continuous operation and reliability of each system in use.

(8) A duress signaling capability will be included in IDS protecting high–risk or high–value facilities and whenever constant surveillance posts are used.

4–16. Funding

a. Procurement

(1) Except as specified in (3), below, procurement of DOD or DA standardized PSE (or commercial PSE that has been approved by the MACOM headquarters) is funded by ATCOM using Army 2 (OPA) appropriated funds.

(1) According to provisions of AR 5–4, the Quick Return on Investment Program, Productivity Enhancing Capital Investment Program, and the Office of the Secretary of Defense Productivity Investment Funding may be used for procurement of PSE in certain situations if OPA funds are used. Requirements to use DOD or DA standardized PSE still apply. When commercial PSE are required, technical review procedures as outlined in paragraph 4–7 (less coordination with ATCOM) will be followed.

(3) MACOMs authorized to use Army Industrial Funds (AIF) to procure PSE may do so according to AR 37–110. Requirements to use DOD or DA standardized PSE still apply. When commercial PSE are required, technical review procedures as outlined in paragraph 4–4e (less coordination with ATCOM unless appropriate) will be followed.

(1) Army family housing funds will not be used to procure, install, or maintain PSE for quarters of high–risk personnel.

b. Installation and maintenance.

(1) Installation and maintenance of PSE is MACOM–funded using OMA appropriated funds. OPA 2 funds may be used if contracts include design, installation, and warranty. Installation and maintenance of PSE in Army Reserve Centers is paid for with OMAR funds.

(2) Installation of PSE may also be paid for with Military Construction, Army (MCA) funding when PSE is installed as a part of an overall construction effort.

(3) AMC and MTMC may also use AIF to install PSE.

c. Lease or lease renewal. Lease renewal, when authorized by the appropriate MACOM, will be paid for with local OMA or OMAR funds, as appropriate.

d. Forecast of PSE Projects.

(1) In the case of OPA 2, the total procurement requirement will be forwarded to ATCOM to be included in its forecast and thereafter adjusted based on funding authorization levels. MACOMs and ATCOM will coordinate directly to ensure adjustments are accomplished as necessary.

(2) Minor PSE projects (for example, procurement of J–SIIDS for an existing arms room will be funded by forecasting OPA 2 requirements to ATCOM; however, OMA base operations (BASOPS) installation funds are the responsibility of the MACOM and its MSCs.

(3) MACOMs normally will consolidate their MSC requirements for PSE projects involving OPA 2 when the combined multiappropriation cost of the individual PSE projects exceed $10K.

Chapter 5
Security Identification Cards and Badges

5–1. General

a. This chapter prescribes minimum uniform standards and procedures in the use of security identification cards and badges to control personnel movement into, and movement within, restricted areas. These standards and procedures are established to safeguard facilities against espionage, sabotage, damage, and theft. To accomplish this, commanders will establish—

(1) A practical, positive system to identify and control personnel entering, departing, and moving within restricted areas.

(2) A method to indoctrinate all assigned personnel concerning their individual security responsibilities.

b. Security identification cards and badges may be used to control access to installations and activities. They will be used in addition to other required identification cards to military personnel, civilian DOD and contractor employees, and visitors entering installations, activities, or restricted areas, as determined by the commander concerned.

5–2. Specifications for security identification cards and badges

a. Cards and badges will identify the name of the installation or activity for which they are valid.

b. Cards and badges will show the name and photograph of the person to whom issued. Visitor cards and badges will show " VISITOR" in place of name and photograph, and will have "ESCORT REQUIRED" or "NO ESCORT REQUIRED" printed across the face of the badge, as appropriate.

c. Cards and badges will contain a serial number.

d. Cards and badges issued for restricted (limited and exclusion) areas will show an expiration date.

e. Cards and badges will identify the area(s) for which they are valid.

f. Cards and badges using mechanical, electronic, or other technological reader to determine access authorization will be evaluated and approved by the Commander, ATCOM, (AMSAT–W–TP), Fort Belvoir, VA 22060–5606, prior to use.

5–3. Control and storage of security identification cards and badges

Control, storage, and classification standards are in AR 640–3.

a. The responsible installation or activity commander will establish detailed procedures controlling the issue, turn–in, recovery, and expiration of security identification cards and badges.

b. Engraved plates and all printed or coded parts of the cards and badges, although unclassified, will be handled and stored the same as CONFIDENTIAL material (see AR 380–5). The source of cards and badges will be controlled to prevent use by, or distribution to, unauthorized persons.

c. Mutilated or defective cards and badges, and those of discharged or transferred personnel, will be treated as CONFIDENTIAL material until destroyed. Lost cards and badges will be invalidated promptly.

d. Security clearances will not be recorded on cards and badges.

5–4. Replacement of security identification cards and badges

a. Restricted (controlled) area cards and badges will be replaced at intervals determined appropriate by the installation or activity commander, or when 10 percent of issued cards and badges are unaccounted for or lost.

b. Restricted (limited) area cards and badges will be replaced not later than 3 years from date of issue, or when 5 percent of the cards and badges issued are unaccounted for or lost.

c. Restricted (exclusion) area cards and badges will be replaced not later than 3 years from date of issue, or when any issued card or badge is unaccounted for or lost.

Chapter 6
Restricted Areas

6–1. General

This chapter sets forth guidance on the definition and designation of restricted areas within the 50 United States. Commanders outside the continental United States (OCONUS) may use information in this chapter to set up local procedures according to U.S. and host country agreements.

6–2. Authority (summarized)

a. Section 793(a), Title 18, United States Code. It is a felony for anyone to obtain information on national defense with the intent, or reason to believe, that such information is to be used to the injury of the United States, or to the advantage of a foreign nation to enter,

fly over, or otherwise obtain information about installations, facilities, or places that are connected with the national defense and controlled by the United States.

b. Section 793(b), Title 18, United States Code. It is a felony for anyone with like purpose and with like intent, attempts to or does copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense.

c. Section 21, Internal Security Act of 1950 (64 Stat. 1005, 50 USC 797). See extract in appendix C.

6–3. Designation of restricted areas

a. When conditions warrant, commanders of Army installations will designate restricted areas in writing to protect classified defense information, or safeguard property or material for which they are responsible.

b. Tenant units and activities on the installation will request the authority of the installation commander to designate their restricted areas.

c. Designation of restricted areas for Army activities not on an installation will be by the authority of the activity commander or officer in charge.

d. When required, physical safeguards will be installed to deter entry of unauthorized persons into the restricted area.

e. Commanders designating or terminating restricted areas to meet the requirements of AR 380–19, AR 380–40, AR 381–14, or AR 530–4, will advise the Commander, U.S. Army Intelligence and Security Command, ATTN: IAOPS–OP, Fort Meade, MD 20755–5995, of the establishment or termination. The applicable regulation will be cited.

6–4. Posting of restricted areas

a. Except when such action would tend to advertise an otherwise concealed area, or when in conflict with Host Nation Agreements, signs or notices will be posted in conspicuous and appropriate places to identify a restricted area. This includes signs posted at each entrance or approach to the area, and on perimeter fences or boundaries of the area.

b. Failure to post conspicuous signs and notices to give people approaching a restricted area actual knowledge of the restriction, may seriously hamper any resulting criminal prosecution.

c. Each sign or notice will be marked with the words, "RESTRICTED AREA," and include the warning notice below.

THIS (INSTALLATION, ACTIVITY, ETC.) HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF (TITLE: COMMANDING GENERAL OR COMMANDING OFFICER) IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 20 AUGUST 1954, PURSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNAUTHORIZED ENTRY IS PROHIBITED.

ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS, OR GRAPHIC REPRESENTATIONS OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED.

d. In areas in which English is but one of two or more languages commonly spoken, warning signs will contain the local languages besides English.

6–5. National defense areas

a. A restricted area may be established on non–federal lands within the United States, its possessions or territories, to protect classified defense information, and DOD equipment or material. When this type of area is established, it will be referred to as a National Defense Area (NDA). Examples of a NDA would include nuclear and chemical event (formerly accident or incident) sites, and aircraft crash sites.

b. Establishing a NDA temporarily places such non–federal lands under the effective control of DOD, and results only from an emergency event.

c. The senior DOD representative at the scene will define the boundary, mark it with a physical barrier, and post warning signs. Every reasonable attempt will be made to obtain the landowner's consent and cooperation in establishing of the NDA; however, military necessity will indicate the final decision regarding location, shape and size of the NDA.

d. The authority to establish a NDA includes the authority to deny access to the NDA. It also includes the authority to remove persons who threaten the orderly administration of the emergency site. Use of force employed to enforce this authority will be in accordance with AR 190–14.

6–6. Restricted area violation procedures

a. The Army installation commander will cause any person who enters a restricted area without authority to be brought immediately before proper authority for questioning.

(1) The person may be searched per AR 190–30. Any notes, photographs, sketches, pictures, maps, or other material describing the restricted area may be seized.

(2) Persons brought before proper authority for questioning will be advised of their rights per AR 190–30, appendix C. Questioning will be conducted without unnecessary delay.

b. If the person was unaware of the restriction, and neither acquired nor intended to acquire knowledge of sensitive or classified information by entering, that person will be warned against reentry and released.

c. If it appears that the person knowingly entered a restricted area, or may have acquired or intended to acquire sensitive or classified information by entering, or may have committed some other offense, the actions below will be taken.

(1) Persons not subject to the Uniform Code of Military Justice (UCMJ) will be taken without delay to civilian law enforcement officials. In the United States, the nearest office of the FBI will be notified, and the person will be turned over to the nearest U.S. Marshal. If the person cannot be turned over to a U.S. Marshal within a reasonable period of time (three or four hours), he or she will be taken before an appropriate state or local official. (See 18 USC 3041.) As soon as possible, the agency to which the person is transferred will be given a written statement of the facts, the names and addresses of the witnesses, and pertinent exhibits as may be available.

(2) A person subject to the UCMJ will be turned over to his or her commander or the proper military law enforcement official.

d. Facts regarding a deliberate violation of a restricted area will be immediately reported per AR 381–12, paragraph 8.

Chapter 7
Department of the Army Physical Security Review Board

7–1. General

a. This chapter establishes the Department of the Army Physical Security Review Board (DAPSRB) as a continuing committee, and outlines the purpose, responsibilities and composition of the Board.

b. The purpose of the DAPSRB is to ensure coordinated and practical DA efforts to reduce or eliminate incidents involving loss, theft, damage, or wrongful appropriation of Government property, including security of military and DA civilians and their personal property within a military facility.

c. The provisions of this chapter are applicable to all Active Army commands and activities at installation level and higher, and may be used by the National Guard and Reserve.

7–2. Function of the DAPSRB

The DAPSRB will evaluate the concepts, management systems, doctrine, construction programs, and supporting materiel systems for physical security within DA. The DAPSRB will determine their suitability and initiate necessary measures to establish staff responsibilities and ensure that physical security support by the Army is effective, responsive, and attainable. Specifically, the DAPSRB will—

a. Evaluate and determine the suitability of physical security concepts, procedures, and responsibilities, and develop detailed recommendations on the appropriate staff relationship for each aspect of physical security.

b. Verify assignment and documentation of physical security responsibilities, and identify the need for clarifying and implementing instructions to MACOMs.

c. Review and analyze reports, data, and other information from all sources which might indicate the need for policy initiation or modification.

d. In coordination with DA and other agencies, when applicable, initiate surveys and activity evaluations to determine compliance with physical security standards and procedures.

e. Review requirements and doctrine regarding PSE needs and policies to ensure Army–wide standardization, and to ensure that physical security criteria are considered in initial plans for research and development projects, as well as new or modified construction projects.

f. Perform related analyses directed by the Chairman, DAPSRB.

7–3. Composition

The Board will consist of the following:

a. Chairman of the Board: Chief, Security, Force Protection and Law Enforcement Division (DAMO–ODL).

b. One voting member (lieutenant colonel, major, or civilian equivalent) will be furnished by each of the following:

(1) The DCSOPS (the Chairman may serve as the DCSOPS representative).

(2) The DCSPER.

(3) The DCSINT.

(4) The DCSLOG.

(5) Physical Security Equipment Management Office.

(6) Chief, National Guard Bureau.

(7) Chief, Army Reserve.

(8) Chief of Engineers.

(9) The Surgeon General.

c. Nonvoting representatives will be furnished by—

(1) The Inspector General.

(2) The Auditor General.

(3) The MACOMs.

(4) U.S. Army Nuclear and Chemical Agency.

(5) USAMPS.

(6) A nonvoting recorder furnished by the Chairman.

(7) Representatives from other Army Staff agencies and MACOMs who request to attend or who are invited by the Chairman to act as advisers to the DAPSRB when items affecting their agencies or commands are to be discussed.

7–4. Direction and control

a. The DAPSRB will meet at the call of the Chairman. Agenda items will be determined by the Chairman. Individual items may be submitted by the members to the Chairman for action by the Board.

b. Administrative support for the Board will be provided by the Chairman. However, requests for travel in conjunction with field visits will be arranged by the individual members and funded by the organizations they represent.

7–5. Correspondence

All communications to the DAPSRB will be addressed to HQDA(DAMO–ODL), ATTN: Chairman, DAPSRB, 400 ARMY PENTAGON, WASH DC 20310–0400.

Chapter 8
Security Forces

8–1. General

A security or guard patrol, or unit personnel, shall periodically check facilities and areas used to store sensitive or critical items or equipment as prescribed herein, and as dictated by a threat and vulnerability analysis. Checks shall be conducted on an irregular basis during nonduty hours to avoid establishing a pattern. Security checks will ensure unauthorized personnel are not in the area, and structures are intact and have not been broken into. During periods of increased vigilance because of a threat situation, security patrols will physically inspect doors and locks on all storage structures in their area of responsibility. Selection of personnel to perform guard duties will be closely monitored by commanders, or their equivalents, to ensure only properly trained and reliable individuals are assigned duty. Supervisory checks will be conducted to ensure guard duties are being performed properly.

a. Security patrols may be conducted by military personnel; civilian security personnel, including contract and contractor personnel; U.S. Marshal Service; or state, local, or campus police.

b. DA–controlled security forces shall be provided with adequate means of communication.

c. Security forces personnel (for example, guards, security patrols, security reaction forces) may be armed with appropriate weapons and ammunition at the discretion of the commander concerned. If such personnel are armed, provisions of AR 190–14 apply.

8–2. Guard procedures

Guard procedures shall be reviewed at least annually, and revised (if necessary) to provide greater application of security measures. Special emphasis will be placed on guard post locations and guard orientation concerning duties to be performed.

8–3. Inspections and guard checks

Inspections and guard checks shall be increased during nights, weekends, and holidays, based upon the local threat and as determined by the installation commander, to provide for deterrence of violations and for the early detection of loss. Checks shall be recorded and will consist of an inspection of the building or facility, including all doors and windows. Records of checks shall be maintained for a minimum of 90 days, and then destroyed.

8–4. Security patrol plans

Security patrol plans shall be coordinated and integrated with the guard plan or other security plans and programs to the maximum extent possible. When facilities are located in civilian communities, liaison shall be established with local civil police agencies to ensure that periodic surveillance is conducted, and that a coordination plan for security exists.

Appendix A
References

Section I
Required Publications

AR 5–9
Intraservice Support Installation Area Coordination. (Cited in paras 1–25d and 2–1b.)

AR 10–13
US Army Communications Command. (Cited in para 1–19b.)

AR 11–2
Internal Control Systems. (Cited in para 2–11a(1).)

AR 37–49
Budgeting, Funding, and Reimbursement for Base Operations Support of Army Activities. (Cited in para 1–23b(8).)

AR 71–9
Materiel Objectives and Requirements. (Cited in paras 1–17d and 4–3f.)

AR 190–30
Military Police Investigations. (Cited in paras 6–6a(1) and 6–6a(2).)

AR 210–10
Administration. (Cited in paras 1–23b(8) and 2–5d.)

AR 310–25
Dictionary of United States Army Terms. (Cited in para 1–23.)

AR 380–5
Department of the Army Information Security Program. (Cited in paras 2–13, 4–15g, and 5–3b.)

AR 380–19
Information Systems Security (Cited in para 6–3e.)

AR 380–40
(C) Policy for Safeguarding and Controlling COMSEC Information (U). (Cited in para 6–3e.)

AR 381–12
Subversion and Espionage Directed Against US Army (SAEDA). (Cited in para 6–6d.)

AR 381–14
(S) Technical Surveillance Countermeasures (TSCM) (U). (Cited in para 6–3e.)

AR 420–43
Electrical Services. (Cited in para 4–13.)

AR 530–1
Operations Security (OPSEC). (Cited in paras 1–6b(3) and 1–23b(4).)

AR 530–4
(C) Control of Compromising Emanations (U). (Cited in para 6–3e.)

AR 600–200
Enlisted Personnel Management System. (Cited in paras 1–23 3–3a.)

AR 611–201
Enlisted Career Management Fields and Military Occupational Specialties. (Cited in para 3–3a.)

AR 640–3
Identification Cards, Tags, and Badges. (Cited in para 5–3.)

AR 690–950
Career Management. (Cited in para 3–1b(1).)

AR 700–84
Issue and Sale of Personal Clothing. (Cited in para 3–6c.)

AR 700–127
Integrated Logistic Support. (Cited in para 1–7a.)

AR 710–2
Supply Policy Below the Wholesale Level. (Cited in para 2–11b(8).)

DODD 3224.3
Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support. (Cited in paras 1–18f(1), 4–1, 4–3a, 4–3i, 4–3j, 4–4b(7), 4–7c, and Summary.) (See app B.)

DODD 5200.8–R
Physical Security Program. (Cited in Summary.)

FM 19–30
Physical Security. (Cited in para 2–9.)

CPR 950–19
Army Civilian Career Program for Intelligence (Cited in para 3–1b(2).)

GS–080–0
Security Administration Series Position Classification Standard. (Cited in paras 3–1b(3), and 3–2b.) This publication can be obtained from the Office of Personnel Management (OPM), WASH DC 20415.

Section II
Related Publications

AR 5–4
Department of the Army Productivity Improvement Program

AR 25–1
The Army Information Resources Management Program

AR 37–110
Budgeting, Accounting, Reporting, and Responsibilities for Industrial Funded Installations and Activities

AR 50–5–1
(C) Nuclear Weapon Security (U)

AR 190–14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190–16
Physical Security

AR 190–51
Security of Army Property at Unit and Installation Level

AR 190–59
Chemical Agent Security Program

AR 525–13
The Army Terrorism Combating Program

AR 600–20
Army Command Policy

AR 700–129
Management and Execution of Integrated Logistics Support for Multi–Service Acquisitions

DA Pam 190–51

Risk Analysis for Army Property

DOD 5200.1–R
Information Security Program Regulation.

Section III
Prescribed Forms

Exact duplicates of any DA or DD forms generated by the automated Military Police Management Information System may be used in place of the printed version of the form.

Forms that have been designated 'approved for electronic generation (EG)' must replicate exactly the content (wording), format (layout), and sequence (arrangement) of the official printed form. The form number of the electronically generated form will be shown as –R–E and the date will be the same as the date of the current edition of the printed form.

DA Form 2806–R (approved for EG)
Physical Security Survey Report. (Prescribed in para 2–10d.)

DA Form 2806–1–R (approved for EG)
Physical Security Inspection Report. (Prescribed in paras 2–11d, 2–11e, and 2–12.)

DA Form 4604–R (approved for EG)
Security Construction Statement. (Prescribed in para 4–15g(6).)

DA Form 4261 and DA Form 4261–1
Physical Security Inspector Identification Card. (Prescribed in para 3–4.)

Section IV
Referenced Forms

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 4930–R (approved for EG)
Alarm/Intrusion Detection Record. (Prescribed in para 4–15e(1).)

DD Form 1391
Military Construction Project Data

Appendix B
DOD Directive 3224.3 (minus enclosures)

Department of Defense Directive

February 17, 1989
NUMBER 3224.3

SUBJECT: Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support

References:

(a) DoD Directive 3224.3, "Physical Security Equipment: Assignment of Responsibility for Research, Engineering, Procurement, Installation, and Maintenance," December 1, 1976 (hereby canceled)
(b) DoD Directive 5000.1, "Major and Non–Major Defense Acquisition Programs," September 1, 1987
(c) DoD Instruction 5000.2, "Defense Acquisition Program Procedures," September 1, 1987

(d) DoD Directive 4120.3, "Defense Standardization and Specification Program," February 10, 1979
(e) through (t), see enclosure 1

I. Reissuance and Purpose

a. This Directive updates and reissues reference (a) to:
(1) Establish practices and procedures consistent with the requirements of references (b) through (t).
(2) Provide updated guidelines to DoD Components for managing and coordinating research, engineering, procurement, installation maintenance, and material support for PSE.
(3) Expand the responsibilities and participation of DoD Components in the PSE program.
(4) Broaden the scope of the PSE program.
b. Current guidance on responsibilities and organizations associated with the PSE program in various DoD memoranda is consolidated in this Directive.
c. All guidance associated with the acquisition of PSE and system security engineering for weapon systems acquisition shall be reviewed for compliance with this Directive.

II. Applicability and Scope

This Directive applies to:
a. The Office of the Secretary of Defense (OSD), the Military Departments, the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as 'DoD Components'). The term 'Military Services,' as used herein, refers to the Army, Navy, Air Force, and Marine Corps.
b. All programs associated with the acquisition of PSE and systems designed, developed, and acquired to support weapon system programs, anti–terrorist installation programs, tactical force protection packages, and the programs described by DoD 5100.76–M; DoD Instructions 5220.30 and 5210.71; and DoD Directives 5210.63, 5210.64, 5210.65, and 5210.73 (references (i) through (o)), except for equipment or techniques used or designated as follows:
(1) Primarily for safety purposes.
(2) Expressly to prevent the unauthorized use of nuclear weapons; i.e., denial, disable, and permissive action link devices.
(3) For technical surveillance and countermeasures.
(4) To provide communications security (COMSEC) protection, including features integral to COMSEC equipment.
(5) For criminal or counterintelligence investigation.
(6) For computer security protection integral to automated information systems.

III. Definitions

a. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent or delay unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage, and theft.
b. Physical Security Equipment (PSE). A generic term encompassing any item, device, or system that is used primarily for the protection of Government property, including nuclear, chemical, and other munitions, personnel, installations, and in the safeguarding of national security information and material, including the destruction of such information and material both by routine means and by emergency destruct methods.

IV. Policy

a. The objective of the DoD PSE program is to select or design, evaluate, and acquire the most efficient and productive security

equipment at the most reasonable cost to ensure the effective protection of DoD resources, including personnel, classified information, material, and readiness assets.

b. The following specific measures are necessary to achieve the objective of the PSE program:

(1) Provide adequate programming, planning, and funding support for both near term and long lead requirements.

(2) Eliminate duplication of research and engineering effort while ensuring interoperability between essential elements of security systems fielded by the DoD Components.

(3) Consider the legitimate differing operational needs of the DoD Components for physical security systems while coordinating research, engineering, and production requirements for items common to the DoD Components.

(4) Use commercial equipment where feasible. Requirements for security equipment must be thoroughly identifiable. In–house research and development projects should be started only when there is no commercially available equipment, which shall approximate the particular requirement or when its performance is not operationally suitable. Before a Military Service or an Agency may start a research, development, test, and evaluation (RDT&E) project within the Department of Defense, that Military Service and/or Agency must certify to OSD that a check of nondevelopmental items (NDI) has been conducted, state how it was conducted, and confirm that only an internal DoD development effort ensures an economic and timely approach to satisfy a particular need. That certification shall be processed through the JRWG and become a part of that group's minutes.

(5) Increase coordination and information sharing among DoD and other Executive branch Departments and Agencies, and consolidating testing when feasible.

(6) Provide a Physical Security Equipment Listing (PSEL) to identify all PSE that the sponsors believe may have DoD application. Procurement of security equipment for the purpose of RDT&E is not limited by this Directive. The use of the PSEL and other procurement procedures are subject to guidelines set out in Section 9.2 of the FAR (reference (f)).

(7) Use single–Service procurement by the DoD Component responsible for development of specific PSE where appropriate, more efficient, and cost effective.

(8) Streamline PSE acquisition organizations in accordance with DoD Directive 5000.1 (reference (b)).

V. Responsibilities

a. The Under Secretary of Defense for Acquisition (USD(A)) shall provide overall DoD oversight for research, engineering, procurement, installation, and maintenance of the PSE programs, and under the Director, Defense Research and Engineering (DDR&E):

(1) The Deputy Under Secretary of Defense (Tactical Warfare Programs) (DUSD(TWP)) shall:

(a) Act for the USD(A) as the DoD centralized coordinator of research, engineering, procurement, deployment, and support of the PSE programs.

(b) Determine the feasibility and assign to the appropriate DoD Component each PSE project or task.

(c) In carrying out this responsibility, be assisted by the Physical Security Equipment Steering Group (PSESG) and the Physical Security Equipment Action Group (PSEAG).

(d) Co–chair the PSESG.

(e) Appoint the PSEAG chairperson.

(2) The Deputy Under Secretary of Defense (Research and Advanced Technology) (DUSD(R&AT)) shall provide senior–level representation on the PSESG and representation on the PSEAG.

(3) The Assistant to the Secretary of Defense (Atomic Energy) (ATSD(AE)) shall:

(a) Serve as the advisor and focal point for issues on nuclear weapons security.

(b) Provide senior–level representation on the PSESG and representation on the PSEAG.

b. The Assistant Secretary of Defense (Production and Logistics) (ASD(P&L)) shall:

(1) Provide the DUSD(TWP) advice on the production, procurement, deployment, and support of the PSE programs.

(2) Provide senior–level representation on the PSESG and representation on the PSEAG.

c. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) shall:

(1) Provide senior–level representation on the PSESG and representation on the PSEAG.

(2) Coordinate PSE development efforts sponsored by the Interdepartmental Group/Terrorism (IG/T) with the PSEAG.

d. The Under Secretary of Defense (Policy) (USD(P)), through the Deputy Under Secretary of Defense for Policy (DUSD(P)), shall:

(1) Develop overall physical security policy.

(2) Evaluate and validate PSE requirements in relation to policy decisions and recommend to the DUSD(TWP) changes, as necessary.

(3) Provide the DoD member on the Interagency Advisory Committee on Security Equipment (IACSE), General Services Administration (GSA).

(4) Co–chair the PSESG.

(5) Provide representation on the PSEAG.

(6) Coordinate information security equipment development efforts by the DoD Security Institute with the PSEAG.

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

(1) Provide DUSD(TWP) advice on special PSE requirements to support anti–terrorist programs.

(2) Coordinate special equipment requirements for physical security with the PSEAG.

(3) Provide senior–level representation on the PSESG and representation on the PSEAG.

f. The Director, Joint Staff, shall:

(1) Provide joint considerations for proposed PSE acquisition programs.

(2) Ensure that the interests of the Unified and Specified Commands are addressed when joint PSE programs require resolution.

g. The Commanders in Chief of the Unified and Specified Commands shall:

(1) Recommend and/or submit requirements for research and development (R&D) or acquisition of PSE through their respective Military Departments.

(2) Participate in meetings of the PSESG and the PSEAG, as required, to provide advice on operational requirements and employment of PSE.

h. The Director, Defense Nuclear Agency (DNA), shall:

(1) In cooperation with the Military Services and the Unified and Specified Commands, develop an exploratory development program through proof–of–concept to determine technologies and techniques to improve the security of nuclear weapons.

(2) Perform the evaluation and prioritization process for selection of the exploratory development of nuclear security–related PSE projects, including robotics, to be implemented each fiscal year.

(3) Provide the PSEAG Chairperson with a program outline of all research efforts.

(4) Provide management, operation, and support functions, including the responsibility for programming, budgeting, funding, and reporting on all exploratory development efforts undertaken in response to the requirements of the Department of Defense in the security of nuclear weapons.

(5) Perform surveys of available commercial items to ensure that developmental effort is required before starting any exploratory development.

(6) Provide members of the PSESG and the PSEAG with results from exploratory development programs for the security of nuclear weapons and related assets that may have applicability to other PSE programs.

(7) Provide a senior–level member on the PSESG and representation on the PSEAG.

(8) Provide representation on the JRWG and the Security Equipment Integration Working Group (SEIWG).

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

(1) Provide appropriate threat information to assist the development of PSE acquisition programs in response to validated requirements.

(2) Identify intelligence community requirements for PSE to the PSESG and the PSEAG.

j. The Executive Secretary to the Secretary of Defense shall provide the DUSD(TWP) with White House Military Office (WHMO) requirements for DoD PSE acquisition programs.

k. The Secretary of the Army shall:

(1) Perform the management, operation, and support functions, including the responsibility for programming, budgeting, funding, and publication of standards, military specifications, and design and performance criteria for research and engineering of interior PSE, including barriers, lighting systems, and command and control systems, and robotics systems as they apply to any of the areas of this paragraph.

(2) Provide assistance, as required in functional areas of responsibility, to the other Military Services in the development, testing, evaluation, acquisition, deployment, and installation of PSE.

(3) Provide technical representation to interagency technical advisory subcommittees addressing PSE.

(4) Review the security requirements of major weapon system developments, with a view towards using PSE currently under development, or in procurement, to replace or augment security personnel.

(5) Recognize and support the JRWG (formerly tri–Service Working Group) (enclosure 3) and the SEIWG (enclosure 4).

(6) Perform the same functions for other programs and tasks that may be assigned by the DUSD(TWP).

l. The Secretary of the Navy (SECNAV) shall:

(1) Perform the management, operation, and support functions, including the responsibility for programming, budgeting, funding, and publication of standards and military specifications, and design and performance criteria for all research and engineering of shipboard and waterside physical security systems, anti–compromise emergency destruct (ACED) systems, explosive detection systems, and robotic systems, as they apply to any of the areas in this paragraph.

(2) Provide assistance, as required in functional areas of responsibility, to the other Military Services in the development, testing, evaluation, acquisition, deployment, and installation of PSE.

(3) Provide technical representation to interagency technical advisory subcommittees addressing PSE.

(4) Develop, test, and procure in coordination with the other Military Services locking devices, security containers, and related delay systems.

(5) Review the security requirements of major weapon system developments, with a view towards using PSE currently under development, or in procurement, to replace or augment security personnel.

(6) Recognize and support the JRWG (enclosure 3) and the SEIWG (enclosure 4).

(7) Perform the same functions for other programs and tasks that may be assigned by the DUSD(TWP).

m. The Secretary of the Air Force shall:

(1) Perform the management, operation, and support functions, including responsibility for programming, budgeting, funding, and publication of standards and military specifications, and design and performance criteria for all research and engineering of exterior PSE (except barriers and lighting systems) including aerial intrusion detection systems associated with facilities, installations, bases, entry control systems, and robotic systems, as they apply to any of the areas in this paragraph.

(2) Provide assistance, as required in functional areas of responsibility, to the other Military Services in the development, testing, evaluation, acquisition, deployment, and installation of PSE.

(3) Provide technical representation to interagency advisory technical subcommittees addressing PSE.

(4) Review the security requirements of major weapon systems developments, with a view towards using PSE currently under development, or in procurement, to replace or augment security personnel.

(5) Recognize and support the JRWG (enclosure 3) and the SEIWG (enclosure 4).

(6) Perform the same function for other programs and tasks that may be assigned by the DUSD(TWP).

n. The Military Services shall:

(1) Forward validated 'Statements of Requirement for PSE' to the JRWG Chairperson for distribution to the other Military Services. Each Military Service shall review the statement to determine whether there are joint Service requirements for the equipment item. At the next meeting of the JRWG, the Military Service submitting the 'Statement of Requirement' shall brief the project, Military Service comments shall be discussed, and a determination shall be made to proceed as a joint Service or as a single–Service project. Single–Service projects shall be returned to the needing Military Service for action. For joint Service projects, the JRWG Chairperson shall determine a lead Military Service based on this Directive (see paragraphs V.K.1., V.L.1., and V.M.1., above) and task the lead Military Service with development of a joint Service operational requirement (JSOR), performance specifications, operational test procedures, and maintenance and/or logistics specifications.

(2) If assigned areas of responsibility herein, or PSE projects and tasks by the DUSD(TWP) or the PSESG:

(a) Establish a program management office structure to discharge its responsibilities and interface with other Military Services and Agencies.

(b) Augment the program management office of other Military Services, as required, to provide coordination.

(c) Act as the DoD procuring Agency for the PSE that the Military Service develops.

(d) Establish and maintain program structure plans, cost summaries, and funding profiles using to the extent practical the guidance and formats in DoD Instruction 5000.2 (reference (c)). Those records shall coincide with the PPBS and shall be available to the PSEAG chairperson on a regular basis and for scheduled meetings of the PSESG and the PSEAG.

(e) Provide a program, funded at a meaningful level, to develop a PSEL. Commercial equipment to be listed shall be limited to areas of assigned responsibilities.

(3) Identify a single point of contact for PSE on each Military Service staff to address and manage programmatic PSE issues.

(4) Provide representatives to the committees identified herein for monitoring and direction of the PSE program.

(5) Use MILHDBK 1013/1 (reference (t)) as a guide for the design of new facilities.

VI. Procedures

a. A centrally managed PSE program shall be established by each Military Service and the DNA to ensure that PSE considerations are incorporated into the planning, development, acquisition, deployment, installation, and support of the programs, as defined in subsection II.B., above.

b. The PSE program for each DoD Component shall comply with references (b) through (g) an (r) through (t).

c. All Military Departments and the DNA shall develop supporting or implementing Directives to guide their respective PSE programs toward achieving the DoD objective.

d. A PSESG shall be formed under the co–chairmanship of the Deputy Under Secretary of Defense (Tactical Warfare Programs) (DUSD)(TWP)) and the Deputy Under Secretary of Defense (Policy) (DUSD(P)) to accomplish the following:

(1) Evaluate the progress made in achieving the DoD PSE program objectives and make recommendations, as required.

(2) Ensure the DoD PSE program receives proper emphasis in the Defense Guidance (DG) and program reviews.

(3) Monitor all DoD PSE acquisition programs to ensure coordination and prevent duplication among DoD Components. Review, monitor, and facilitate the transition of DNA PSE exploratory development programs to the Military Departments for continued development, as required.

(4) Facilitate the exchange of information among DoD Components and between the Department of Defense and other Federal Agencies.

(5) Review the 'System Security Engineering Programs' of new major weapon systems and facility acquisitions to ensure that the DoD security equipment research, development, and acquisition (RD &A) system is providing them with adequate, timely, state–of–the–art support.

(6) The following shall provide a general and/or flag officer, or equivalent civilian grade member, to the PSESG:

(a) DUSD(TWP): co–chair.

(b) DUSD(P): co–chair.

(c) Assistant Secretary of Defense (Production and Logistics) (ASD(P&L)).

(d) Assistant Secretary of Defense (Special Operations and Low–Intensity Conflict) (ASD(SO/LIC)).

(e) Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)).

(f) Deputy Under Secretary of Defense (Research and Advanced Technology) (DUSD(R&AT)).

(g) Assistant to the Secretary of Defense (Atomic Energy) (ATSD(AE)).

(h) Department of the Army.

(i) Department of the Navy.

(j) Department of the Air Force.

(k) DNA.

(7) Normally, the Military Services shall represent the Commander in Chiefs (CINCs). However, the JCS may attend meetings to address joint issues. When a CINC has an issue of specific interest to the respective command, a CINC representative may attend the meeting.

(8) Due to their special role in supporting the DoD PSE program, the Defense Intelligence Agency (DIA) shall provide the following senior representation to the PSESG:

(9) Observers from other DoD and Federal Agencies may be invited for specific programs of joint interest.

(10) The PSESG shall meet at least annually at the call of the PSESG Chair.

e. Physical Security Equipment Action Group (PSEAG)

(1) The DoD PSEAG, chartered by signature on this Directive, shall perform additional duties, as directed by the PSESG and described in enclosure 2.

(2) The JRWG, chartered by signature on this Directive, shall support the PSEAG, as described at enclosure 3.

(3) The SEIWG, chartered by signature on this Directive, shall support the PSEAG, as described in enclosure 4.

VII. Effective Date and Implementation

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense (Acquisition) within 120 days.

William H. Taft, IV
Deputy Secretary of Defense

Appendix C
Extract from Internal Security Act of 1950 (50 USC, Section 797)

Figure C–1 is an extract from the Internal Security Act of l950 (50 USC, Section 797), which provides guidance regarding restricted areas.

Security regulations and orders, penalty for violation Sec. 21

(a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, waterfront facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, and Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse of other unsatisfactory conditions thereon, or the ingress thereto or egress of removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss or injury by accident or by enemy action, sabotage, or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine not to exceed $5,000 or to imprisonment for nor more that one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

Title 18, US Code, Section 1382

Sec. 1382. Entering military, naval, or Coast Guard property. Whoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation for any purpose prohibited by law or lawful regulation; or

Whoever reenters or is found within any such reservation, post, fort, arsenal, yard, station, or installation, after having been removed there from or ordered not to reenter by any officer or person in command or charge thereof—

Shall be fined not more that $500 or imprisoned not more that six months, or both.

Figure C-1. Extract from Internal Security Act of 1950

Appendix D
Authority of Military Commanders

The military commanders below are hereby designated as having the authority to enforce the necessary regulations to protect and secure places and property under their command according to the Internal Security Act of 1950.

a. Commanding officers of all military reservations, posts, camps, stations, or installations subject to the jurisdiction, administration, or in the custody of DA.

b. Commanders of installations or activities subject to the jurisdiction, administration, or in the custody of Defense agencies or separate operating activities.

c. The military commander in the chain of command immediately above an installation or activity not headed by a military commander. Such commanders will enforce regulations or orders pertaining to an installation or activity not headed by a military commander, and issued under the authority of the Internal Security Act of 1950.

Appendix E
Specifications for Intrusion Detection System Signs

E–1.
A sample intrusion detection system sign that may be used is shown in AR 190–11, figure F–1. The sign is flat with shape, size and legend as shown. The sign face should consist of reflectorized sheeting bonded to an aluminum backing.

E–2.
The sign backing is flat, degreased, etched, and unpainted aluminum alloy, type 6061T6, not less that 1/16–inch thick. For interior posting, plastic or wood may be used.

E–3.
In non–English speaking overseas areas, a sign in the language of the host country, should be mounted alongside the English language sign. In the United States and possessions where a major minority language is spoken, similar signs may be posted as a safety precaution.

Glossary

This is the consolidated glossary for the Physical Security Handbook.

Section I
Abbreviations

AA&E
arms, ammunition, and explosives

AC
Active Component

ACSI
Assistant Chief of Staff for Intelligence

ADP
automatic data processing

AE
ammunition and explosives

AFB
Air Force Base

AFH
Army family housing

AFI
annual formal inspection

AFSPA
Air Force Security Police Agency

AG
Adjutant General

AGS
Armed Guard Surveillance

AIF
Army Industrial Funds

AMC
U.S. Army Material Command

AMDF
Army Master Data File

AP
acquisition plan

APSEAG
Army Physical Security Equipment Action Group

AR
Army regulation

ARDEC
U.S. Army Armament Research, Development and Engineering Center

ARNG
Army National Guard

ARSTAF
Army Staff

ASA (IL&E)
Assistant Secretary of the Army (Installations, Logistics, and Environment)

ASA (RDA)
Assistant Secretary of the Army (Research, Development, and Acquisition)

ASI
additional skill identifier

ASI H3
ASI for physical security inspector

ASI P7
ASI for patrol/narcotics or contraband detector dog handler

ASI Z6
ASI for patrol/explosives detector dog handler

ASL
authorized stockage list

ASP
ammunition supply point

AT
antiterrorism

ATC
Air Training Command

ATCOM
U.S. Army Aviation and Troop Command

BASOPS
base operations

BATF
Bureau of Alcohol, Tobacco, and Firearms

BCU
battery coolant unit

BRDEC
Belvior Research & Development Engineering Center

CB
close boundary

CBT/T
combatting terrorism

CCI
controlled cryptographic items

CCP
circulation control point

CCTV
closed circuit television

CDR
commander

CE
U.S. Army Corps of Engineers

CECOM
U.S. Army Communications-Electronics Command

C-E
communications-electronics

CFM
cubic feet per minute

CG
commanding general

CL
carload

CMP
Civilian Marksmanship Program

COA
Comptroller of the Army

COCO
contractor-owned, contractor-operated

COE
Chief of Engineers

COFC
container-on-flatcar

COMDT
commandant

COMSEC
communications security

CONEX
container express

CONUS
continental United States

CONUSA
the numbered armies in the Continental United States

CPA
Chief of Public Affairs

CPCO
Central Port Call Office

CPR
civilian personnel regulation

CQ
charge of quarters

CRC
U.S. Army Crime Records Center

CSS
Constant Surveillance Service

CT
counterterrorism

CUCV
commercial utility and cargo vehicle

DA
Department of the Army

DAPSRB
Department of the Army Physical Security Review Board

DCSINT
Deputy Chief of Staff for Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations

DCSPER
Deputy Chief of Staff for Personnel

DDPS
Dual Driver Protective Service

DEA
Drug Enforcement Administration

DEFCON
defense readiness condition

DEH
Director of Engineering and Housing

DLA
Defense Logistics Agency

DNA
Defense Nuclear Agency

DOD
Department of Defense

DODD
Department of Defense directive

DOL
Director of Logistics

DPDO
Defense Property Disposal Office

DRMO
Defense Reutilization Marketing Offices

DTS
Defense Transportation System

DUSD(P)
Deputy Under Secretary of Defense for Policy

EDD
explosives detector dog

ENTNAC
Entrance National Agency Check

EOC
Emergency Operations Center

EOD
explosive ordnance disposal

FAA
Federal Aviation Administration

FBI
Federal Bureau of Investigation

FISO
Force Integration Staff Officer

FM
field manual

FMS
foreign military sales

FOA
field operating agency

FOB
free on board

FSC
Federal supply classification

FY
fiscal year

GBL
Government bill of lading

GOCO
Government-owned, contractor-operated

GOGO
Government-owned, Government-operated

GS
greater security

GSA
General Services Administration

GT
general technical aptitude area

GTR
Government transportation request

HQDA
Headquarters, Department of the Army

HQMC
Headquarters, United States Marine Corps

HSP
high security padlock

HUMINT
human intelligence

ID
identification

IDS
intrusion detection system

IED
improvised explosive device

IES
Illuminating Engineering Society

ILS
integrated logistic support

INSCOM
U.S. Army Intelligence and Security Command

ITO
installation transportation office(r)

JCS
Joint Chiefs of Staff

JMSNS
Justification for Major System New Start

JROTC
Junior Reserve Officers' Training Corps

JRWG
Joint Requirements Working Group

J-SIIDS
Joint-Service Interior Intrusion Detection System

JTAG
Joint Test Advisory Group

LAW
light antitank weapon

LCC
life cycle cost

LEA
law enforcement activity

LEC
law enforcement command

LIN
line item number

LOA
letter of agreement

LOI
Letter of Instruction

LR
letter requirement

LTC
lieutenant colonel

LTL
less than truckload

MAC
Military Airlift Command

MACOM
major Army command

MAJ
major

MATCU
military air traffic coordinating unit

MCA
major construction, Army

MEDCEN
U.S. Army Medical Center

MEDDAC
medical department activity

MEVA
mission essential or vulnerable area

MHE
materials handling equipment

MI
military intelligence

MILPO
military personnel office

MILSPEC
military specification

MILSTRIP
military standard requisitioning and issue procedures

MILVAN
military-owned demountable container

MIPR
military interdepartmental purchase request

MOS
military occupational specialty

MP
military police

MPA
military personnel, Army

MPI
Military Police Investigator

MSC
major subordinate command; Military Sealift Command

MSD
maximum stress diet

MSR
main supply route

MTOE/TDA
modified table of organization and equipment/table of distribution and allowances

MTMC
Military Traffic Management Command

MTX
Military Traffic Expediting Service

MUSAREC
major U.S. Army Reserve command

MWD
military working dog

NAF
non-appropriated fund

NATO
North Atlantic Treaty Organization

NBC
nuclear, biological, and chemical

NBS
National Bureau of Standards

NCDD
narcotics/contraband detector dog

NCEL
Naval Civil Engineering Laboratory

NCIC
National Crime Information Center

NCO
noncommissioned officer

NCOIC
noncommissioned officer in charge

NDA
National Defense Area

NDI
nondevelopmental item

NGR
National Guard regulation

NIS
Naval Investigative Service

NSN
national stock number

OACSI
Office of the Assistant Chief of Staff for Intelligence

OCE
Office of the Chief of Engineers

OCIE
organizational clothing and individual equipment

OCONUS
outside continental United States

OCPA
Office of the Chief of Public Affairs

ODCSLOG
Office of the Deputy Chief of Staff for Logistics

ODCSOPS
Office of the Deputy Chief of Staff for Operations

ODCSPER
Office of the Deputy Chief of Staff for Personnel

ODUSDP
Office of the Deputy Under Secretary of Defense for Policy

OJT
on-the-job training

OMA
Operation and Maintenance, Army

OMAR
Operation and Maintenance, Army Reserve

OPA
Other Procurement, Army

OPLAN
operation plan

OPM
Office of Personnel Management

OPSEC
operations security

OSD
Office of the Secretary of Defense

pam
pamphlet

PAO
public affairs officer

PAP
personnel assistance point

PARR
Program Analysis Resource Review

PCP
phencyclidine

PCS
permanent change of station

PDIP
Program Development Increment Package

PECIP
Productivity Enhancing Capitol Investment Program

PERSCOM
U.S. Total Army Personnel Command

PIF
productivity investment funding

PM
product manager; program manager; project manager; provost marshal

POC
point of contact

POD
port of debarkation

POE
port of embarkation

POL
petroleum, oils, and lubricants

POV
privately-owned vehicle

PPBES
Planning, Programming, Budgeting, and Execution System

PS
physical security

psi
pounds per square inch

PSC
physical security councils

PSE
physical security equipment

PSEAG
Physical Security Equipment Action Group

PSI
physical security inspector

PSS
Protective Security Service

PT
physical training

QPL
qualified products list

QRIP
Quick Return on Investment Program

RAM
reliability, availability, and maintainability

RAM-D
reliability, availability, maintainability, and durability

RC
Reserve component

RCS
reports control symbol

RDA
research, development, and acquisition

RDT&E
research, development, test, and evaluation

RDX
research department explosive

RESHIP
report of shipment

RF
radio frequency, response forces

RFP
request for proposal

ROC
required operational capability

ROTC
Reserve Officers' Training Corps

RSS
Rail Surveillance System

SCIF
sensitive compartmented information facilities

SECDEF
Secretary of Defense

SF
standard form

SFC
sergeant first class

SGA
standards of grade authorization

SJA
Staff Judge Advocate

SIR
serious incident report

SOFA
Status of Forces Agreement

SOP
standing operating procedure

SQT
skills qualification test

SRT
special reaction team

SSG
staff sergeant

SSN
social security number

SSS
Signature Security Service

SSSC
self-service supply center

TAADS
The Army Authorization Documents System

TAG
The Adjutant General

TASA
television audio support activity

TASC
training and audiovisual support center

TB
technical bulletin

TC
training circular

TCE
Technical Center of Expertise

TCP
traffic control point

TDA
tables of distribution and allowances

TDP
technical data package

TDY
temporary duty

THC
tetrahydrocannabinol

THREATCON
terrorist threat condition

TISA
Troop Issue Subsistence Activity

tl
truckload

TM
technical manual

TMDE
test, measurement, and diagnostic equipment

TMF
threat management force

TNT
trinitrotoluene

TOFC
trailer-on-flatcar

TOVEX
water gel (explosive)

TRADOC
U.S. Army Training and Doctrine Command

TSG
The Surgeon General

TSRWG
Tri-Service Requirements Working Group

TTS
technical training squadron

TTG
technical training group

TTW
technical training wing

UCMJ
Uniform Code of Military Justice

UL
Underwriter Laboratories

USACE
U.S. Army Corps of Engineering

USACIDC
United States Army Criminal Investigation Command

USAF
United States Air Force

USAISC
U.S. Army Information Systems Command

USAMPS
U.S. Army Military Police School

USAR
U.S. Army Reserve

USAREUR
U.S. Army, Europe, and Seventh Army

USC
United States Code

USMA
United States Military Academy

USS
United States standard

WSM-PSE
Weapons Systems Manager-Physical Security Equipment

WSN
weapon serial number

WTCA
Water Terminal Clearance Authority

Section II
Terms

Access (when pertaining to a restricted area or CCI)
Personnel movement within a restricted area that allows the chance for visual observation of, or physical proximity to, either classified or protected materiel. It is also the ability and opportunity to obtain detailed knowledge of CCI through uncontrolled physical possession. External viewing or escorted proximity to CCI does not constitute access.

Aggressor
Any person seeking to compromise an asset. Aggressor categories include criminals, terrorists and protestors.

Ammunition
A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame, for use in connection with defense or offense, including demolition. Excluded from this definition are devices charged with chemical agents defined in JCS Pub. 1 and nuclear or biological materiel. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition and caliber .22 ammunition are excluded.

Antiterrorism
Defensive measure used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by military forces.

Armed Guard Surveillance
A service that provides armed guards to maintain constant and specific surveillance of shipments for which the service is requested. “Armed” is defined as having a firearm and appropriate ammunition readily available for immediate use. (DOD 5100.76–M)

Arms
A weapon included in AR 190–11, appendix A, that will or is designated to expel a projectile or flame by the action of the explosive, and the frame or receiver of any such weapon.

Asset
Any resource requiring protection.

Aviation Facility
A department of the Army activity or area collocated with facilities for the takeoff and landing of aircraft. The facility has the mission of command and control of administrative, operational, training, and/or logistical support of Army aviation.

Badge
A security credential that is worn on the possessor's outer garment and validates (his or her) authority for access to a restricted area.

Bulk Storage
Storage in a facility above the using or dispensing level specifically applicable to logistics warehouse and depot stocks. This applies to activities using controlled medical substances and items (such as pharmacies, wards, or clinics) only when a separate facility (building or room) is used to store quantities that exceed normal operating stocks.

Cable Seal Lock
A seal in which the cable is passed through the locking hardware of a truck trailer or railcar door and the bullet nose is inserted into the barrel and the end of the cable until securely anchored. Once locked any force exerted to separate the lockpoint from the lockbody will strengthen its connection. (DOD 5100.76–M)

Carrier Custodian
An employee who has been assigned responsibility for controlled shipments containing SECRET material by the carrier and who has been issued a personnel security clearance by the Government. (DOD 5100.76–M)

Certification
The process whereby a patrol or detector dog's and handler's proficiency is verified to be in compliance with minimum training standards.

Chains
Chains used to secure racks or containers will be of heavy-duty, hardened steel chain, welded, straight-link steel. The steel will be galvanized of at least 5/16-inch thickness or of equal resistance required to force, to cut, or break an approved low security padlock. An example of such a chain is Type 1, Grade C, Class 4 NSN 4010–0–149–5583, NSN 4010–00–149–5575, or NSN 4010–00–171–4427.

Closed Circuit Television
Television that serves a number of different functions, one of which is physical security. As it pertains to the field of physical security, CCTV is used to augment, not replace, existing intrusion detection systems (IDS) or security patrols. It is not used as a primary sensor, but rather as a means of assessing alarms. CCTV also may be used as a surveillance means, but if used in this way, it will augment, not replace, existing IDS.

Closed post
An army installation or activity to which ground and water access is controlled at all times by perimeter barriers with limited, manned entry control points.

Closed vehicle or equipment
A conveyance that is fully enclosed with permanent sides and a permanent top, with installed doors that can be locked and sealed. (DOD 5100.76–M)

Combatting Terrorism
Actions, including AT and CT, taken to oppose terrorism throughout the entire threat spectrum.

Commercial-type vehicle
A vehicle designed to meet civilian requirements, and used without major modifications, for routine purposes in connection with the transportation of supplies, personnel, or equipment.

Constant Surveillance Service
A service that is an integral part of the provisions of 49 CFR 397 (reference (b)) that a carrier must apply when transporting hazardous or Class A and B explosive materials. It provides constant surveillance over a shipment. The transporting conveyance containing the shipment must be attended at all times by a qualified representative of the carrier. A motor vehicle is "attended" when the person in charge of the vehicle is awake and not in a sleeper berth and

is within 100 feet of the vehicle, provided the vehicle is within the person's obstructed field of vision. The qualified representative "attending" the vehicle must:

a. Be aware of the nature of the material contained in the vehicle.
b. Have been instructed on procedures to follow in case of emergency.
c. Be authorized to move the vehicle and have the means and capability to do so.

Note. CSS does not include a signature and tally service as provided under Signature Security Service (SSS). (DOD 5100.76–M)

Container Express
A reusable container for shipment of troop support cargo, quasi-military cargo, household goods, and personal baggage.

Containerization
A box or other device in which a number of packages are stored, protected, and handled as a unit in transit; for example, CONEX, MILVAN, and SEAVAN. This term also refers to the shipping system based on large cargo-carrying containers that can be easily interchanged between trucks, trains, and ships, without rehandling of contents. (DOD 5100.76–M)

Container on a flat car
A large box-like demountable body without undercarriage used to transport cargo that is mounted on a railroad flat car. (DOD 5100.76–M)

Constant Surveillance
Observing or protecting a storage facility containing AA&E by a human, intrusion detection system, closed circuit television, or combination, to prevent unobserved access, or make known any unauthorized access to the protected facility.

Continuous Surveillance
Constant unobstructed observance of items or an area to prevent unauthorized access. Continuous surveillance may be maintained by dedicated guards, other on-duty personnel, or intrusion detection systems and those enhanced by closed-circuit television.

Controlled Area
See restricted area.

Controlled cryptographic item
A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but is controlled.

Controlled medical substance
A drug or other substance, or its immediate precursor, listed in current schedules of 21 USC 812 in medical facilities for the purpose of military treatment, therapy, or research. Categories listed in this section are narcotics, amphetamines, barbiturates, and hallucinogens.

Counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism.

Crime analysis
The process used to determine the essential features of a criminal act. It is a mandatory part of any crime prevention program.

Crime prevention
The anticipation, recognition, and appraisal of a crime risk, and initiation of some action to remove or reduce it. Crime prevention is a direct crime control method that applies to before-the-fact efforts to reduce criminal opportunity, protect potential human victims, and prevent property loss.

Crime prevention inspection
An on-site evaluation of the crime prevention program of a unit, section, office, or other facility.

Crime risk management
The development of systematic approaches to reduce crime risks.

Crisis management team
A team found at a major command or installation level. A crisis management team is concerned with plan, procedures, techniques, policies, and controls for dealing with terrorism, special threats, or other major disruptions occurring on Government installations and facilities. A crisis management team considers all aspects of the incident and establishes contact with the AOC.

Critical communications facility
A communications facility that is essential to the continuity of operations of the National Command Authority during the initial phases of national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

Cryptographic component
The embodiment of a cryptographic logic in either hardware or firmware form, such as a modular assembly, a printed circuit board, a microcircuit, or any combination of these.

Cryptographic equipment
Any equipment employing a cryptographic logic.

Cryptographic logic
A deterministic logic by which information may be converted to an unintelligible form and reconverted to an intelligible form. Logic may take the form of engineering drawings, schematics, hardware, or firmware circuitry.

Day gate
Any barriers, used in a doorway or entrance to pharmacy or medically sensitive item storage areas, that prevents unauthorized personnel access during operating hours. Such barriers normally are not the sole protection afforded the entrance during nonoperating hours; however, during operating hours, the barrier ensures positive entry control by on-duty personnel (for example, electronic buzzer control entry to the area after positive identification by receptionist or on-duty personnel).

Dedicated guards
Individuals charged with performing the primary task of safeguarding designated facilities, material, and personnel within a defined area during a tour of duty. A dedicated guard may perform this function as a static post. He or she remains within or on the perimeter of a protected area and maintains continuous surveillance over that which is being protected during the tour of duty.

Defense Transportation System
Consists of military controlled terminal facilities, Military Airlift Command (MAC) controlled airlift, Military Sealift Command (MSC) controlled or arranged sealift, and Government controlled air or land transportation. (DOD 5100. 76–M)

Demilitarization
The act of destroying the offensive or defensive characteristics inherent in certain types of equipment and materiel. The term comprehends mutilation, scrapping, burning, or alteration designed so as to prevent the further use of such equipment and materiel for its originally intended military or lethal purpose.

Double-locked container
A steel container of not less than 26 gauge which is secured by an approved locking device and which encases an inner container that also is equipped with an approved locking device. Cabinet, medicine, combination with narcotic locker, NSN 6530–00–702–9240, or equivalent, meets requirements for a double-locked container.

Dromedary
A freight box carried on and securely fastened to the chassis of the tractor or on a flat-bed trailer. The dromedary is demountable by the use of a forklift truck, is protected by a plymetal shield, and is equipped with doors on each side that may be locked with seals or padlocks. All explosive items carried in the dromedary must be compatible and in compliance with 49 CFR 177 (ref (c)) or host nation regulations. (DOD 5100.76–M)

Dual Driver Protective Service
A service requiring SSS plus continuous attendance and surveillance of the shipment through the use of two drivers.
a. The vehicle containing the shipment must be attended at all times by one of the drivers. A vehicle is attended

when at least one of the drivers is in the cab of the vehicle, awake, and not in a sleeper berth or is within 10 feet of the vehicle.

b. SSS signature and tally requirements are not required between the same pair of drivers for a particular movement. (DOD 5100.76–M)

Duress alarm system
A method by which authorized personnel can covertly communicate a situation of duress to a security control center or to other personnel in a position to notify a security control center. (DOD 5100.76–M)

Duress or holdup alarms
Devices which allow personnel on duty to transmit a signal to the alarm monitoring station from which an armed response force can be dispatched if a holdup or a duress situation occurs.

Emergency Aircraft
An aircraft designated by the commander to respond to emergency situations and provide life-saving and property-saving services. Normally, such aircraft has special equipment and markings. Air Ambulances and firefighting aircraft are examples.

Emergency vehicle
A vehicle designated by the commander to respond to emergency situations and provide life-saving and property-saving services. Normally, the vehicle has special equipment and markings. Ambulances and firefighting and military or security police vehicles are examples.

Enclosed vehicle or equipment
A conveyance that is fully enclosed with permanent sides and permanent top, with installed doors that can be locked and sealed.

Entry control (when pertaining to a restricted area)
Security actions, procedures, equipment, and techniques, employed within restricted areas to ensure that persons who are present in the areas at any time have authority and official reason for being there.

Escorted personnel (when pertaining to a restricted area)
Those persons authorized access to a restricted areas who are escorted at all times by a designated person.

Escorts and couriers
Military members, U.S. civilian employees, or DOD contractor employees responsible for the continuous surveillance and control over movements of classified material. Individuals designated as escorts and couriers must possess a Government-issued security clearance at least equal to that of the material being transported.

Exception
An approved permanent exclusion from specific requirements of this regulation. Exceptions will be based on a case-by-case determination and involve unique circumstances which make conformance to security standards impossible or highly impractical. An exception can also be an approved permanent deviation from the provisions of this regulation. There are two types of exceptions:

a. Compensatory Measures Exception. This is a deviation in which the standards are not being met, but the DOD component (HQDA(DAMO–ODL–S) concerned determines it is appropriate, because of physical factors and operational requirements. Compensatory measures are normally required.

b. Equivalent Protection Exception. This is a deviation in which nonstandard conditions exist, but the totality of protection afforded is equivalent to or better than that provided under standard criteria.

Exclusion area
See restricted area.

Exclusive use
A conveyance unit or vehicle that is used only for a shipment from origin to destination without transfer of lading, and that permits locking of the unit and use of seals. (DOD 5100.76–M)

Explosives
Any chemical compound, mixture or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives (dynamite,

trinitrotoluene (TNT), C–4, and other high explosives), and other explosives consisting of 10 pounds or more; for example, gunpowder or nitroguanidine.

Facility
Any single building, project, or site.

Force Protection
Security program developed to protect soldiers, civilian employees and family members, facilities and equipment, in all locations and situations. This is accomplished through the planned integration of combatting terrorism, physical security, operations security, protective services and law enforcement operations, all supported by foreign intelligence, counterintelligence and other security programs.

Greater security (GS)
A seal tracing and inspection rail service for unclassified sensitive cargo that includes a military traffic expending (MTX) service and provides:

a. Inspection of railcars at major terminals by railroad personnel for evidence of forced entry or tampering with seals or security devices.

b. Name of carrier reporting.

c. Time of inspection; that is, a.m. or p.m.

d. Actual arrival and actual departure time from inspection terminal. (DOD 5100.76–M)

Handler
A military police person or DOD civilian guard or police person who has been qualified by training and certification to care for, train, and employ a military working dog.

Handling
Controlled physical possession without access.

High risk personnel
Personnel who, by their grade, assignment, value, location, or specific threat, are more likely to be attractive or accessible terrorist targets.

Independent power source
A power source, normally battery, independent of any other source (DOD 5100.76–M)

Industrial and utility equipment
Equipment used in the manufacture or in support of the manufacture of goods and equipment used to support the operation of utilities such as power and water distribution and treatment.

In flight
The condition of an aircraft from the moment when all external doors are closed following embarkation until the moment when one such door is opened for disembarkation.

Installations
Such real properties as reserve centers, depots, arsenals, ammunition plants (both contractor- and Government-operated, hospitals, terminals, and other special mission facilities, as well as those used primarily by troops. (See also JCS Pub. 1)

Internal controls (when pertaining to a restricted area)
Security actions, procedures, and techniques employed within restricted areas to ensure persons who are present in these areas at any time have authority and official reason.

Intrusion detection system
The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system and reporting directly to an alarm monitoring station. The IDS will be an approved DOD standardized system, such as the Joint Service Interior Intrusion Detection System or MACOM-approved commercial equipment.

Justification for Major System New Start
A requirement document that the combat developer prepares with the material developer, training developer, manpower

and personnel planner, and logistician. A JMSNS is prepared to describe the mission need and justifies the acquisition of a major new system at program initiation in the acquisition cycle.

Kennel facilities

The buildings, the kennels, the runs, and the exercise and training areas which are used to house, care for, and train military working dogs.

Key and lock control system

A system of identifying both locks and their locations and personnel in possession of keys and/or combinations.

Keying

The process of establishing a sequence of random binary digits used to initially set up and periodically change permutations in cryptographic equipment for purpose of encrypting or decrypting electronic signals, for controlling transmission security processes, or for producing other keys.

King Tut block

A King Tut block is a specially designed large concrete block. It is placed in front of an igloo or magazine entrance with a fork lift. Access to the igloo or magazine therefore requires a fork lift to move the block. The King Tut block is of sufficient weight to prevent removal without a fork lift.

Letter of agreement

A document jointly prepared and signed by the combat and materiel developers when a potential materiel system need has been identified and it has been determined that one or more technological approaches may satisfy the need. Even though it may be in an early stage of development, the LOA will address the materiel system from the Total System Management standpoint. The LOA describes operational, technical, training, personnel, and logistical system unique events that must be undertaken to produce the total system.

Letter requirement

An abbreviated procedure for acquisition of low-unit cost, low-risk developmental, or commercial items. It will be used instead of the ROC when applicable. The total system definitive requirements for training, personnel, and logistics requirements are the same for the LR as for the ROC. The LR is jointly prepared by TRADOC and AMC.

Lightweight construction

Building construction other than reinforced concrete or masonry (concrete block or clay brick) such as wood or metal siding.

Limited access post

An Army installation or activity that meets one of the criteria below:

a. No permanent fences or other physical barriers exist, but entry can be temporarily closed to vehicular traffic and other movements using roads and other conventional points of entry.

b. Permanent perimeter barriers exist and access is controlled only after normal duty hours; for example, gates are secured or manned with guards after dark.

c. No permanent perimeter barriers exist, but vehicular traffic and other movements using roads and other conventional points of entry are continuously controlled.

Limited area

See restricted area.

Locked container

A container or room of substantial construction secured with an approved locking device. For pharmacy operating stocks, lockable automated counting systems meet requirements for a locked container.

Locking devices

a. Padlocks, military specifications MIL–P–43607 (High Security Padlock); shrouded shackle, NSN

5340–01–217–5068 or horizontal sliding bolt, NSN 5340–00–799–8248) or MIL–P–43951 (medium security padlock; regular shackle, NSN 5340–00–799–8016).

b. Padlocks, Commercial Item Description A–A–1927 (low security padlock) having a hardened steel shackle and body; NSN 5340–00–158–3807 (with chain), NSN 5340–00–158–3805 (without chain).

c. GSA-approved changeable three-position padlock, Federal Specification FF–P–110.

d. High security hasps. Military Specifications MIL–H–43905 or MIL–H–29181A.

e. Hasps and staples for low-security padlocks which are of heavy pattern steel, securely fastened to the structure with smooth-headed bolts, rivets, or welding to prevent removal.

Locks

Locks should be considered as delay devices only, not as positive bars to unauthorized entry, since any lock can be defeated by expert manipulation or force.

a. Padlocks

High security padlocks: Military Specification MIL–P–43607, shrouded shackle with clevis and chain, NSN 5340–01–217–5068 or NSN 5340–00–188–1560; horizontal sliding bolt with clevis and chain, NSN 5340–00–799–8248.

Medium security padlocks: Military Specification MIL–P–43951, open shackle with clevis and chain, NSN 5340–00–799–8016. Authorized for continued use to secure Categories III and IV AA&E only until stocks are depleted or replaced.

Low security padlocks: Commercial Item Description A–A–1927, hardened steel shackle and case, without chain: NSN 5340–00–158–3805; with chain: NSN 5340–00–158–3807.

(Any questions regarding the above specifications will be addressed to the DOD Lock Program Technical Manager, Naval Facilities Engineering Service Center, Code C66, 560 Center Drive, Port Hueneme, CA 93043–4328 (DSN 551–1567 or –1212).

b. Certain locks, such as high or medium security padlocks, provide excellent protection when used in conjunction with a high security hasp. Hasps installed for protection of AA&E will provide protection comparable to that given by the lock used. Determination of "comparable protection" will be addressed to the DOD Lock Program Technical Manager, Naval Civil Engineering Laboratory, Code L56, 560 Center Drive, Port Hueneme, CA 93043–4328 (DSN 551–1567 or –1212).

NAPEC high security shrouded hasp (MIL–H–29181A) is approved for use with the high security padlock to secure all categories of AA&E. The hasp has a cover that protects the lock from cutting or hammer tools and inclement weather. It should be used to secure Category I and II AA&E storage facilities. When replacement of a hasp on Category III, IV or uncategorized AA&E is necessary, this hasp should also be used. The Natick high security hasp (MIL–H–43905) is a high security hasp that also is approved for protection of Category III and IV AA&E when used with an approved high security padlock.

Hasp, pin-type, locking "T" is a hasp that was authorized previously to secure ammunition storage magazines. Magazines were secured using the installed locking bar in conjunction with a "T" pin and high security padlock. The locking "T" hasp does not provide adequate security for sensitive AA&E. It must be replaced with a high security hasp to enhance security. It will not be used to secure Category I and II ammunition storage facilities.

c. Another lock is the cable seal lock. Once locked, any force exerted to separate the lockpoint from the lockbody strengthens the connection. Such locks are not approved for use in securing storage facilities containing AA&E. The same restriction applies to d below.

d. A complementary device to locks is the No. 5 American Wire Gauge wire twist. This is a U-shaped wire place in the hasp along with the shackle and twisted tightly in place. Another device is a wire cable of a thickness equivalent to or larger than No. 5 wire. This is placed through the hasp, a metal sleeve slipped over it, and crimped into place.

e. Built-in combination locks, meeting Underwriters Laboratories Standard 768, Group 1 (NSN 5340–01–375–7593) are approved for use on GSA-approved Class 5 vault doors and GSA-approved Class 5 weapons containers storing unclassified material and unclassified AA&E.

LOGAIR

Long-term contract airlift service within the continental United States for the movement of cargo in support of the logistics system of the Military Services (primarily the Army and Air Force) and Defense Agencies. (DOD 5100.76–M)

Major disruption on installations

Acts. Threats, or attempts to commit such acts as kidnapping, extortion, bombings, hijackings, ambushing, major weapons thefts, arson, assassination, and hostage taking on a military installation. These acts that have potential for widespread publicity require special response, tactics, and management.

Medically sensitive items

Standard and nonstandard medical items designated by medical commanders to be sufficiently sensitive to warrant a

stringent degree of physical security and accountability in storage. Included within this definition are all items subject to misappropriation and/or misuse such as needles and syringes.

Military Traffic Expediting (MTX) Service
A service providing for movement from origin to destination in the shortest time possible for specifically identified rail shipments, and which is required for the shipment of firearms and other sensitive shipments. This service uses electrical communications between members of the Association of American Railroads, is available for either single line haul or jointline movements, and provides progress reports as required. (DOD 5100.76–M)

Military van (MILVAN)
Military-owned demountable container, conforming to U.S. and international standards, operated in a centrally controlled fleet for movement of military cargo. (DOD 5100.76–M)

Military working dog
Dogs required by the using DOD component for a specific purpose, mission, or combat capability. MWDs include patrol, patrol and narcotic/contraband, and patrol and explosive detector dogs.

Military working dog team
The MWD and its appropriately qualified, assigned handler.

Mission-critical personnel
Personnel who are essential to the operation of an organization of function.

Mission essential and vulnerable areas
Facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful accomplishment of the installation's State National Guard, or MUSARC mission. This includes areas nonessential to the installation's/facility's operational mission but which, by nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.

Motor pool
A group of motor vehicles used as needed by different organizations or individuals and parked in a common location when not in use. On an Army installation, a nontenant Army activity with 10 or less assigned commercial-type vehicles but no local organizational maintenance support does not have a motor pool, under this regulation, even though the vehicles are parked together.

Motor vehicle
A self-propelled, boosted, or towed conveyance used to transport a burden on land. This includes all Army wheeled and track vehicles, trailers, and semitrailers, but not railroad locomotives and rolling stock.

National Defense Area
An area set up on non-Federal lands located within the United States, its possessions or territories, to safeguard classified defense information or DOD equipment or materiel. Establishment of a National Defense Area temporarily places such non-Federal lands under the effective control of DOD and results only from an emergency event.

Negotiations
A dialogue between authorities and offenders which has as the ultimate goal for the safe release of hostages and the surrender of the offenders.

Note C controlled medical items
Sets, kits, and outfits containing one or more component Note Q or Note R items.

Note Q controlled medical items
All standard drug items identified as Note Q in the Federal Supply Catalog, Nonstandard Drug Enforcement Administration (DEA) Schedule III, IV, V Controlled Substances.

Note R controlled medical items
All items identified as Note R in the Federal Supply Catalog, Nonstandard DEA Schedule II Controlled Substances.

One dog-one handler
The concept that each MWD will have only one handler. Personnel shortages may necessitate assigning a handler responsibility for more than one dog. However, two or more handlers cannot handle the same dog.

Open post
Installations or activities that do not qualify as closed or limited access posts. Access to the installation or activity is not controlled during or after normal duty hours.

Perimeter fence
Fences for the security of unclassified, non-sensitive items that meet the requirements of U.S. Army Corps of Engineers Drawing Code STD 872–90–00 Series. The minimum height will be 6 feet. Use of NATO Standard Design Fencing is also authorized.

Perimeter wall
Any wall over 6 feet tall which delineates a boundary and serves as a barrier to personnel and/or vehicles. These walls may be constructed of reinforced concrete, masonry, or stone.

Physical protective measures
Physical security measures used to counter risk factors that usually do not change over a period of time such as mission impact, cost, volume, and criticality of resources and vulnerabilities. The measures are usually permanent and involve expenditure of funds.

Physical security
That part of the Army security system, based on threat analysis, concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, materiel, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft. Operations security (OPSEC) and security targeted against traditional criminal activity are included.

a. Physical security procedures include, but are not limited to, the application of physical measures to reduce vulnerability to the threat; integration of physical security into contingency, mobilization, and wartime plans; the testing of physical security procedures and measures during the exercise of these plans; the interface of installation OPSEC, crime prevention and physical security programs to protect against the traditional criminal; training of guards at sensitive or other storage sites in tactical defense against and response to attempted penetrations; and creating physical security awareness.

b. Physical security measures are physical systems, devices, personnel, animals, and procedures employed to protect security interests from possible threats and include, but are not limited to, security guards; military working dogs; lights and physical barriers; explosives and bomb detection equipment; protective vests and similar equipment; badging systems; electronic entry control systems and access control devices; security containers; locking devices; electronic intrusion detection systems; standardized command, control, and display subsystems; radio frequency data links used for physical security; security lighting; delay devices; artificial intelligence (robotics); and assessment and/or surveillance systems to include closed-circuit television. Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans.

Physical security equipment
A generic term for any item, device, or system that is used primarily to protect Government property, including nuclear, chemical, and other munitions, personnel, and installations, and to safeguard national security information and material, including the destruction of such information and material both by routine means and by emergency destruct measures.

a. Interior physical security equipment. Physical security equipment used internal to a structure to make that structure a secure area. Within DOD, DA is the proponent for those functions associated with development of interior physical security systems.

b. Exterior physical security equipment. Physical security equipment used external to a structure to make the structure a secure area. Within DOD, the Department of the Air Force is the proponent for those functions associated with the development of external physical security systems; however, the Army will develop lights, barriers, and robotics.

c. Intrusion detection system. See previous definition.

Physical security inspection
A formal, recorded assessment of physical procedures and measures implemented by a unit or activity to protect its assets.

Physical security measures
See physical security.

Physical security plan
A comprehensive written plan providing proper and economical use of personnel, land, and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

Physical security procedures
See physical security.

Physical security program
The interrelationship of various components that complement each other to produce a comprehensive approach to security matters. These components include, as a minimum, the physical security plan; physical security inspections and surveys; participation in combatting terrorism committees and fusion cells; and a continuing assessment of the installation's physical security posture.

Physical security resource plan
Plan developed by the physical security officer that identifies physical security needs, and shows proposed programmed procurement of those needs.

Physical security survey
A formal, recorded assessment of the installation physical security program.

Physical security system architecture
A system ensuring that IDS components designed by the various services are compatible when used together. The Air Force is responsible for systems architecture.

Pier service
Ocean carrier booking is restricted over ocean movement from port of embarkation (POE) to port of debarkation (POD). It precludes prearranged-through-booking employing surface transportation to inland destinations. (DOD 5100. 76–M)

Pilferable assets
Any asset which can be stolen and which does not fall under the other asset categories discussed in this publication.

Pilferage-coded items
Items with a code indicating that the material has a ready resale value or civilian application and, therefore, is especially subject to theft.

Portable
Capable of being carried in the hand or on the person. As a general rule, a single item weighing less than 100 pounds (45.34 kilograms) is considered portable.

Primary electrical power source
That source of power, either external (commercial) or internal, that provides power to site facilities on a daily basis. (DOD 5100.76–M)

Protection in depth
A system providing several supplementary security barriers. For example, a perimeter fence, a secure building, a vault, and a locked container provide four layers of protection. (DOD 5100.76–M)

Protective layer
Any envelope of building components which surrounds an asset and delays or prevents aggressor movement toward the asset or which shields the asset from weapons and explosives effects.

Protective Security Service
A service to protect shipments. PSS involves a transporting carrier that must be a "cleared carrier" under provisions of DOD 5220.22–R, paragraph 1–702.a (ref (d)). A shipment must be under the constant surveillance of designated carrier employees, unless it is stored in containers or an area approved by the cognizant Defense Investigative Service regional

office. The designated carrier employees providing constant surveillance when PSS is required must possess a Government-issued SECRET clearance and a carrier-issued identification. (DOD 5100.76–M)

QUICKTRANS
Long-term contract airlift service within the continental United States (CONUS) for the movement of cargo in support of the logistic system for the Military Services (primarily the Navy and Marine Corps) and Defense agencies. (DOD 5100.76–M)

Rail Surveillance Service
An inspection service of rail shipments. An inspection is made within one hour after each stop, if the trailer containing a shipment remains at a halt. Reinspection is made a minimum of once each hour, as long as the railcar containing the shipment remains at a halt. (DOD 5100.76–M)

Report of Shipment
An advanced report furnished by message or telephone immediately upon dispatch of a shipment within CONUS for domestic shipments. A report goes to both Water Terminal Clearance Authority (WTCA) and the water port transshipping facility for surface export shipments, or to the Military Air Traffic Coordinating Officer (MATCO) for air export shipments. The advance notice of shipments shall include the following applicable data:

a. For domestic shipments, see AR 55–355/NAVSUPINST 4600.70/AFM 75–2/MCO P4600.14A/DLAR 4500.3, Routing Instruction Note (RIN) 146, Appendix L (reference (e)).

b. For export shipments, see chapter 4, DOD 4500.32–R (reference (f)). (DOD 5100.76–M)

Required operational capability
A requirements document that the combat developer prepares with input from the training developer in coordination with the material developer, logistician, and manpower and personnel planner. The ROC is a concise statement of the minimum essential operational, RAM, technical, personnel and manpower, training, safety, health, human factors engineering, logistical, and cost information to start full scale development or procurement of a material system.

Restricted area
Any area to which entry is subject to special restrictions or control for security reasons or to safeguard property or material. This does not include those designated areas over which aircraft flight is restricted. Restricted areas may be of different types. The type depends on the nature and varying degree of importance, from a security standpoint, of the security interest or other matter contained therein.

a. Exclusion area. A restricted area containing—

(1) A security interest or other matter of such nature that access to the area constitutes, for all practical purposes, access to such security interests or matter; or—

(2) A security interest or other matter of such vital importance that proximity resulting from access to the area is treated equal to (1) above.

b. Limited area. A restricted area containing a security interest or other matter, in which uncontrolled movement will permit access to such security interest or matter; access within limited areas may be prevented by escort and other internal restrictions and controls.

c. Controlled area. That portion of a restricted area usually near or surrounding an exclusion or limited area. Entry to the controlled area is restricted to authorized personnel. However, movement of authorized personnel within this area is not necessarily controlled. Mere entry to the area does not provide access to the security interest or other matter within the exclusion or limited area. The controlled area is provided for administrative control, safety, or as a buffer zone for security in depth for the exclusion or limited area. The proper commander establishes the degree of control of movement.

Ride awhile-walk awhile method
A law enforcement or security patrolling technique. The MWD team patrols for a period of time in a vehicle and then dismounts for an appropriate period of time to patrol an area on foot. This method increases the potential area the team can cover, as well as allowing the team to concentrate their foot patrols in especially critical areas.

Risk
The degree or likelihood of loss of an asset. Factors that determine risk are the value of the asset to its user in terms of mission criticality, replaceability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the asset to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the asset.

Risk analysis
Method of examining various risk factors to determine the risk value of likelihood of resource loss. This analysis will be used to decide the level of security warranted for protection of resources.

Risk factors
Elements that make up the total degree of resource loss liability. Factors to be considered in a risk analysis include the importance of the resource to mission accomplishment; the cost, volume, criticality and vulnerabilities of the resources; and the severity of threats to the resources.

Risk level
An indication of the degree of risk associated with an asset based on risk analysis. Risk levels may be Levels I, II, or III, which correspond to low, medium, and high.

Risk value
Degree of expectation or likelihood of resource loss. The value may be classified as low, medium, or high.

Safe
A GSA Class 5 Map and Plans Security Container, Class 6 Security Filing Cabinet or refrigerator or freezer, secured with an approved locking device and weighing 500 pounds or more, or secured to the structure to prevent removal.

Schedule I drug
Any drug or substance by whatever official name (common, usual, or brand name) listed by the DEA in Title 21 of the Code of Federal Regulations, chapter II, Section 308.11, intended for clinical or non-clinical use. A list of Schedule I drugs and substances is contained in AR 40-7, appendix A.

Seal
A device to show whether the integrity of a shipment has been compromised. Seals are numbered serially, are tamperproof, and shall be safeguarded while in storage. The serial number of a seal shall be shown on Government Bills of Lading (GBL). A cable seal lock provides both a seal and locking device.

Sealed containers
Wooden boxes, crates, metal containers, and fiber containers sealed in a way to show when the containers are tampered with after sealing. The method of sealing depends of the type of construction of the containers. Sealing may be by metal banding, nailing, airtight sealing, or wax dripping (for fiber containers). In key control, a sealed container is also a locked key container or a sealed envelope containing the key or combination to the key container.

Sealed protection
A container or an area enclosed by a plastic or soft metal device which is opened easily without the use of a key or combination.

SEAVAN
A commercial, Government-owned or leased shipping container and without bogey wheels attached that is moved by ocean transportation and must be lifted on and off the ship. (DOD 5100.76–M)

Security card
An official distinctive identification (pass or card) that identifies and authorizes the possessor to be physically present in a U.S. Army designated restricted area.

Security engineering
The application of engineering principles to the protection of assets against various threats through the application of construction and equipment application.

Security lighting
The amount of lighting necessary to permit visual surveillance by security police or by supervisory personnel.

Security procedural measures
Physical security measures to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. The procedures can usually be changed within a short amount of time and involve manpower.

Sensitive conventional arms, ammunition, and explosives
See categorization of such items in appendix A, AR 190–11.

Sensitive items
Material requiring a high degree of protection to prevent unauthorized acquisition. This includes arms, ammunition, explosives, drugs, precious metals, or other substances determined by the Administrator, Drug Enforcement Administration to be designated Schedule Symbol II, III, IV, or V under the Controlled Substance Act of 1970.

Signal intelligence
Intelligence derived from communications means (such as telephone, telegraph, radio), electronic signal emitters (such as navigation radar, identification friend or foe, and weapons guidance devices) and instrumentation signals (such as telemetry and beaconry).

Signature Security Service
A service designed to provide continuous responsibility for the custody of shipments in transit. A signature and tally record is required from each person responsible for the proper handling of the shipment at specified stages of its transit from origin to destination.

a. The initial signature on the signature and tally record should be the same as that of the carrier's agent on the GBL. When SSS is used in conjunction with DDPS, both drivers in each pair of drivers shall sign the signature and tally record when that pair assumes responsibility for the shipment.

b. Commercial carriers offering SSS must be able to trace a shipment in less than 24 hours. The following forms shall be used to obtain SSS:

(1) *Surface shipments.* DD Form 1907 (Signature and Tally Record) shall accompany every surface shipment of classified or protected material accorded a signature and tally service by surface commercial carriers. Carrier tariffs and tenders may describe this type of service under different titles for example, Hand-to-Hand Signature Service or Signature Service.

(2) *Commercial air shipments.* The air industry internal Form AC–10 (Airlines Signature Service Record) shall be used by regulated and nonscheduled airlines to obtain the signature and tally record. Air taxi operators and air freight forwarders providing SSS may use DD Form 1907 instead of AC–10. No receipt is required from the flight crew or attendants while the aircraft is in flight. A signature and tally record is required; however, from air carrier personnel whenever the aircraft is on the ground and access to the cargo compartment containing the sensitive arms, ammunition, and explosives (AA&E) is available for any purpose. A signature and tally record is also required from pickup and delivery carriers used by the airlines for such purposes.

(3) *Military air shipments.* The AF Form 127 (Traffic Transfer Receipt) or similar document, will be used to provide hand-to-hand receipt control for sensitive and classified shipments being transferred in the DTS. (DOD 5100. 76–M)

Steel bar
A flat bar, 3/8 inch by one inch minimum; or round bar 1/2 inch diameter minimum.

Steel mesh
High carbon, manganese steel not less than 15/100 inch (8-gauge) in thickness, and a grid of not more than two inches center to center.

Storage
Any area where AA&E are kept. Storage does not include items in process of manufacture, in use, or being transported to a place of storage or use.

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

Tactics
The specific methods of achieving the aggressor's goals to injure personnel, destroy Army assets, or steal Army materiel.

Tactical vehicle
A vehicle with military characteristics designed primarily for use by forces in the field in direct connection with, or support of, combat or tactical operations, or the training of troops for such operations.

Tenant activity
A unit or activity of one Government agency, military department, or command that occupies facilities on an installation of another military department or command and that receives supplies or other support services from that installation.

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

Terrorism counteraction measures
Term used previously for combatting terrorism (see definition of this term).

Terrorist group
A politically, religious, or ideologically oriented group which uses terrorism as its prime mode of operations.

Threat management force
An action force from the installation that responds to major disruptions on installations. The TMF should be of sufficient size to manage the disruption and will usually involve a command element, security element, negotiation team, SRT, and logistical element.

TOW
A tube-launched, optically traced, wire-command missile designed as an antitank weapon system. (DOD 5100.76–M)

Upper rail loc
A set screw operated variation of a "C" clamp designed for gripping the upper sliding rail which supports or guides the weight of some styles of railroad boxcar doors. Gripping the upper sliding rail, the "loc" blocks and prevents the door's roller hangers or carriers from sliding past, thereby effectively preventing the door from being moved. (DOD 5100. 76–M)

Waiver
Temporary relief from specific standards imposed by this manual (regulation) pending actions accomplishment of actions that will conform to the standards required. Compensatory measures are required.

Section III
Special Abbreviations and Terms
There are no entries in this section.

Index

This index is organized alphabetically by topic and by subtopic within topic. Topics and subtopics are identified by paragraph number.

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.56

PIN: 002202–000
DATE: 09-27-01
TIME: 10:37:37
PAGES SET: 60

DATA FILE: ps4.fil
DOCUMENT: AR 190–13
DOC STATUS: REVISION