

**FOR OFFICIAL USE ONLY**

**Army Regulation 190-13**

**Military Police**

# **The Army Physical Security Program**

**Distribution Restriction Statement.**  
This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside the U.S. Government for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to the Office of the Provost Marshal General (DAPM-MPP-PS), 2800 Army Pentagon, Washington, DC 20310-2800.

**Destruction Notice.**  
Destroy by any method that prevents disclosure of contents or reconstruction of the document.

**Headquarters  
Department of the Army  
Washington, DC  
25 February 2011**

**FOR OFFICIAL USE ONLY**

# ***SUMMARY of CHANGE***

AR 190-13

The Army Physical Security Program

This major revision, dated 25 February 2011--

- o Adds responsibilities for the Provost Marshal General in developing and executing the Army Physical Security Program (chap 1, sec II).
- o Changes policy proponentcy for the Army Physical Security Program from the DCS, G-3/5/7 to the Provost Marshal General (para 1-8).
- o Provides guidance for directors, supervisors, and commanders of Army organizations not on military installations (para 1-20).
- o Establishes the security criteria deviation process (para 2-3).
- o Clarifies identification and prioritization of mission essential and vulnerable areas (para 2-7).
- o Prescribes use of the U.S. Army Military Police Security Management System (para 2-13).
- o Updates policy on the physical security survey, the physical security inspection, the report of action taken, and the security engineering survey (paras 2-14, 2-15, 2-16 and 2-18).
- o Revises the selection for physical security personnel and identifies required credentials to conduct physical security inspections and surveys (chap 3).
- o Updates policy for physical security resources, security identification cards and badges, and restricted areas (chaps 4, 5, and 6).
- o Establishes policy for physical security councils (para 7-2).
- o Reorganizes the Department of the Army Physical Security Review Board and the Army Physical Security Equipment Action Group (paras 7-3 and 7-4).
- o Establishes policy for installation access control, physical security equipment planning, and security forces (chaps 8, 9, and 10).
- o Revises installation and stand-alone facility physical security plans (app B).
- o Adds a baseline Internal Control Evaluation Checklist (app C).

# FOR OFFICIAL USE ONLY

Headquarters  
Department of the Army  
Washington, DC  
25 February 2011

\*Army Regulation 190–13

Effective 27 March 2011

## Military Police


### The Army Physical Security Program

---

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.  
*General, United States Army*  
*Chief of Staff*

Official:

  
JOYCE E. MORROW  
*Administrative Assistant to the*  
*Secretary of the Army*

**History.** This publication is a major revision.

**Summary.** This regulation implements DOD 5200.08–R and DODI 3224.03. It prescribes policies, procedures, and guidance to plan and implement the Department of the Army Physical Security Program. It provides general guidance concerning requirements for and use of physical security equipment; the appointment of physical security officers and inspectors; the conduct of physical security inspections and surveys; the management of physical security credentials; the management and use of identification cards and badges; restricted areas; access control for installations and stand-alone facilities; and security forces.

**Applicability.** This regulation applies to the active Army, the Army National Guard/Army National Guard of the United

States, and the U.S. Army Reserve, unless otherwise stated.

**Proponent and exception authority.** The proponent of this regulation is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

**Army internal control process.** This regulation contains internal controls and identifies key internal controls that must be evaluated (see appendix C).

**Supplementation.** Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Provost Marshal General (DAPM–MPP–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

**Suggested improvements.** Users are invited to send comments and suggested

improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Provost Marshal General (DAPM–MPP–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

**Committee Continuance Approval.**

The Department of the Army committee management official concurs in the establishment and/or continuance of the committee(s) outlined herein. AR 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the U.S. Army Resources and Programs Agency, Department of the Army Committee Management Office (AARP–ZX), 2511 Jefferson Davis Highway, 13th Floor, Taylor Building, Arlington, VA 22202–3926. Further, if it is determined that an established “group” identified within this regulation, later takes on the characteristics of a committee, as found in the AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

**Distribution.** This publication is available in electronic media only and is intended for command levels, C, D, and E for the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

---

**Distribution Restriction Statement.**

This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside the U.S. Government for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to the Office of the Provost Marshal General (DAPM–MPP–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

**Destruction Notice.**

Destroy by any method that prevents disclosure of contents or reconstruction of the document.

---

\*This regulation supersedes AR 190–13, dated 30 September 1993.

# FOR OFFICIAL USE ONLY

## Contents (Listed by paragraph and page number)

### Chapter 1

#### Introduction, page 1

##### Section I

General, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

##### Section II

Responsibilities, page 1

Assistant Secretary of the Army (Acquisition, Logistics, and Technology) • 1-4, page 1

Assistant Secretary of the Army for Civil Works • 1-5, page 1

Assistant Secretary of the Army (Installations, Energy and Environment) • 1-6, page 1

Assistant Secretary of the Army (Manpower and Reserve Affairs) • 1-7, page 1

Provost Marshal General • 1-8, page 1

Deputy Chief of Staff, G-1 • 1-9, page 2

Deputy Chief of Staff, G-2 • 1-10, page 2

Deputy Chief of Staff, G-3/5/7 • 1-11, page 2

Deputy Chief of Staff, G-4 • 1-12, page 2

Chief Information Officer/G-6 • 1-13, page 2

Assistant Chief of Staff for Installation Management • 1-14, page 2

The Inspector General • 1-15, page 2

The Surgeon General • 1-16, page 2

Chief of Engineers • 1-17, page 3

Commanding General, U.S. Army Corps of Engineers • 1-18, page 3

Commanding General, U.S. Army Training and Doctrine Command • 1-19, page 3

Directors and supervisors of Army staff agencies and commanders of Army organizations not on military installations • 1-20, page 4

Senior commanders • 1-21, page 4

Commanders and directors of Army commands, Army service component commands, direct reporting units, the Army National Guard, and U.S. Army Corps of Engineers divisions and districts • 1-22, page 4

Product manager, force protection systems • 1-23, page 5

Commanders of posts, camps, stations, installations, Army-managed Armed Forces Reserve Centers, Army Reserve Centers, Army National Guard Armories, and similar Army facilities subject to Department of the Army jurisdiction or administration, or in Department of the Army custody • 1-24, page 5

Commanders of host and tenant activities • 1-25, page 6

Provost marshals, Directors of Emergency Services, or physical security officers • 1-26, page 7

Installation and garrison engineers and master planners • 1-27, page 7

### Chapter 2

#### Department of the Army Physical Security Program, page 7

General • 2-1, page 7

Privacy and freedom of information • 2-2, page 7

Security criteria deviation process • 2-3, page 7

Crime prevention • 2-4, page 9

Program assessment • 2-5, page 9

Planning factors • 2-6, page 9

Mission essential and vulnerable areas • 2-7, page 10

Planning considerations • 2-8, page 10

Planning coordination • 2-9, page 11

Contingency plans • 2-10, page 11

Security threat assessment • 2-11, page 11

# FOR OFFICIAL USE ONLY

## Contents—Continued

Physical security plans • 2–12, *page 11*  
U.S. Army Military Police Security Management System • 2–13, *page 12*  
Physical security surveys • 2–14, *page 12*  
Physical security inspections • 2–15, *page 13*  
Report of action taken • 2–16, *page 14*  
Report classification • 2–17, *page 14*  
Security engineering surveys • 2–18, *page 14*

## Chapter 3

### Physical Security Personnel and Credentials, *page 15*

Physical security officer • 3–1, *page 15*  
Physical security inspectors • 3–2, *page 15*  
Management of additional skill identifier H3, physical security inspector credentials, and physical security specialists  
• 3–3, *page 16*  
Additional training • 3–4, *page 16*  
DA Form 4261 and 4261–1 (Physical Security Inspector Identification Card) • 3–5, *page 17*  
Uniforms • 3–6, *page 17*

## Chapter 4

### Physical Security Resources, *page 18*

General • 4–1, *page 18*  
Management decision evaluation package physical security matters • 4–2, *page 18*  
Requirements and resources • 4–3, *page 18*  
Physical security for military construction • 4–4, *page 18*  
Planning for physical security resources • 4–5, *page 18*

## Chapter 5

### Security Identification Cards and Badges, *page 19*

Purpose • 5–1, *page 19*  
General • 5–2, *page 19*  
Security card and badge computerized systems • 5–3, *page 19*

## Chapter 6

### Restricted Areas, *page 19*

General • 6–1, *page 19*  
Command authority • 6–2, *page 19*  
Prohibited actions • 6–3, *page 20*  
Security procedures concerning the prohibition on commercial image collection and surveillance • 6–4, *page 20*  
Perimeter controls for installations and stand-alone facilities • 6–5, *page 20*  
Restricted area signs • 6–6, *page 20*  
National Defense Areas • 6–7, *page 21*  
Procedures for restricted area violations • 6–8, *page 22*

## Chapter 7

### Physical Security Councils, Working Groups, and Boards, *page 22*

Purpose • 7–1, *page 22*  
Installation or garrison physical security council • 7–2, *page 22*  
Department of the Army Physical Security Review Board • 7–3, *page 23*  
Army Physical Security Equipment Action Group • 7–4, *page 24*

## Chapter 8

### Army Access Control, *page 25*

General • 8–1, *page 25*  
Security functions at primary and secondary installation access control points for commanders of host activities  
• 8–2, *page 25*  
Security functions at primary and secondary installation access control points • 8–3, *page 26*

# FOR OFFICIAL USE ONLY

## Contents—Continued

Unescorted personnel • 8-4, *page 26*  
Escorted personnel • 8-5, *page 27*  
Special event access control measures • 8-6, *page 27*  
Installation access control point automation design requirements • 8-7, *page 27*  
Trusted Traveler Program • 8-8, *page 28*  
Construction standards • 8-9, *page 28*  
Installation area access control plan • 8-10, *page 28*  
Installation access control point security forces • 8-11, *page 30*  
Outside the continental United States provisions • 8-12, *page 30*  
Controlling entry of privately owned arms and ammunition • 8-13, *page 30*

## Chapter 9

### Physical Security Equipment Planning, *page 30*

System certifications • 9-1, *page 30*  
Intrusion Detection System • 9-2, *page 31*

## Chapter 10

### Security Forces, *page 32*

General • 10-1, *page 32*  
Personnel selection and training • 10-2, *page 32*  
Procedures • 10-3, *page 32*  
Inspections and guard checks • 10-4, *page 32*  
Patrol plans • 10-5, *page 33*

## Appendixes

- A. References, *page 34*
- B. Physical Security Plan, *page 38*
- C. Internal Control Evaluation Checklist, *page 42*

## Table List

Table 8-1: Installation access control points types, *page 25*

## Figure List

Figure 6-1: Warning sign for installation IACPs and facility entry control points, *page 21*  
Figure 6-2: Warning sign for property perimeters, *page 21*  
Figure 9-1: IDS warning sign, *page 32*

## Glossary

# FOR OFFICIAL USE ONLY

## Chapter 1 Introduction

### Section I General

#### 1-1. Purpose

This regulation prescribes policy and assigns responsibility for developing, executing, 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 glossary.

### Section II Responsibilities

#### 1-4. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

The ASA (ALT) will—

- a. Coordinate early in the research, development, and acquisition process concerning physical security requirements for Army materiel.
- b. Establish an integrated logistics support program for centrally managed physical security equipment (PSE) per AR 700-127.
- c. Provide one nonvoting advisor (major (O-4), lieutenant colonel (O-5), or civilian equivalent (CE)) to the Department of the Army Physical Security Review Board (DAPSRB) per paragraph 7-3.
- d. Provide one nonvoting advisor (O-4, O-5, or CE) to the Army Physical Security Equipment Action Group (APSEAG) per paragraph 7-4.

#### 1-5. Assistant Secretary of the Army for Civil Works

The ASA (CW) will ensure physical security requirements are included in civil works and like projects.

#### 1-6. Assistant Secretary of the Army (Installations, Energy and Environment)

The ASA (IE&E) will—

- a. Program physical security requirements in military construction projects through a formalized process.
- b. Coordinate PSE requirements funded by other procurement, Army with the Provost Marshal General (PMG) and the Commanding General (CG), U.S. Army Corps of Engineers (USACE).

#### 1-7. Assistant Secretary of the Army (Manpower and Reserve Affairs)

The ASA (M&RA) will oversee PMG operations per Department of the Army General Orders No. 2003-09.

#### 1-8. Provost Marshal General

The PMG is the Army staff (ARSTAF) principal officer responsible for the Army physical security program. The PMG will—

- a. Develop policies, goals, and objectives for the program.
- b. Direct the Chief, Military Police Policy Division (DAPM-MPP) to—
  - (1) Coordinate physical security policy to ensure integration and synchronization with other programs.
  - (2) Coordinate with the ARSTAF and other Army elements when establishing physical security policies, procedures, and standards.
  - (3) Approve waivers and exceptions to this regulation when determined to be appropriate.
  - (4) Validate, prioritize, and program Army physical security resource requirements.
  - (5) Centrally plan and direct certain PSE efforts.
  - (6) Use risk-based resourcing when allocating funds.
  - (7) Sustain and continuously improve the U.S. Army Military Police Security Management System (SMS).
  - (8) Chair the DAPSRB per paragraph 7-3.
  - (9) Provide one voting member and one alternate voting member to represent the Army in the DOD Physical Security Equipment Action Group (PSEAG).
  - (10) Provide one voting member to the APSEAG per paragraph 7-4.

# FOR OFFICIAL USE ONLY

(11) Provide one voting member to the DOD Joint Requirements Working Group (JRWG), who will also chair the JRWG as the responsibility rotates among the military departments.

## **1–9. Deputy Chief of Staff, G–1**

The DCS, G–1 will—

- a. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- b. Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

## **1–10. Deputy Chief of Staff, G–2**

The DCS, G–2 will—

- a. Provide intelligence and counterintelligence functions in support of security programs and planning related to protection of Army personnel, materiel, facilities, and operations from espionage, sabotage, criminal activity, subversion, terrorism, and sedition.
- b. Identify threats that may increase physical security requirements.
- c. Coordinate with the CG, USACE to ensure the threat definition is uniform and sufficiently specified to serve as a basis for physical security requirements in construction design.
- d. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.

## **1–11. Deputy Chief of Staff, G–3/5/7**

The DCS, G–3/5/7 will—

- a. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- b. Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

## **1–12. Deputy Chief of Staff, G–4**

The DCS, G–4 will—

- a. Provide copies of surveys, inventory adjustments, and reports that indicate actual or possible criminal activities to HQDA (DAPM–MPP–PS) and CG, U.S. Army Criminal Investigation Command (USACIDC), upon request by the PMG.
- b. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- c. Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

## **1–13. Chief Information Officer/G–6**

The CIO/G–6 will—

- a. Coordinate with the PMG for applicability of the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) to PSE.
- b. Coordinate with the PMG concerning other information technology and physical security matters.
- c. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- d. Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

## **1–14. Assistant Chief of Staff for Installation Management**

The ACSIM will—

- a. Establish a formal process to track physical security requirements in military construction, Army projects.
- b. Establish a formal process to coordinate with the CG, USACE for proper planning, evaluation, application, design, installation, and construction of facility enhancements for all aspects of physical security and antiterrorism protective construction through the mandatory centers of expertise per paragraph 1–18.
- c. Coordinate with the PMG on construction policies and design standards that may impact on physical security.
- d. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- e. Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

## **1–15. The Inspector General**

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

## **1–16. The Surgeon General**

The Surgeon General will—

- a. Provide technical assistance to the PMG concerning physical security policy for medical assets and facilities.
- b. Establish a formal oversight process for the U.S. Army Health Facilities Planning Agency to ensure physical security policy requirements are incorporated in the construction of Army medical facilities.
- c. Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.



# FOR OFFICIAL USE ONLY

- d. Provide one voting member (O-4, O-5, or CE) to the APSEAG per paragraph 7-4.

## 1-17. Chief of Engineers

The COE will—

- a. Establish a formal process to ensure physical security design criteria are considered for proposed construction 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 (IE&E), the PMG, and other principal ARSTAF officers.
- d. Provide one voting member (O-4, O-5, or CE) to the DAPSRB per paragraph 7-3.

## 1-18. Commanding General, U.S. Army Corps of Engineers

The CG, USACE will—

- a. Coordinate with the ACSIM to ensure proper planning, evaluation, application, design, installation, and construction of facility enhancements for all aspects of physical security and antiterrorism protective construction through the mandatory centers of expertise in paragraph 1-18h.
- b. Provide criteria and guidance for the proper design, installation, and acceptance testing of commercial Intrusion Detection Systems (IDSs) installed in construction projects, and other electronic security systems (ESSs), where required. This requirement does not pertain to DOD or DA standardized systems.
- c. Develop and maintain guidance and criteria documents, and provide training for planning, evaluation, application, design, installation, and construction of projects requiring physical security related protective construction and equipment. Designs will incorporate protective construction criteria, electronic security, intrusion detection and PSE, as required.
- d. Develop requirements and execute programs for research and development efforts supporting physical security related protective construction, and PSE applications for protective construction.
- e. Identify problem areas that impact the design and installation of IDS and other PSE.
- f. Coordinate security engineering surveys with the local provost marshal (PM), Director of Emergency Services (DES), or senior physical security officer (PSO) for surveys conducted for the U.S. Army Recruiting Command and U.S. Army Cadet Command.
- g. Provide one voting member (O-4, O-5, or CE) to the APSEAG per paragraph 7-4.
- h. Maintain the Protective Design Center (PDC) and the Electronic Security Center (ESC) as mandatory centers of expertise for protective design and electronic security system technical expertise to Army organizations.
  - (1) The PDC will also support Office of the Provost Marshal General (OPMG) for the review, analysis, and application of facilities standards, and criteria to meet physical security, antiterrorism, and general force protection policies and objectives.
  - (2) The ESC will also support OPMG for the review, analysis, and application of facilities standards, and criteria to meet electronic security system policies and objectives.
  - (3) The PDC and ESC will each provide one nonvoting advisor to the DAPSRB per paragraph 7-3, and to the APSEAG per paragraph 7-4.
- i. Ensure commanders of divisions and districts responsible for civil works and like projects comply with requirements in paragraph 1-22.

## 1-19. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

- a. Formulate concepts, doctrine, organizational structure, materiel objectives, and requirements to employ U.S. Army forces in a theater of operations, in control of civil disturbances, to secure garrisons and to combat terrorism.
- b. Develop physical security concepts and determine the actions necessary to implement these concepts as they impact Army doctrine, organization, training, materiel, leadership, and education, personnel, and facilities.
- c. Maintain an operational tester for Army IDS and other PSE.
- d. Provide training and doctrine support in developing physical security procedures and measures.
- e. Comply with AR 71-9 to ensure that materiel, training, personnel, logistics, doctrine, tactics, and essential system requirements for a PSE item are identified, integrated early, tested, and refined, throughout the materiel acquisition process.
- f. Ensure the requirements above are included in requirements documents, development contracts, tests, evaluations, and other key actions in the acquisition of materiel systems.
- g. Determine future Army PSE requirements.
- h. Ensure physical security requirements and related subsystems, measures, and procedures are identified in the developmental process for new materiel systems in coordination with the product manager, force protection systems and as an integral part of the combat development process.

# FOR OFFICIAL USE ONLY

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

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

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

(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 Army elements to identify requirements for PSE and coordinate the preparation and staffing of capability needs statements.

(4) Resource the conventional physical security/crime prevention course (7H–31D/830–ASIH3) at a level required to satisfy training requirements for Army Servicemembers, civilians, and contract support personnel.

(5) Provide one nonvoting advisor (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.

(6) Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

*k.* Under HQ TRADOC, the CG, U.S. Army Maneuver Support Center, or the Commandant, U.S. Army Military Police School will—

(1) Provide one nonvoting advisor (O–4, O–5, or CE) to the Army voting member to the JRWG.

(2) Provide one nonvoting advisor (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.

(3) Provide one nonvoting advisor (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.

## **1–20. Directors and supervisors of Army staff agencies and commanders of Army organizations not on military installations**

These commanders are responsible for physical security within their activities per applicable Army policy. Coordination for support with the nearest Army physical security office is encouraged, as needed.

### **1–21. Senior commanders**

The senior commanders will—

*a.* Establish a formal physical security program consistent with this regulation.

*b.* Issue formal written orders appointing a command PSO who will serve as the single point of contact for all command physical security matters.

*c.* Establish a formal management assessment program for physical security matters to satisfy oversight and audit responsibilities.

*d.* Ensure compliance with applicable physical security regulations by inspecting subordinate and tenant organizations and surveying installations.

*e.* Provide command guidance to subordinate and tenant organizations to ensure program compliance.

*f.* Coordinate threat information across the command and other senior commanders, as applicable.

*g.* Use the SMS per paragraph 2–13.

*h.* Coordinate physical security matters with the land managing command.

*i.* Review and approve physical security resource requirements identified by the garrisons and like organizations.

*j.* Issue orders pertaining to an installation or activity not otherwise headed by a military commander under the authority of the Internal Security Act of 1950.

### **1–22. Commanders and directors of Army commands, Army service component commands, direct reporting units, the Army National Guard, and U.S. Army Corps of Engineers divisions and districts**

The commanders and directors of ACOMs, ASCCs, DRUs, ARNG, USACE will—

*a.* Establish a physical security program to plan and coordinate physical security matters and to ensure practical, effective, and common sense measures are used.

*b.* Issue formal written orders appointing a command PSO who will serve as the single point of contact for all command physical security matters.

*c.* Review, approve, and maintain a copy of the physical security plans of subordinate installations and stand-alone facilities.

*d.* Identify physical security resource requirements and forward them through command channels to DAPM–MPP–PS.

*e.* Execute physical security funds in accordance with OPMG resource guidance.

*f.* Coordinate with TRADOC as the user representative and with product manager, force protection systems as the physical security materiel developer when an operational need is identified for PSE performance requirements. Correspond with—

(1) Commander, U.S. Army Maneuver Support Center and Fort Leonard Wood (ATZT–CDR), 320 Manscen Loop, Fort Leonard Wood, MO 65473–9084.

# FOR OFFICIAL USE ONLY

(2) Product Manager, Force Protection Systems (SFAE–CBD–GN–F), 5900 Putman Road, Suite 1, Fort Belvoir, VA 22060–5420.

- g.* Use the SMS per paragraph 2–13.
- h.* Support TRADOC in the preparation and coordination of requirements documents.
- i.* Review threat statements prepared for installations and activities for content and accuracy.
- j.* Ensure engineers, physical security personnel, and antiterrorism personnel coordinate design criteria for new construction projects, and document the coordination for construction projects.
- k.* Ensure physical security personnel track construction projects at every milestone of the planning, design, and construction process, and document the tracking process.
- l.* Implement procedures for the issue, control, accountability, and destruction of physical security inspector (PSI) credentials.
- m.* Ensure Army Forces deploying to overseas areas designate personnel to carry out physical security responsibilities to safeguard personnel, facilities, equipment, operations, and materiel against hostile intelligence, terrorists, other criminal, dissident, or other disruptive activity.
- n.* Ensure designated personnel, qualified per paragraph 3–2, are provided inspector credentials for the duration of their deployment tour. After deployment, ensure issued credentials are recovered and accounted for per paragraph 3–5.
- o.* Establish a formal management assessment program for physical security matters to satisfy oversight and audit responsibilities.
- p.* Establish a formal process to record, track, and resolve deficiencies found during physical security inspections and surveys.
- q.* Conduct business case analysis to determine the feasibility of—
  - (1) Multisite maintenance contracts with post-award competition to gain best value service.
  - (2) Multisite IDS monitoring to gain cost efficiencies while maintaining operational effectiveness.
  - (3) Analysis should involve the program analysis and evaluation officer and a review by the senior legal officer.
- r.* Provide one nonvoting advisor (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- s.* Provide one voting member (O–4, O–5, or CE) to the APSEAG per paragraph 7–4.
- t.* The USACE commanders and directors will, also apply these requirements to civil works and like projects.
- u.* State adjutants general will—
  - (1) Establish a physical security program per paragraphs 1–22*a* through 1–22*q*.
  - (2) Coordinate requirements with the Director, ARNG to ensure program synchronization and efficiency.

## **1–23. Product manager, force protection systems**

The product manager, force protection systems will—

- a.* Practice centralized research, development, and acquisition management of PSE for Army use, and for PSE developed by the Army for Joint Service applications in accordance with DODI 3224.03.
- b.* Manage PSE projects as assigned per the management standards of AR 70–1 and AR 700–127. For projects resourced by OPMG, requirements of AR 700–127 will be applied if a rigorous business case analysis indicates a financial benefit is achievable for the Army.
- c.* Implement and sustain post-award competition.
- d.* Ensure site surveys conducted for installation of the Integrated Commercial Intrusion Detection System (ICIDS) identify assets and areas that have regulatory requirements for IDSs. If additional local requirements are identified beyond those established by policy, segregate them in planning documents for evaluation.
- e.* Develop and implement standard design templates for common type new facilities to the extent feasible.
- f.* Maintain a catalog of design templates to facilitate the installation of ICIDS in future Army facilities.
- g.* Serve as the Army representative to the Joint Service Security Equipment Integration Working Group.
- h.* Serve as a technical advisor to the Army representative at the PSEAG and the Joint Service Requirements Working Group.
- i.* Assist OPMG to acquire, procure, deploy, and install certain PSE items, provide quarterly performance briefings concerning execution of the plan, and coordinate business processes.
- j.* Provide one voting member (O–4, O–5, or CE) to the DAPSRB per paragraph 7–3.
- k.* Chair the APSEAG per paragraph 7–4.
- l.* Chair the Physical Security Equipment Working Group (PSEWG) per paragraph 7–4*e*(1).

## **1–24. Commanders of posts, camps, stations, installations, Army-managed Armed Forces Reserve Centers, Army Reserve Centers, Army National Guard Armories, and similar Army facilities subject to Department of the Army jurisdiction or administration, or in Department of the Army custody**

These commanders will—

- a.* Protect personnel and property in their commands against trespass, terrorism, sabotage, theft, arson, and other

# FOR OFFICIAL USE ONLY

illegal acts, and secure personnel, places, and property under their command per this regulation and the Internal Security Act of 1950. An adequate security posture will be determined by considering—

- (1) The types of activity areas or resources and their criticality to the mission.
- (2) Current threats to the installation or activity area, including trespassing, terrorism, sabotage, theft, arson, and other illegal acts.
- (3) The vulnerability of the installation, including construction and physical layout of the installation or activity area, geographical location, and social and political environment.
  - b. In writing, designate restricted areas per chapter 6.
  - c. In writing, designate mission essential and vulnerable areas (MEVA) under their control as identified by the senior law enforcement officer or PSO, and by commanders of tenant organizations.
  - d. 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.
  - e. Issue written appointment orders establishing a physical security council (PSC) chaired by the senior installation law enforcement officer. The council will assist the commander in discharging security duties.
  - f. Direct the organization responsible for threat assessments to—
    - (1) Develop an installation or activity threat statement in coordination with the PSO, local intelligence and law enforcement support elements, based on DA and combatant command threat statements.
    - (2) Pass threat information to all military activities on/off the installation.
  - g. Appoint a PSO in writing who will report through the PM/DES/SO (or in coordination with, if in another office) to the commander on all physical security matters, and will develop an installation or activity physical security plan. The PSO may be at the next higher command level for U.S. Army Reserve (USAR) and ARNG facilities.
  - h. Use the SMS per paragraph 2–13.
  - i. Include physical security as an annex to all applicable orders and plans.
  - j. Provide information about the organization and its activities to the supporting military intelligence element as needed for the force protection mission.
    - (1) Provide physical security support when requested by tenant activities per AR 37–49.
    - (2) Ensure security programs provide for safeguarding of personnel, facilities, equipment, operations, and materiel during mobilization and war.
    - (3) Conduct physical security surveys of installations per paragraph 2–14, and conduct physical security inspections of assets per paragraph 2–15.
    - (4) Perform risk analysis per DA Pam 190–51 for new and existing facilities in which assets in AR 190–51 are expected to be located.

## **1–25. Commanders of host and tenant activities**

- a. Army host commanders will—
  - (1) Appoint a PSO in writing.
  - (2) Execute installation access control operations per chapter 8 of this regulation.
  - (3) Designate and approve MEVAs in writing.
  - (4) Provide law enforcement or guard patrols as required to protect personnel and government assets.
  - (5) Install, operate, and maintain IDS and other PSE as required per AR 37–49 for reimbursable costs.
  - (6) Respond to alarms annunciated by IDS if not within the tenant activity's capability.
  - (7) Use the SMS per paragraph 2–13.
  - (8) Conduct physical security surveys of the installation per paragraph 2–14.
  - (9) Conduct physical security inspections of tenant activities per paragraph 2–15 and provide tenants with copies of the inspection reports.
- b. Tenant commanders will—
  - (1) Request physical security requirements or enhancements beyond their means from the host commander.
  - (2) Inform the host commander of all physical security measures in effect.
  - (3) Designate and approve MEVAs in writing and forward the list to the host commander for inclusion in the installation physical security plan.
  - (4) Appoint a PSO officer in writing.
  - (5) Coordinate physical security plans with the host commander.
  - (6) Forward a copy of physical security plans to the host commander for inclusion as an annex in the installation physical security plan.
  - (7) Reimburse host commanders, as required, to install, operate, and maintain IDS and other PSE.

# FOR OFFICIAL USE ONLY

## **1–26. Provost marshals, Directors of Emergency Services, or physical security officers**

The PMs, DES, or PSOs will—

- a.* Assess installation physical security needs by conducting physical security surveys and inspections per paragraphs 2–14 and 2–15.
- b.* Use the SMS per paragraph 2–13.
- c.* Recommend physical security and antiterrorism design considerations in the preparation of installation engineer construction projects for new construction, renovation, modification, or lease acquisition.
- d.* Serve as the installation single PSE point of contact for units under control of and within the area of responsibility of the installation or garrison commander. Ensure coordination of equipment requirements with users, facility engineers, logistics, and communications personnel.
- e.* Provide technical support to the organization responsible for threat assessments.
- f.* Monitor resource management of the installation physical security program. Plan and program necessary resources for physical security projects in the program budget cycle in coordination with the comptroller.
- g.* Monitor appropriate funding status of all physical security program resource requirements.
- h.* Coordinate physical security with operations security and antiterrorism officers.
- i.* Coordinate with installation engineers during the planning, design, and construction of all projects to identify physical security requirements, including supporting communications, and to ensure the 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 and document concurrence or nonconcurrence.
- k.* Provide an advisor to engineer planning and design charrettes.

## **1–27. Installation and garrison engineers and master planners**

Installation and garrison engineers and master planners will—

- a.* Coordinate with the PM or PSO 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 PSO.

## **Chapter 2**

### **Department of the Army Physical Security Program**

#### **2–1. General**

- a.* The Army Physical Security Program is a systematic approach to physical security to ensure adequate protection of DA assets on installations, in stand-alone facilities, for civil works and like projects, and other locations occupied by DA elements.
  - b.* The intent of the program is to counter threats to Army assets and capabilities during peacetime, contingencies, mobilization, and wartime by addressing the spectrum of—
    - (1) Aggressors defined as unsophisticated criminals, sophisticated criminals, and organized criminal groups, vandals/activists and extremist protesters, domestic terrorists, international terrorists, state-sponsored terrorists, saboteurs and foreign intelligence agents.
    - (2) Aggressor tactics that may be used.
    - (3) Human threat tools, weapons, and explosives based on historical and current use.
- c.* Physical security plans, processes, and procedures will be synchronized with other security programs such as antiterrorism, information security, and personnel security, and related efforts such as continuity of operations, information assurance, and resource management.

#### **2–2. Privacy and freedom of information**

Requirements of AR 340–21 and AR 25–55 will be rigorously applied to all aspects of physical security planning and operations.

#### **2–3. Security criteria deviation process**

- a.* The purpose of the security criteria deviation process is to—
  - (1) Ensure prescribed security requirements are properly observed and implemented.
  - (2) Provide a management tool to monitor corrective actions.
  - (3) Ensure deviations from established security requirements are systematically and uniformly identified and approved by the proper level of command.

# FOR OFFICIAL USE ONLY

b. Waivers and exceptions are deviations from specific security requirements.

(1) *Waivers to policy.*

(a) A waiver may be approved for temporary relief from a specific requirement pending actions to conform to the requirement.

(b) A waiver may be approved for a period not to exceed 12 months and extended only after a review of the circumstances that necessitate the extension.

(c) Compensatory security measures are required in the interim. Compensatory security measures approved by the commander/director will remain in effect pending formal review and final approval by HQDA (DAPM–MPP–PS). Deficiencies correctable within 60 days do not require a waiver; however, the commander/director will ensure compensatory security measures are taken during the interval. In such cases, the compensatory measure must be in writing, approved by the commander/director and the next higher commander in the chain of command.

(d) Waivers will not be used to reduce or eliminate minimum security requirements.

(2) *Exceptions to policy.*

(a) Exceptions may be approved only when correction of the deviation is not considered to be feasible or cost effective, and only after a most careful and critical evaluation of the facts in the case.

(b) The HQDA (DAPM–MPP–PS) authority will be notified through command channels when the exception is no longer needed.

(c) All exceptions will be reviewed during physical security inspections or when a major change in site configuration or mission offers the opportunity for corrective action to terminate the exception.

(d) The commander/director to whom the exception was granted will conduct the review. All reviews will be forwarded through command channels to the OPMG.

(e) Compensatory security measures are required in the interim. Compensatory security measures approved by the commander/director will remain in effect pending formal review and final approval by HQDA (DAPM–MPP–PS).

(f) Exceptions will not be used to reduce or eliminate minimum security requirements.

c. *Compensatory measures.*

(1) Compensatory measures will be initiated for each deficiency.

(2) One compensatory measure may suffice for more than one deficiency if appropriate.

(3) Measures will compensate for the specific vulnerability created by a deficiency when a minimum security requirement cannot be met. A security requirement cannot serve as a compensatory measure for a deficiency.

(4) Compensatory measures may include additional security forces, procedures, and/or physical security devices such as additional locks, alarms, lighting, and delay devices. The criteria for accepting compensatory measures will be designed to specifically enhance the security posture caused by the deficient situation.

(5) Compensatory measures that consist primarily of instructions to the security force to increase their alertness will not provide a comparable level of security.

(6) The commander/director will ensure that prescribed compensatory measures are implemented as required.

(7) Security forces will be advised of all standing deviations and compensatory measures in assigned duty areas.

(8) Compensatory measures for individual deficiencies must not unrealistically task the security forces when considered in total.

d. *Requests for waivers and exceptions.*

e. Requests are initiated by the commander/director and forwarded through appropriate command channels to HQDA (DAPM–MPP–PS). Waivers and exceptions concerning facility design will also be coordinated with the ACSIM.

f. *Include the following information:*

(1) *Subject of request.* For example, Request for Waiver at Dugway Proving Grounds-Intrusion Detection System.

(2) *Reasons for request.* State the problems and/or deficiencies that constitute requirements below those cited in this regulation. Cite policy references and requirements.

(3) *Reasons for noncompliance.* Explain why the organization cannot comply with the requirements of this regulation. For waivers, show what actions have been taken, planned, or scheduled to correct the deficiencies.

(4) *Compensatory measures.* Detailed information on current compensatory measures.

(5) *A list of all waivers and exceptions currently in effect.* Explain why these deviations, collectively, will not establish an overall site vulnerability greater than the stated compensatory measures.

(6) *Coordination.* Show coordinated efforts with the affected staff agencies (PM/security officer, supporting judge advocate of the installation, supporting engineer, and so forth) or activity.

(7) *Commander's evaluation of the requests.* Commanders in the chain of command will review and endorse each waiver or exception request. At the major subordinate command and senior commander level, commanders may delegate the review and endorsement to a senior executive service civilian assigned to that headquarters who is responsible for physical security matters in the command. Endorsement from each command chain level will include

# FOR OFFICIAL USE ONLY

comments assessing the adequacy of compensatory measures, taking into consideration the required criteria for waivers and exceptions.

(8) *Classification*. Requests for waivers or exceptions may require appropriate security classification according to criteria in AR 380–86.

## 2–4. Crime prevention

*a.* Crime prevention is a command responsibility. A successful program needs continuing command emphasis to prevent criminal activity from detracting from mission accomplishment.

*b.* An effective crime prevention program serves to maximize the security of a military community in peace and war. Its goals are similar to, and support those of the physical security and operations security programs (see AR 530–1). The methods used to identify and analyze crime problems complement each other.

*c.* A crime prevention program reduces crime by—

(1) Stimulating appropriate crime prevention attitudes, procedures, and behavior through public awareness campaigns and programs.

(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.

*d.* The USACIDC provides support for crime prevention surveys.

## 2–5. Program assessment

Commanders will assess the following factors, at a minimum, to determine the type and extent of the commitment of resources toward physical security programs—

*a.* Assessment factors per DA Pam 190–51.

*b.* Local threat assessment.

*c.* Definition and analysis of the area to be protected including—

(1) Nature and arrangement of the activity.

(2) Number of personnel involved.

(3) Monetary, tactical, or strategic value of materiel.

(4) Storage of classified information and equipment.

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

*d.* Whether the protected area is designated as a mission essential or vulnerable area.

## 2–6. Planning factors

These factors will be considered when developing a physical security plan—

*a.* During peacetime, the planning for mobilization, war, and 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 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 525–13) so that equivalent levels of physical security measures and procedures are added as the threat intensifies and readiness increases.

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

*d.* A plan to control 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.

*e.* The application of physical security procedures should be tested during unit training and operations that require security precautions to protect against—

(1) Hostile intelligence gathering operations such as satellites, offshore monitoring, and human intelligence.

(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 such as hospital wards, USAR schools, and logistics warehouses. Buildings and facilities should be

# FOR OFFICIAL USE ONLY

evaluated for physical security requirements once the mobilization assignment has been made. Reasonable efforts should be made to correct identified physical security deficiencies within the means of the organization.

## 2-7. Mission essential and vulnerable areas

*a.* Mission essential and vulnerable areas (MEVAs) will be identified and prioritized as a decision support tool for the commander to prioritize resource allocation. The numerical output of the risk analysis process per DA Pam 190-51 should serve as the baseline for prioritizing MEVAs. Most facilities and areas can be considered to have assets critical to an organization's mission, but practicality must be applied when developing the MEVA list so it can be constrained to a manageable size (see glossary for more discussion).

*b.* Evaluate assets or capabilities in a facility or area under consideration for MEVA status as follows:

- (1) Criticality to the National Defense, to the Army mission, and to the organization's mission.
- (2) Local criminal and terrorist threat assessments.
- (3) Nature and arrangement of the activity.
- (4) Number of personnel involved.
- (5) Strategic, tactical, or monetary value of assets.
- (6) Classification level.
- (7) Other factors such as natural or human-made hazards.
- (8) Risk analysis results per DA Pam 190-51 for each potential MEVA.

*c.* At a minimum, the following areas will be designated as MEVAs:

(1) Ammunition and explosive storage rooms, facilities or areas, and arms storage, manufacturing, rebuilding, or demilitarizing facilities and areas. When such spaces are empty, the IDS, lock and key accountability, and other requirements will be maintained unless the space has been repurposed.

(2) Primary and alternate electric power supply transmission and generation facilities.

(3) On-post utility distribution systems to include tank farms, supply points, and distribution hubs.

(4) On-post water sources and treatment facilities.

(5) Airfields and aircraft parking or aircraft maintenance areas.

(6) Classified sites.

(7) Primary and alternate command posts.

(8) Communications facilities to include Network Enterprise Centers.

(9) Consolidated supply and storage operations.

(10) Controlled drug vaults or storage areas.

(11) Field maintenance shops.

(12) Finance offices.

(13) The IDS monitor stations.

(14) Motor pools and maintenance activities.

(15) Petroleum, oil, lubricants storage, and dispensing points.

(16) Medical treatment facilities (for example, medical centers, hospitals, troop medical clinics, dental clinics).

(17) The USACIDC evidence rooms.

## 2-8. Planning considerations

*a.* Integrate physical security requirements into plans for mobilization, war, contingencies and stability operations to provide effective protection of personnel, facilities, and equipment.

*b.* Evaluate peacetime planning considerations to permit adjustments in physical security measures as the threat changes.

*c.* Tie physical security planning to the force protection condition (FPCON) system so physical security measures and procedures are added as the threat intensifies and readiness increases.

*d.* Establish a plan to control access to roads that enter and exit the installation. Coordinate road closures and road restriction plans with the servicing public works directorate and with local and state law enforcement agencies. Include contingency road closings in the installation physical security plan.

*e.* Include restricting movement within specific areas of the installation, as required.

*f.* Establish evacuation route plans.

*g.* During unit training and operations that require security precautions, the application of physical security procedures should be tested to protect against hostile intelligence gathering operations, paramilitary forces, terrorists, saboteurs, criminals, protest groups, and disaffected persons.

*h.* For installations or organizations that expand during times of mobilization must identify buildings and facilities to be assigned to expanded activities (for example, hospital wards, schools, logistics warehouses). Evaluate physical



# FOR OFFICIAL USE ONLY

security requirements for those buildings and facilities once the mobilization assignment has been made. Make reasonable efforts to correct physical security deficiencies within the means of the installation.

## 2-9. Planning coordination

*a.* Coordination through close liaison should be effected between the military commander while developing a security plan with—

- (1) Adjacent installations or units.
- (2) Federal agencies.
- (3) State and local agencies.
- (4) Similar host country agencies.
- (5) For USACE, with tribal nations, as applicable.

*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.* The host activity coordinates the physical security efforts of all tenants as outlined in support agreements and the host activity security plan. Applicable provisions will be included as an appendix to, the support agreement to include assignment of physical security responsibilities. The agreement will be based on the design approach of protection-in-depth and should address—

- (1) Maximum quantities to be stored or extent of capabilities as determined by the commander.
- (2) Physical safeguards to be employed.
- (3) Frequency and responsibility for physical inventories or reconciliations.
- (4) Reporting of losses for subsequent investigation.
- (5) Lock and key control.
- (6) Identity of the organization with overall responsibility.
- (7) Procedures for authorization and identification of individuals to receipt for and physically take custody of Army property.

*d.* Authority, jurisdiction, and responsibility must be set forth in a manner to best ensure protection and avoid duplication of effort.

## 2-10. Contingency plans

It will be necessary in most instances to increase security for arms, ammunition, and explosives (AA&E) and other sensitive assets 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 physical protective measures and security procedural measures 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.

## 2-11. Security threat assessment

*a.* Installations and civil works and like projects will develop a local threat statement covering the entire spectrum of aggressors and tactics listed in DA Pam 190-51 and Unified Facilities Criteria (UFC) 4-020-01. The 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. Coordination will be established with the following agencies, at a minimum:

- (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, and included as an annex in the installation physical security plan.

*c.* Commanders will also use security assessment documents that identify vulnerabilities to help determine security weakness that may be compromised by threat forces. These may include documents such as risk assessments and security engineering vulnerability assessments.

## 2-12. Physical security plans

A physical security plan will be developed for each installation, unit, and activity.

*a.* Appendix B provides a format guide for developing the plan.

*b.* The plan and annexes will be exercised annually and in coordination with antiterrorism and other emergency or contingency plans to the greatest extent practical.

*c.* The plan will not be subordinate to the antiterrorism plan as it has a broader scope of concern than only terrorism.

# FOR OFFICIAL USE ONLY

*d.* The plan will be reviewed annually, revised as required, and certified in writing as being current. A brief statement indicating the plan is current will be placed on the front page.

*e.* Annexes to the plan may be separated for operational purposes. The other publication containing the annexes will be cited. At a minimum, annexes to the plan will include—

- (1) The installation threat statement (criminal and terrorist).
- (2) A terrorism counteraction plan.
- (3) A bomb threat plan that includes—
  - (a) Control of operations.
  - (b) Evacuation.
  - (c) Search.
  - (d) Finding the device.
  - (e) Disposal.
  - (f) Detonation and damage control.
  - (g) Control of publicity.
  - (h) After-action report.
- (4) Site closure plan.
- (5) A natural disaster plan in compliance with National Incident Management System standards. The plan will be coordinated with plans of local jurisdictions, and at a minimum, will provide guidance for—
  - (a) Control of operation.
  - (b) Evacuation.
  - (c) Communication.
  - (d) Control of publicity.
  - (e) Physical security.
  - (f) After-action report.
- (6) A civil disturbance plan based on local threats.
- (7) A resource plan for minimum essential physical security needs.
- (8) A communications plan addressing communications with other Federal agencies and local law enforcement agencies to share information about possible threats. The plan should address all communication needs for the paragraphs, above.
- (9) A list of designated restricted areas.
- (10) A list of MEVAs.
- (11) Copies of memorandums of agreement/understanding with local (external) first responders.

## **2-13. U.S. Army Military Police Security Management System**

*a.* The SMS will be used by all Army physical security personnel and planners to standardize the procedures used to conduct physical security inspections, surveys, and the conduct of planning and programming.

*b.* The SMS is—

- (1) A web-enabled, enterprise software solution that optimizes the process of collecting information by automating routine tasks.
- (2) A decisionmaking planner's tool that presents a coherent view of the physical security posture for any defined area of responsibility.
- (3) An optimizer of planning procedures by providing objective, risk-based prioritization of action.
- (4) A standardized set of risk analysis measurements based on risk management techniques published by the National Institute of Standards and Technology.

*c.* The SMS will be used to—

- (1) Schedule, conduct, and record physical security inspections and surveys.
- (2) Submit timely information to higher headquarters.
- (3) Justify program requirements.
- (4) Create risk mitigation action plans based on trend analysis, cost/benefit analysis, and loss expectancy analysis as means to determine the best use of resources.

## **2-14. Physical security surveys**

*a.* A physical security survey is a formal recorded assessment of an installation's overall physical security program to include electronic security. The survey provides the commander with an assessment of the security posture in view of the threat and mission, and informs the commander about the installation physical security strengths and weaknesses.

*b.* Surveys are not required for stand-alone facilities if a physical security inspection provides the commander with information necessary to determine the physical security posture of the facility, not just the tenant units. For example, an Armed Forces Reserve Center managed by the USAR might not require a survey if the center is assessed by

# FOR OFFICIAL USE ONLY

conducting one inspection for each unit to include the landlord unit, and then conducting an additional inspection of the landlord unit to cover shared space such as a motor pool and property perimeter.

c. Surveys will be recorded and results analyzed in the SMS. DA Form 2806 (Physical Security Survey Report) may be used if the SMS is not immediately available. Survey reports will show findings of policy deficiencies and also observations concerning potential means to improve site security. Procedures and measures to evaluate will include—

- (1) Threat assessment procedures.
- (2) Security forces types, availability, training, equipment, and guard orders.
- (3) Compliance with access control procedures per chapter 8.
- (4) Control of visitors and packages.
- (5) Use of PSE.
- (6) Security lighting.
- (7) Control, issuance, and accountability of keys used at the installation perimeter such as for limited access gates, and for industrial spaces.
- (8) Identification of critical areas or facilities.
- (9) Process used to track physical security work orders and vulnerability mitigation efforts.
- (10) Outstanding waivers and exceptions to policy.

d. Surveys will be conducted every 36 months except—

- (1) When an installation is activated.
- (2) When no record exists of a previous physical security survey.
- (3) For sites with AA–E conventional bulk storage (see AR 190–11) and for sites with surety assets, every 24 months.
- (4) When the commander determines that greater frequency is required.

e. Physical security surveys will include—

- (1) An executive summary for the senior commander.
- (2) A detailed assessment of the security posture of the installation.
- (3) Recommended prioritized application of resources for reducing vulnerabilities.
- (4) Exhibits, such as photographs, sketches, graphs, and charts to clarify findings and recommendations, and an assessment of criticality and vulnerability.

f. A copy of the physical security survey, and exhibits, if beneficial, will be provided to—

- (1) The installation commander.
- (2) The ACOM, DRU, ARNG command chain for information and additional action.
- (3) The ASCC.

g. A commander's report of corrective action taken will be submitted in response to the survey if policy deficiencies, not observations, were found. A copy will be furnished to the PMO/DES and retained until the next survey is completed.

h. A formal process will be followed to ensure policy discrepancies are corrected. After corrective actions are taken, the physical security posture will be reassessed based on—

- (1) Mission.
- (2) Actual and potential threats.
- (3) Findings of the survey team.
- (4) Comparison of findings from previously conducted surveys and inspections.
- (5) Areas considered over or under protected.

i. The assessment will be used to form the physical security resource plan to recommend allocation priorities and any revisions to existing measures and procedures, or the development of new measures and procedures. Highest priority should usually be given to activities considered essential to mission accomplishment. Forward this plan to the commander for approval and inclusion in the installation physical security plan.

## 2–15. Physical security inspections

a. A physical security inspection is a formal recorded assessment of the physical protective measures and security procedural measures implemented to protect assets. The SMS will be used to gather and record inspection information. DA Form 2806–1 (Physical Security Inspection Report) may be used if the SMS is not immediately available.

- (1) The PSI will not engage in illegal or dangerous conduct to demonstrate security weaknesses.
- (2) Inspections may be unannounced, but inspectors will first review unit schedules to minimize adverse impact with training, mobilization, demobilization or similar requirements.
- (3) Assets listed in the 190-series of Army regulations, at a minimum, will be inspected for compliance with minimum physical protective and security procedural measures. Physical security plans required by this regulation will also be inspected.

# FOR OFFICIAL USE ONLY

(4) One report will be produced for an inspected organization regardless of the number of inspectable assets in the organization (for example, AA&E, wheeled and tracked vehicles, aircraft).

*b.* Physical security inspections will be conducted—

(1) Every 18 months for conventional AA&E not in bulk storage per AR 190–11.

(2) Every 24 months for conventional AA&E bulk storage, nuclear reactors, special nuclear materials, chemical agents, and biological select agents and toxins.

(3) Every 24 months for other assets when—

(*a*) A MEVA is identified.

(*b*) A unit or activity is activated.

(*c*) No record exists of a prior physical security inspection.

(*d*) There is a change in the unit or activity that may impact on existing physical security plans.

(*e*) There is an indication or reported incident of significant or recurring criminal activity.

(*f*) The commander determines a greater frequency is required.

*c.* Reserve Officer Training Corps regional physical security personnel will conduct a physical security inspection during the overarching annual formal inspection.

*d.* The PSI will be granted access to facilities, assets, records, and other information on a need-to-know basis, consistent with the inspector's clearance for access to defense information and provisions of applicable regulations.

*e.* A copy of the physical security inspection report, with exhibits if beneficial, 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 inspected organization.

(3) Installation PSO.

*f.* Security deficiencies beyond the capabilities of the local commander to correct will be reported to the next higher commander to program resource requirements.

*g.* The submission of a work order does not resolve a deficiency. Compensatory measures will be employed within available resources until the work order is completed.

*h.* Recurring deficiencies will be tracked during future physical security inspections until corrected.

*i.* A follow-up inspection will be conducted 6 months later if the initial inspection resulted in an unsatisfactory rating.

## 2–16. Report of action taken

*a.* A report of action taken is required for surveys and inspections with unsatisfactory ratings.

(1) For inspections, the report will be provided by the inspected commander to—

(*a*) The supporting garrison.

(*b*) The activity's chain of command.

(2) For surveys, the report will be provided by the inspected garrison commander to—

(*a*) The installation commander.

(*b*) The senior commander.

(*c*) The ASCC.

(*d*) The garrison chain of command.

*b.* A copy will be maintained by the inspected activity or garrison and by the supporting physical security office until at least the next physical security inspection or survey is conducted. The report of action taken will address each individual deficiency and may also include observations and comments.

## 2–17. Report classification

Classify and safeguard completed surveys and inspections per AR 380–5, as appropriate.

## 2–18. Security engineering surveys

A security engineering survey is an on-site assessment of physical security engineering requirements. Security engineering surveys will be performed when planning new construction, renovations to facilities when the value of the replacement cost is at least 50 percent, or the facility is determined to be a MEVA. 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 assets requiring protection.

(2) Identify threats to the assets and required protection measures.

(3) Identify protective measures to reduce vulnerabilities.

(4) Determine the cost of proposed protective measures.

(5) Develop a prioritized list of protective measures based on risk assessment using DA Pam 190–51 and UFC 4–020–01.

# FOR OFFICIAL USE ONLY

*b.* The following personnel or their representatives should participate or provide input to the security engineering survey at a minimum:

- (1) Director of public works or equivalent installation engineer, to include the master planner.
- (2) The PM or equivalent security officer, to include the PSO.
- (3) Antiterrorism officer.
- (4) Operations officer.
- (5) Intelligence officer.
- (6) Facility user.
- (7) Logistics officer.
- (8) Safety officer.
- (9) Communications officer.
- (10) Electronic security manager for the ARNG.

*c.* Personnel to support security engineering surveys are available on a cost reimbursable basis from the USACE PDC, the USACE ESC, or the ARNG program manager (non reimbursable if for ARNG use) at these addresses—

Commander, U.S. Army Engineer District  
ATTN: CENWO-ED-S  
1616 Capital Avenue  
Omaha, NE 68102-4929  
email: dll-cenwo-pdc-hd@nwo02.usace.army.mil  
<https://pdc.usace.army.mil>

Commander, Huntsville Engineering and Support Center  
ATTN: CEHNC-ED-ME-T  
4820 University Square  
Huntsville, AL 35816-1822  
email: contact-esc@usace.army.mil  
<http://www.hnd.usace.army.mil/esc/default.aspx>

Director, Army National Guard  
ATTN: ARNG-ARI-FM-ESS (Electronic Security System Program Manager)  
111 S. George Mason Drive  
Arlington, VA 22204-2905

## **Chapter 3** **Physical Security Personnel and Credentials**

### **3-1. Physical security officer**

*a.* A PSO will be appointed in writing at the unit (battalion and higher), garrison, ACOM, ASCC, DRU, and ARNG command levels. Appointees will be knowledgeable of physical security and will meet at least one of the following requirements:

- (1) Demonstrated ability to manage a physical security program through prior experience.
- (2) Formal training in military police or physical security operations.
- (3) Completion of the Army physical security course per paragraph 3-2a(3).

*b.* Department of the Army civilians and ARNG state technicians may be appointed as PSOs per—

- (1) AR 690-950.
- (2) Position Classification Standards for Security Administration Series 0080 as published by the Office of Personnel Management.
- (3) State or territory personnel directives for physical security specialists also apply for the ARNG.

### **3-2. Physical security inspectors**

Selection of personnel to the position of PSI will be made by the local commander, commander's representative, or the PM/DES/PSO.

*a.* Military inspectors will be—

- (1) Qualified in primary military occupational specialty 31B or 31E if assigned to the U.S. Disciplinary Barracks (USDB).
- (2) A staff sergeant (E-6) or above or waived by the local PM/DES/SO to sergeant (E-5).

# FOR OFFICIAL USE ONLY

(3) Formally trained at the U.S. Army Military Police School Conventional Physical Security/Crime Prevention Course (7H-31D/830-ASIH3).

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

(5) Awarded additional skill identifier (ASI) H3.

b. U.S. Government civilian employees will—

(1) Meet the current Office of Personnel Management 0080 qualification standards.

(2) Be formally trained at the 7H-31D/830-ASIH3 course.

(3) Be cleared for access to at least secret national defense information.

c. The PSI credentials will not be issued to contracted persons.

d. Weapons will not be issued to civilian physical security specialists as they are not police personnel and do not have authority to enforce the law.

### **3-3. Management of additional skill identifier H3, physical security inspector credentials, and physical security specialists**

a. The ASI H3 will be awarded per applicable regulations to military police Soldiers qualified to be physical security specialists. The ASI H3 will only be awarded on the recommendation of the PM/DES/PSO, or the Commander, USDB.

b. The PM/DES/PSO will initiate action to withdraw ASI H3, collect credentials, and remove a person from the physical security program on determination that the person is no longer qualified to perform physical security specialist duties. Disqualification or relief from duty 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) Any other conduct that may adversely affect a person's continued performance of duties.

c. A physical security specialist will be suspended from duty when the person—

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

(2) Has had their security clearance suspended.

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

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

(2) Attained the rank of sergeant major and will not be assigned to a physical security assignment.

e. Names of persons in the categories listed in the above paragraph will be forwarded to the U.S. Army Human Resources Command (AHRC-EPL-M) for removal of the ASI and annotation in official records. A copy of the action will be furnished to the local military personnel office for inclusion in the Soldier's personnel file. The local commander may restore ASI H3 to a qualified person in accordance with paragraph 3-3a.

### **3-4. Additional training**

a. The PSOs and specialists are encouraged to attend the following training to increase skills in management and technical expertise:

(1) The USACE training should include—

(a) The Security Engineering Training.

(b) The electronic security system design.

(c) The ICIDS Operator Training.

(2) The DOD/DA basic and advanced antiterrorism officer courses, resource management courses, and associated or supporting skills such as antiterrorism, operations security, information security, continuity of operations, critical infrastructure risk management, and general program management.

b. Career program 19. The career program 19 provides resources for technical and management enhancing courses for civilian law enforcement and physical security personnel (available at <http://cpol.army.mil/library/train/catalog/ch03cp19.html>).

c. Additional courses available for ARNG personnel—

(1) The electronic security system/IDS certification course. Successful completion is a prerequisite for the following courses.

(2) The electronic security system manager course.

(3) Access control systems/closed circuit television 101 course.

# FOR OFFICIAL USE ONLY

d. For safe and vault technicians, Federal Standard 809A requires that any servicing of General Services Administration (GSA) approved containers or vault doors, to include neutralization, repair, combination lock servicing, or replacement will be accomplished only by persons who have successfully completed the GSA Certified Safe and Vault Technician course. The changing of combinations or selection of operator modes for combination locks is exempt from this requirement. Course information is available at <https://portal.navfac.navy.mil/go/locks> or by contacting the DOD Lock Program at DSN 551-1212, 1-800-290-7607 or 1-805-981-1212.

## 3-5. DA Form 4261 and 4261-1 (Physical Security Inspector Identification Card)

### a. Overview.

(1) Personnel who perform PSI duties and meet the criteria of paragraph 3-2 will present DA Form 4261 and 4261-1 to appropriate personnel when conducting physical security inspections and surveys.

(2) The combined DA Form 4261-1 is the only authorized credential for PSIs. Reproducing the credential or use of locally fabricated credentials is prohibited.

(3) Physical security credentials are serially numbered with a letter and a 4-digit number.

(4) A DA Form 4261-1 that displays a social security number will be immediately destroyed and a new form issued with the social security number field left blank until the current stock is depleted.

(5) Credentials will be signed by the inspector, authenticated by the PM/DES/SO or Commander, USDB, and laminated by the issuing authority. For organizations that do not have these command positions, the commander or director will sign the credentials. Non-laminated credentials are not valid.

(6) 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. Issuance.

(1) HQDA (DAPM-MPP-PS) will issue credentials by serial numbered lots to appropriate ACOMs, ASCCs, DRUs, and ARNG, as needed. Requests for credentials will be sent to Headquarters, Department of the Army, (DAPM-MPP-PS), 2800 Army Pentagon, Washington, DC 20310-2800.

(2) Commands that administer credentials will develop accountability procedures for the issue, control, accountability, and destruction of credentials and also prescribe actions to be taken consistent with this regulation if credentials are lost or misused.

(3) New credentials are not required when a new issuing authority is determined. The new authority, however, will indicate continued suitability of inspectors to possess credentials issued by a previous authority by signing an updated credential control log.

(4) Credentials will only be issued to personnel meeting the qualification requirements of paragraph 3-2. Personnel in management positions do not necessarily require credentials. Issuance of credentials to personnel in management positions will be determined by the command chain, keeping in mind that credentials should be limited to the least practical number consistent with operational needs.

(5) Credentials will be issued for a period not to exceed 48 months from the date of issue.

### c. Withdrawal.

(1) Credentials will be withdrawn for cause per paragraph 3-3b.

(2) Credentials will be withdrawn upon the inspector's departure due to permanent change of station, expiration of term of service, or reassignment from PSI duties.

(3) Credentials will be temporarily withdrawn when the inspector is being investigated for criminal conduct or other conduct determined by the issuing authority to be inappropriate, which might result in permanent withdrawal for cause.

d. *Reporting information.* Issuing authorities will report the full name, rank, social security number, and credential number of each person to whom PSI credentials are issued or from whom credentials are withdrawn. This information will be reported in writing to the PM or PSO 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 the PM/DES/PSO will establish and maintain a control log to ensure accountability for the issue, withdrawal, and destruction of credentials.

## 3-6. Uniforms

a. Military PSIs will wear the duty military uniform.

b. The PM/DES/PSO may authorize the wearing of appropriate civilian clothing when official duties require foreign travel where wearing a military uniform is prohibited.

# FOR OFFICIAL USE ONLY

## Chapter 4 Physical Security Resources

### 4-1. General

Physical security resources will be used to ensure protection of Army assets and capabilities including national security information and materiel. Commercial equipment may be used if DOD or DA standardized equipment is not available or does not meet a technical requirement. An operational needs statement will be forwarded to the TRADOC user representative when there is a need to develop DOD or DA standardized equipment. Once a component or system is developed or adopted from commercial sources it is considered standardized and may be adopted by all DOD components to satisfy joint operational requirements.

### 4-2. Management decision evaluation package physical security matters

The MDEP physical security matters is part of the Army base program and is used to resource physical security requirements with appropriated funds for operations and maintenance, Army; operations and maintenance, Army Reserve; operations and maintenance, Army National Guard; and other procurement, Army. In general categories, physical security matters resources the procurement, operation and sustainment of barriers, blast mitigation devices, physical security communication systems, explosives detection devices, IDS, personnel protection equipment and systems, site improvements (for example, fencing and security lighting), management and planning (for example, civilian pay), security forces and technicians, and contract security guards.

### 4-3. Requirements and resources

*a.* The physical security matters is not generally used for activities organized under DOD or DA business rules that require resourcing by other than the Army base program. The physical security matters is not intended to for commercial establishments such as banks, credit unions and non-DOD commercial activities, chemical program fund activities, and RDT&E activities.

*b.* General officer quarters are usually resourced with Army Family housing funds. The potential use of physical security matters resources for these quarters will be closely coordinated.

*c.* Minimum physical security requirements will be provided to—

(1) The Army and Air Force Exchange Service (AAFES) per AR 215-8. The AAFES Directive EOP 16-1 will be used for planning.

(2) The Defense Commissary Agency (DeCA) per DODD 5105.55. The DeCA Directive 30-18 will be used for planning.

(3) Nonappropriated fund activities to a reasonable extent as determined by the servicing physical security office.

*d.* The physical security matters may be an optional funding source for working capital operations. The OPMG will determine funding support to working capital, if any. The physical security matters support is not assured so physical security should be programmed in working capital budgets until such support, if provided, is verified on a case-by-case basis.

### 4-4. Physical security for military construction

*a.* Physical security requirements for military construction are identified for planning purposes per AR 420-1. In general, construction funds are provided for physical security requirements such as those required by UFC 4-010-01, and for real property items such as fencing, security lighting, vehicle barriers, warning signs, and signaling devices.

*b.* Equipment requirements unique to the using organization are annotated in construction documents, but are not resourced with construction funds. Construction funds resource the equipment installation, not the actual equipment purchase.

*c.* The using organization will ensure that PSE requirements not resourced with construction funds are programmed per paragraph 4-5.

*d.* For the ARNG, engineering personnel for USAR Centers managed by the ARNG and for other ARNG facilities will ensure that storage of AA&E meets minimum physical security criteria such as for IDS, locks, and hasps, lighting, as necessary, for the category of AA&E involved. Maintenance of physical security measures will be planned and executed by engineer personnel coinciding with the acceptance of new facilities upon beneficial occupancy.

### 4-5. Planning for physical security resources

*a.* Planners will announce requirements through the Planning, Programming, Budgeting, and Execution System. Requirements will be validated by the chain of command and recorded in Schedule 75 of the Automated Schedule and Reporting System.

*b.* Requests for purchase, issue, lease, or lease renewal of commercial IDS is subject to approval by HQDA.



# FOR OFFICIAL USE ONLY

## Chapter 5 Security Identification Cards and Badges

### 5-1. Purpose

Security identification cards and badges provide a visual means to determine if the bearer is authorized to be in a certain area. The intent of using security identification cards and badges is to combine their use with physical protective measures and other security procedural measures to increase safeguards to Army assets against espionage, sabotage, damage, destruction, and theft by controlling personnel movement in restricted areas.

### 5-2. General

a. The DOD common access card (CAC) may be used as a credential to provide access to Army spaces at the commander's determination. The CAC will not be used as a security identification badge. The CAC is a controlled item and will not be used for temporary badge issuance exchanges.

b. Determination will be made if security identification cards and badges are to be used in addition to other required identification cards for military personnel, DOD civilian employees, contractors and visitors entering installations, buildings, and other areas.

c. Security cards and badges will be designed and managed per AR 600-8-14, controlled and accounted for, and will contain—

- (1) A passport-style photograph for personnel who have been granted privileges for continuous access.
- (2) For visitors, the term VISITOR will be prominently displayed and the term ESCORT REQUIRED or ESCORT NOT REQUIRED.

d. A method to indoctrinate all assigned personnel concerning their individual security responsibilities will be established and monitored.

e. Lost cards and badges will be immediately reported to the issuing office.

### 5-3. Security card and badge computerized systems

a. Systems that generate a personal identification number (PIN) for security cards and badges will be programmed to—

(1) Identify when a card or badge is being used that has been reported lost or stolen, has not been issued, or is foreign to the system.

(2) Report the specific location of the attempted use.

(3) Deactivate the PIN for an issued card or badge.

b. Security procedural measures will be established to respond to the site of an attempted card or badge use.

c. Cards and badges will be reissued at the following rate—

- (1) Every 3 years for limited and exclusion restricted areas.
- (2) Every 5 years for controlled restricted areas. This requirement does not apply to issuance of the DOD CAC but is only for security cards and badges issued to supplement the CAC, as required by the cognizant authority.
- (3) Immediately when believed to be comprised.

d. A new PIN will be generated annually and when a replacement card or badge is issued.

## Chapter 6 Restricted Areas

### 6-1. General

a. This chapter provides guidance on the definition and designation of restricted areas within the 50 United States. Outside the continental United States (OCONUS) commanders may use information in this chapter to set local procedures according to U.S. and host nation agreements.

b. Army installations, facilities, and operational areas of civil works and like projects are restricted areas. At a minimum the type of restriction is at the level called controlled (see restricted area in the glossary).

c. Minimum requirements for controlling access to installations will be per this regulation. Minimum requirements for controlling entry to facilities will be per AR 190-51.

d. Commercial imaging surveillance by photography or video recording is prohibited at Army locations. Written procedures will be established and coordinated with supporting legal and public affairs offices, at a minimum. Procedures will establish rules for noncommercial imaging (for example, photography or video recording by Family members) and commercial imaging of events (for example, graduations and weddings).

### 6-2. Command authority

a. DODI 5200.08, per Section 797, Title 50, United States Code (50 USC 797) (Section 21 of the "Internal Security

# FOR OFFICIAL USE ONLY

Act of 1950”), authorizes military commanders to issue regulations to safeguard DOD property and places under their command. Commanders of military installations and facilities have the authority to publish and enforcement rules.

*b.* The military commander in the chain of command immediately above an installation or activity that is not headed by a military commander will enforce regulations or orders pertaining to such an installation or activity issued under the authority of 50 USC 797.

## **6–3. Prohibited actions**

*a.* A summary of pertinent sections of Title 18 of the USC follows concerning the prohibited acts announced on installation access control point (IACP) signage seen in figure 6–1.

*b.* Title 18 USC 795 prohibits photographing and sketching defense installations without permission.

*c.* Title 18 USC 797 prohibits publication and sale of photographs of defense installations without permission.

*d.* Title 18 USC 1382 restricts entering or reentering military, naval, or coast guard property for any purpose prohibited by law.

## **6–4. Security procedures concerning the prohibition on commercial image collection and surveillance**

*a.* Establish and periodically validate procedures to ensure commercial surveillance vehicles are denied access to Army installations. Installation access control personnel should be on the lookout for these vehicles and should question commercial vehicle access requests in detail. Public affairs officers should also be made aware that access is not to be granted in these cases.

*b.* Immediately report cases where access has been granted to commercial organization and/or installation imagery is available on a Web site.

*c.* Coordinate efforts within installation-level force protection working groups to provide situational awareness and promote a multidisciplined approach for countering this potential threat.

## **6–5. Perimeter controls for installations and stand-alone facilities**

*a.* Materials such as fencing will be used to channel vehicles and pedestrians to IACPs and also as a physical barrier marking the perimeter of the installation or stand-alone facility.

*b.* Where fencing is practical, the best choice for the terrain will be determined in coordination with engineers and physical security personnel. If fencing is practical, it will be per USACE standard drawing STD 872–90–03.

*c.* Other material will be used for channeling and for barriers where fencing is not practical.

*d.* Where no reasonable type of barrier material is practical (for example, along a shoreline), surveillance will be implemented in conjunction with the FPCON system.

## **6–6. Restricted area signs**

*a.* Signs or notices will be posted in conspicuous and appropriate places to identify the site as a restricted area except when such action would tend to advertise an otherwise concealed area, or when in conflict with host nation agreements. Announcement of the site as restricted will include posting signs at each entrance to the site and on perimeter fences or other boundary material.

*b.* Signs will be positioned to avoid concealment of an intruder or obstruct visual assessment by friendly forces. Failure to post conspicuous signs and notices to give persons approaching a restricted area actual knowledge of the restriction may hamper any resulting legal procedure.

(1) Signs will be posted per figure 6–1 at IACPs and facility entry control points. The following declarations, individually or in combination, may be added where applicable:

*(a)* Deadly force authorized.

*(b)* Area patrolled by military working dog (MWD) teams.

*(c)* The introduction of weapons, ammunition, or explosives or other prohibited items and photography is prohibited without specific authorization from the commander.

**WARNING**

**RESTRICTED AREA**

**THIS (INSTALLATION, ACTIVITY, ETC.) HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF THE COMMANDER IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE, 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.**

---

Figure 6-1. Warning sign for installation IACPs and facility entry control points

---

(2) Signs will be posted per figure 6-2 along property perimeters in sufficient numbers so the warning can be readily seen and understood by approaching persons.

---

**WARNING**

**RESTRICTED AREA**

**KEEP OUT**

**AUTHORIZED PERSONNEL ONLY**

---

Figure 6-2. Warning sign for property perimeters

---

(3) Both warnings notices will be posted in English. For OCONUS, the warning notices will also be posted in the host-nation language. For both continental United States (CONUS) and OCONUS, the warning notice is also encouraged to be posted in other languages predominant to the area as a safety and legal precaution.

## **6-7. National Defense Areas**

*a.* A restricted area may be established on non-Federal lands within the United States and its possessions and 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 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. Military necessity, however, will determine the final decision regarding NDA location, shape, and size.

*d.* The authority to establish a NDA includes the authority to deny access to it. It also includes the authority to

# FOR OFFICIAL USE ONLY

remove persons who threaten the orderly administration of the NDA. Any use of force employed to enforce this authority will be per AR 190–14.

## 6–8. Procedures for restricted area violations

a. The installation commander will cause any person who enters a restricted area without authority to be immediately brought 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. Questioning will be conducted without unnecessary delay.

b. If the person was unaware of the restriction, and did not acquire or intend 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 will be taken 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 (generally 3 to 4 hours), the person 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 facts with the names and addresses of witnesses and pertinent exhibits as may be available.

(2) A person subject to the Uniform Code of Military Justice will be turned over to their commander or the proper military law enforcement official.

d. Facts concerning a deliberate violation of a restricted area will be immediately reported per AR 381–12.

## Chapter 7

### Physical Security Councils, Working Groups, and Boards

#### 7–1. Purpose

The purpose of these forums at installations, commands, and HQDA is to closely coordinate actions to ensure personnel, equipment, supplies, and supporting real property are protected to the greatest extent practical.

#### 7–2. Installation or garrison physical security council

a. *Purpose.* A PSC serves as a forum through which the commander can gain community involvement in program design and implementation. The PSC will not be subordinate to antiterrorism working groups since physical security considers the entire threat spectrum, not just terrorism. The efforts of the two groups, however, should be synchronized and complimentary.

b. *Functions.* Each Army installation, area support group, U.S. Army garrison, or similar construct will establish a formal PSC to—

(1) Provide guidance for the development and distribution of the installation threat assessment (criminal and terrorist).

(2) Coordinate the development of the installation physical security plan.

(3) Evaluate the effectiveness of the installation security program and ensure regulatory compliance.

(4) Recommend priorities for the commitment of security resources to the commander.

(5) Evaluate the results of security inspections, surveys, and exercises, and recommend corrective actions.

(6) Review installation visitor control procedures.

(7) Evaluate crime prevention programs and levy specific tasks in support of these programs upon commanders or officers in charge and heads of staff agencies.

(8) Evaluate reports of significant losses or thefts and corrective actions taken.

(9) Develop security education requirements.

(10) Review existing regulations, directives, and plans to ensure that the installation can support a terrorism counteraction program suited to the local situation.

(11) Coordinate with the USACE PDC on a reimbursable basis for the review, proper application, and implementation of facilities standards and criteria to meet physical security and antiterrorism requirements.

c. *Composition.*

(1) The PM/DES/PSO will chair the PSC.

# FOR OFFICIAL USE ONLY

(2) Membership should include representatives from all tenant organizations and also key members of the installation staff (for example, resource management, operations security, intelligence, logistics, information management, and facilities management).

*d. Other forums.* Other forums such as a force protection committee or council may be used to substitute for the PSC if the requirements above are a formal part of the agenda and the group membership is equally inclusive.

## 7-3. Department of the Army Physical Security Review Board

*a. General.* The DAPSRB is an ARSTF board with advisors from ACOMs, ASCCs, DRUs, the ARNG, and other organizations.

*b. Purpose.* To ensure practical efforts are undertaken to reduce or eliminate incidents involving loss, theft, damage, or wrongful appropriation of Army property, including security of military and DA civilians and their personal property within a military facility.

*c. Functions.* Evaluate physical security concepts, management systems, doctrine, construction programs, and supporting materiel systems. Determine suitability and initiate necessary measures to establish staff responsibilities, and ensure that physical security support by the Army is effective, responsive, and attainable. To facilitate these functions, the DAPSRB—

(1) Verifies assignment and documentation of physical security responsibilities, and identifies the need for clarifying and implementing instructions to Army elements.

(2) Reviews and analyzes reports, data, and other information from all sources that might indicate the need for policy initiation or modification.

(3) In coordination with other agencies, when applicable, initiates surveys and activity evaluations to determine compliance with physical security standards and procedures.

(4) Reviews requirements and doctrine regarding PSE needs and policies to ensure Army standardization, and to ensure physical security criteria are considered in initial plans for research and development projects, as well as new or modified construction projects.

(5) Performs related analyses as directed by the Chair.

*d. Composition.*

(1) The Chief, DAPM-MPP-PS will chair the board.

(2) One voting member (O-4, O-5, or CE) or one nonvoting advisor will be provided by each of the following organizations:

*(a) Voting members.*

1. DCS, G-1.

2. DCS, G-2.

3. DCS, G-3/5/7.

4. DCS, G-4.

5. CIO/G-6.

6. Chief, Army Reserve (or HQ USARC on behalf of the Chief, Army Reserve).

7. COE (or HQ USACE on behalf of the COE).

8. ACSIM.

9. The Surgeon General.

10. ARNG.

*(b) Nonvoting advisors.*

1. ASA (ALT).

2. The Inspector General.

3. ACOMs, ASCCs, DRUs, and the ARNG.

4. Other organizations at the Chair's invitation.

*e. Administration.*

(1) The Chair will provide a nonvoting recorder and other administrative support.

(2) The DAPSRB will meet at least annually as called by the Chair.

(3) The Chair will identify voting members by name and organization at least once each meeting before votes are recorded.

(4) A simple majority will satisfy quorum requirements.

(5) Action items due for resolution will be carried by a simple majority vote.

(6) Correspondence will be sent to Headquarters, Department of the Army, (DAPM-MPP-PS), (DAPSRB Chair), 2800 Army Pentagon, Washington, DC 20310-2800.

*f. Subgroups.* Working groups subordinate to the DAPSRB may be established by the Chair as needed to consider specific requirements.

# FOR OFFICIAL USE ONLY

## 7-4. Army Physical Security Equipment Action Group

*a. Purpose.* Assist HQDA in accomplishing PSE objectives.

*b. Functions.*

- (1) Provide direction to Army PSE research, development, and acquisition programs.
- (2) Review priorities for development and procurement of PSE.
- (3) Provide priority recommendations to HQDA (DAPM-MPP-PS) or ASA (ALT) for consideration.
- (4) Ensure Army PSE development programs and inventories are continually assessed to assure they address PSE deficiencies.
- (5) Influence PSE design, installation, and maintenance policies and procedures to optimize standardization and user satisfaction.
- (6) Collaborate with other Defense organizations concerning PSE matters and provide representation to the working groups established per DODI 3224.03.
- (7) Ensure Army PSE exploratory development initiatives are incorporated by the Defense Threat Reduction Agency into their PSE exploratory development programs.

*c. Composition.*

- (1) The product manager, force protection systems will chair the APSEAG.
- (2) One voting member (O-4, O-5, or CE) or nonvoting advisor will be provided by each of the following organizations:

*(a) Voting members.*

1. OPMG.
2. DCS, G-1.
3. DCS, G-2.
4. DCS, G-3/5/7.
5. DCS, G-4.
6. CIO/G-6.
7. ACSIM.
8. The Surgeon General.
9. HQ TRADOC.
10. HQ USACE.

*(b) Nonvoting advisors.*

1. ASA (ALT).
2. ACOMs (less TRADOC), ASCCs, DRUs, and the ARNG.
3. USACE PDC.
4. USACE ESC.
5. Maneuver Support Center (U.S. Army Military Police School).
6. Other organizations at the Chair's invitation.

*d. Administration.*

- (1) The Chair will provide a nonvoting recorder and other administrative support.
- (2) The APSEAG will meet annually, or more frequently at the call of the Chair.
- (3) The Chair will identify voting members by name and organization at least once per meeting before votes are recorded.
- (4) A simple majority will satisfy quorum requirements.
- (5) Action items due for resolution will be carried by a simple majority vote.
- (6) Correspondence will be sent to the Product Manager, Force Protection Systems (APSEAG Chair), 5900 Putnam Road, Building 365, Suite 1, Fort Belvoir, VA 22060-2420.

*e. Subgroups.* Groups subordinate to the APSEAG will be established as needed to address specific equipment requirements.

(1) *Physical Security Equipment Working Group.* The PSEWG assists the APSEAG in the accomplishment of its objectives. The PSEWG reviews and continually updates Army RDT&E budget activities for 6.2 (exploratory development) PSE priority listings; reviews and recommends changes to the Army 6.3 (advanced development) and 6.4 (engineering development) PSE programs; reviews commercial and government PSE proposals of potential interest to the Army; works with other Defense organizations on PSE matters; accomplishes other PSE related tasks as directed. The PSEAG does not consider the feasibility of commercial off-the-shelf items due to the fact that equipment suitable is determined by meeting applicable requirements Defense, Army, GSA or other government specifications. The PSEWG Chair, voting members, and nonvoting advisory representatives will be per the APSEAG construct.

(2) *Intrusion Detection Systems Working Group.* The IDSWG assists the APSEAG in developing efficient processes

# FOR OFFICIAL USE ONLY

and procedures for procurement, installation, maintenance and operation of ICIDS and commercial IDS. The organization of the IDSWG Chair, voting members, and nonvoting advisory representatives will be per the APSEAG construct.

## Chapter 8 Army Access Control

### 8-1. General

a. This chapter prescribes general policies and automated system requirements for controlling access to Army installations and stand-alone facilities in CONUS and OCONUS. Installation access control is a critical aspect of the Army physical security program. Commanders responsible for installation security must clearly define access control measures consistent with DOD policy and this regulation to prevent unauthorized access. Access control restricts, and/or controls entrance to property, and/or installations to only those authorized persons and their vehicles. Persons authorized access will be either escorted or unescorted. Commanders will employ access control measures at an installation perimeter to enhance security and protection of personnel, resources, and the installation.

b. The IACPs are points at the outermost boundary of the installation (or cantonment area of large installations) where security checks can be performed on personnel, vehicles, and materials before potential threats can gain close proximity to Army assets. The IACPs consist of both passive and active barriers arranged as an integrated part of a contiguous, controlled perimeter. The IACPs and a controlled perimeter are fundamental to the Army's defense-in-depth approach to physical security. The IACPs are not facility entry control points to individual facilities.

c. The IACPs are classified by usage type as shown in table 8-1.

**Table 8-1**  
**Installation access control points types**

Use classification	Operational hours	Preferred operations
Primary	Continuous operations.	Registration of vehicles and issuance of visitor passes. Could also be designated as a truck and delivery gate.
Secondary	Less than continuous operations, but with regular operating hours.	Regular operations for visitors with authorization. Could also be designated as truck and delivery gate.
Limited use	Open only for special purposes or events.	Tactical vehicles and special events.
Pedestrian	Varies.	Personnel only. Could be located near installation housing areas or schools, or as a part of a primary or secondary IACP.

### 8-2. Security functions at primary and secondary installation access control points for commanders of host activities

Commanders are responsible for—

a. Establishing and maintaining a Visitor Control Program to ensure only authorized individuals enter the installation.

b. Establishing means to verify a person's need to have access to the installation. The CAC holders, military retirees, and military Family members have an inherent official purpose and are authorized access to Army installations. Non-CAC holder visitors, contractors, and vendors must have a DOD component-validated need for one-time, intermittent, or routine physical access to installations. The process to verify a person's need for installation access will include establishing procedures for—

(1) Unit, organization, or Servicemember sponsorship of visitors and guests.

(2) Unit, organization, or Servicemember requests to employ contractors who have an official military purpose to gain access to perform a service.

c. Screening and vetting personnel records .

(1) A check of records through the National Crime Information Center (NCIC) Interstate Identification Index (III) is the Army minimum baseline background check for entrance onto Army installations for non-CAC holders to include entrance of visitors. The FBI permits the use of NCIC III for vetting visitors to ensure the security of military installations.

(2) A similar records check will be conducted at OCONUS locations per status of forces agreement (SOFA) and other theater regulations.

d. Register vehicles as part of the access control program per AR 190-5 that states individuals who live on or require regular access to the installation for activities such as use of medical facilities and regular recurring activities

# FOR OFFICIAL USE ONLY

on the installation should register their vehicles according to a standard operating procedure established by the installation commander. Commanders responsible for installation security can grant limited temporary registration for up to 30 days, pending permanent registration, or in other circumstances for longer terms.

*e.* Implement visitor identification passes. Locally produced, temporary issue visitor identification system passes may continue to be used. Strict adherence to expiration dates and times will be given to temporary credentials as a security measure.

*f.* Implement Automated Installation Entry (AIE) when available. The AIE is being fielded in accordance with specifications in CONUS to automate authentication of personnel identification and vehicle registration information against DOD authoritative databases. Deviations from the Army AIE Standard and Specifications are not authorized without written approval from HQDA (DAPM–MPP–PS). Army organizations will not procure or field automated IACP systems of any type on Army property without prior written approval from HQDA (DAPM–MPP–PS).

(1) Existing legacy automation systems may continue to be used until replaced by AIE.

(2) The OCONUS installations utilizing the Defense Biometric Identification System (DBIDS) or the Installation Access Control System may continue to utilize these systems and provide system updates, as required.

## 8–3. Security functions at primary and secondary installation access control points

Guards will conduct the following procedures:

*a. Validate personnel identification.* Verify the identity of all personnel entering an installation. Guards will inspect by visually examining CAC, Teslin card, or locally produced, temporary visitor identification or passes to include—

(1) Visually matching the photograph with the face of the person presenting the identification.

(2) Verifying authenticity by visually checking the anti-counterfeit or fraud protection measures embedded in the credential.

(3) Authenticating identification cards using automated means at installations where the AIE is fielded.

*b. Screen vehicles.* Assess all vehicles for authorized access to the installation (for example, the vehicle is properly registered or provided a pass per installation policy and there are no obvious signs of concern).

## 8–4. Unescorted personnel

*a.* Personnel in lawful possession of a valid form of the following identification credentials are authorized unescorted access onto Army installations—

(1) DOD CAC.

(2) DD Form 2A (ACT) (Active Duty Military Identification Card), DD Form 2 (ACT) (Armed Forces of the United States-Geneva Conventions Identification Card (Active)), DD Form 2 (RES) (Armed Forces of the United States-Geneva Conventions Identification Card (Reserve)), DD Form 2 (RET) (United States Uniformed Identification Card (Retired)), DD Form 2S (ACT) (Armed Forces of the United States-Geneva Conventions Identification Card (Active)), DD Form 2S (RES) (Armed Forces of the United States-Geneva Conventions Identification Card (Reserve)), DD Form 2S (RET) (United States Uniformed Identification Card (Retired)), DD Form 2S (RES RET) (United States Uniformed Identification Card (Reserve) (Retired)).

(3) Locally issued DBIDS or DBIDS-like card for regular access.

(4) DA Form 1602 (Civilian Identification) (see para 8–4c).

(5) Local pass for temporary unescorted access. Commanders will use a locally produced, temporary issue, visitor identification system pass with expiration date pending the installation of AIE or DBIDS.

*b.* Guidance.

(1) The DBIDS, DBIDS-like card, and local passes will only be issued to non-DOD cardholder personnel who successfully pass an NCIC check and meet the vehicle registration requirements of AR 190–5, but otherwise do not meet the requirement for issuance of a CAC or DOD Teslin card.

*(a)* This applies to contractors and vendors who are sponsored as having an official purpose and are approved for access by the installation commander or designated representative.

*(b)* Contractors and vendors requiring physical access to a single Army installation or facility longer than 24 hours but do not require logical access to a DOD computer network, will have a government employee sponsor who will provide the contractual agreement with a cover memorandum signed by a verifying officer vouching for the need to possess a long term DBIDS card. The expiration date of the credential will be the end date of the contract or visit, or the expiration date of the sponsor's credential, whichever occurs first.

*(c)* Contractors will be processed through the contractor verification system for issuance of a CAC if physical access to an Army installation and logical access to a DOD computer network are both required.

(2) A DBIDS or DBIDS-like card will only be issued for routine physical access onto the single installation or facility where it is issued.

(3) Personnel with personal identity verification credentials per Federal Information Processing Standards (FIPS) 201, DBIDS cards, and DBIDS-like cards will undergo an NCIC III check.



# FOR OFFICIAL USE ONLY

(4) Search procedures and random antiterrorism measures (RAM) apply to personnel to whom a DBIDS or DBIDS-like card is issued.

c. Family care providers and Army volunteers will be issued a DBIDS card, a DBIDS-like card, or a DA Form 1602 if there is a consistent, recurring need to access the installation according to the following guidance.

(1) Unit commanders will use the Family care plan per AR 600–20 to review and validate requests by Soldiers to grant installation access to Family care providers.

(2) The director of an activity will review and validate requests to grant for installation access for Army volunteers.

(3) Requests will be forwarded through the installation commander (also the installation volunteer coordinator for Army volunteers) to the office responsible for issuance of a DBIDS or DBIDS-like credential, or DA Form 1602, and to the office responsible for vehicle registration per AR 190–5.

(4) Vehicle registration decals and identification cards for Family care providers and Army volunteers are valid for no more than 1 year. Installation commanders may extend the authorization as long as the unit commander or activity director certifies that the Family care provider or Army volunteer continues in a satisfactory status.

d. Current forms of OCONUS identification may continue to be used per SOFA.

e. The OCONUS installations will continue to initiate background checks and allow installation access to foreign nationals, contractors, and vendors per SOFA and other theater regulations.

## 8–5. Escorted personnel

a. Non-DOD affiliated personnel will be escorted while on the installation, as determined by local policy.

b. A valid state driver's license, state identification card with photo, or a valid U.S. passport, or a valid passport from other countries cleared by the State Department will be presented to request access to an Army installation.

c. Personnel will be checked per paragraph 8–2c.

d. Official foreign visitors subject to provisions of Army policy concerning foreign disclosure and contacts with foreign representatives will be cleared per AR 380–10, receive a NCIC III check prior to entering the installation, and will be escorted.

## 8–6. Special event access control measures

a. Commanders with installation security responsibilities will clearly define the access control measures required to manage special events on the installation. They will define these measures in the Installation Area Access Control Plan per paragraph 8–10.

b. A NCIC III screening for personnel attending special events and activities may be waived where screening is impractical.

c. Compensatory security measures for special events will be implemented when the requirements of this regulation cannot be met. Examples are—

(1) Isolating event traffic and parking to specific locations or areas on the installation.

(2) Transporting attendees to and from the event site by government transportation.

(3) Directing, at minimum, individuals (with no DOD credential per para 8–3) attending a large function on the installation (for example, football games, 4th of July, air shows, graduations, concerts) to the specific gate(s) where security measures are conducted prior to entrance onto the installation.

d. Hand-held identification scanning technology may be used, and depending on the FPCON or local threat, may also include random vehicle checks by MWDs and the deployment of magnetometers at the event site.

## 8–7. Installation access control point automation design requirements

Commanders will comply with the following guidance regarding access control automation:

a. The use of an AIE System will be per the Army Standard for Automated Installation Entry and the Army Automated Installation Entry System Specifications. Deviations from the standard and specifications are not authorized without prior written approval from HQDA (DAPM–MPP–PS).

b. Automated systems designed per the AIE standards and specifications and approved by HQDA (DAPM–MPP–PS) will be installed to control entry onto Army installations. This requirement includes HQDA approval for the use of DBIDS.

c. Existing legacy systems may continue to be used until replaced by AIE.

d. Only IACP automated systems designed and installed per paragraph 8–2 may be installed and utilized to authorize entry onto Army installations.

e. All Army IACP automation must be compliant with FIPS 201, DODD 1000.25, and DODD 8190.3.

f. The IACP automation must meet DIACAP requirements and all DOD privacy policy and Freedom of Information Act requirements per the AIE Standards and Specifications. Commanders will ensure visitor control procedures implement these privacy mandates.

# FOR OFFICIAL USE ONLY

g. Implementation of AIE. The product manager, force protection systems and USACE will execute the HQDA centrally managed IACP Program per written direction of HQDA (DAPM-MPP-PS).

## 8-8. Trusted Traveler Program

a. Installation commanders may initiate a Trusted Traveler Program (TTP) upon the commissioning of an AIE system.

b. The TTP allows for uniformed Servicemembers and spouses, DOD employees, and retired uniformed Servicemembers and spouses to vouch for occupants in their immediate vehicle, provided the Trusted Traveler vehicle operator possesses a valid identification card and has a clear NCIC III check. The intent of the TTP is to—

(1) Expedite access to Army installations for uniformed Servicemembers and spouses, DOD employees, and retired uniformed Servicemembers and spouses.

(2) Provide a high degree of security with faster vehicle throughput.

(3) Mitigate traffic congestion on adjoining highways.

(4) Provide the flexibility for trusted travelers to vouch for Family members and official visitors.

(5) Reduce guard force manpower.

c. The TTP is not authorized for military dependants (except for spouses), contractors, volunteers, or Family care providers.

d. The TTP does not authorize vehicle occupants to enter a MEVA, defense critical asset, task critical asset, or limited area, or exclusion area without first meeting the security requirements and procedures for those areas.

e. Trusted travelers are entirely responsible for the actions of all occupants in their vehicle and for meeting all local security requirements for escort as established by Army regulations and requirements of the installation commander.

f. Trusted travelers cannot vouch for persons with foreign passports or identification cards who must, instead, be cleared per paragraph 8-2 of this regulation.

g. Vehicle occupants who are 10 years of age or older must be in possession of a valid picture identification card (for example, drivers license, state identification, DD Form 1173 (Uniform Services Identification and Privilege Card), DD Form 2 series, passport) issued by an authoritative agency (state/Federal) so they can be readily identified while on the installation. Occupants below the age of 18 who do not possess a valid picture identification card may be vouched for by an adult occupant of the vehicle who has been cleared to enter the installation.

h. Commanders at their discretion may suspend the TTP based on the local threat or may revoke individual trusted traveler privileges.

i. The TTP will be suspended at FPCON Charlie and Delta. Commanders will ensure the Installation Area Access Control Plan reflects procedures when the TTP is suspended.

j. Persons registering for trusted traveler status will register at the visitor control center, PMO/DES, or other designated registration office. The trusted traveler token and vehicle registration information will be registered into the AIE database.

k. During the registration process, personnel from the visitor control center, PMO/DES, or other designated registration office will electronically authenticate that the registrant's driver's license is valid and conduct an NCIC III check.

## 8-9. Construction standards

a. Facility construction and road work for IACPs will be per the Army standard for access control points. Deviations from the standard are not authorized without prior written approval per AR 420-1.

b. Planners will coordinate with USACE and the Surface Deployment and Distribution Command Traffic Engineering Agency on IACP projects that may affect adjoining public roads, and also coordinate with state and local authorities during all phases of an IACP project.

c. For OCONUS installations, designers will coordinate with USACE and the host nation government agencies and the appropriate SOFA subcommittee.

## 8-10. Installation area access control plan

An area access control plan will be implemented, will clearly define access control measures required to safeguard facilities and accomplishment of the mission, will be synchronized with AT plans, and will contain, at a minimum—

a. A defense-in-depth concept to provide graduated levels of protection from the installation or activity perimeter to critical assets that includes—

(1) The use of physical or natural barriers, gates, electronic security system, and guards deployed to detect, delay, and deny entry to unauthorized personnel or vehicles at the activity perimeter.

(2) The designation of and supplemental protection for critical and high risk assets and restricted areas.

b. Access control measures that include but are not limited to—

(1) Armed sentries.

(2) Active barriers capable of stopping unauthorized entry of suspect vehicles per the Army Standard for access control points and the OPMG criteria included with the Army Access Control Points Standard Definitive Design.

# FOR OFFICIAL USE ONLY

- (3) Procedures to search for and detect explosives and other prohibited items.
- (4) Provisions to reject unauthorized personnel or vehicles that have penetrated the installation perimeter.
- (5) Closing all nonoperational IACPs to include locking them with approved locking devices or having barriers installed that preclude entry and exit.
- (6) The degree of control required over personnel and equipment entering or leaving the installation and restricted areas within it. This must include a description of access control measures in use and the method for establishing authorization for entering and leaving each area, as it applies to both personnel continually authorized access to the area and to visitors, including any special provisions concerning non-duty hours.
- (7) Use of security badges and military identification cards, CAC and DBIDS or DBIDS-like cards, to include—
  - (a) Details of where, when, and how they will be displayed for access control.
  - (b) Procedures to be followed in cases of loss, theft, forgery, or damage.
  - (c) Replacement procedures.
- (8) Procedures for inspecting persons, their property, and vehicles at entry and exit points of installations and restricted areas including:
  - (a) When and how frequently inspections are conducted, and whether they are random or mandatory for all.
  - (b) Legal review by the appropriate legal advisor prior to issuance.
  - (c) Use of RAM within existing security operations to reduce patterns, change schedules, and visibly enhance the security profile of the installation.
  - (d) Emergency plans for increased vigilance and restricting access at installations for national emergencies, natural and manmade disasters, heightened FPCON, significant criminal activity, civil disturbance, and other contingencies that would seriously affect the ability of installation personnel to perform their mission.
  - (e) Process for coordinating with local, state, Federal, or host country officials as well as tenant organizations to ensure integrity of restricted access to the installation and reduce the impact on primary missions and surrounding civilian communities.
- (9) Maintenance of adequate physical barriers that will be installed to control access to the installation or restricted area.
- (10) Designation of posts, personnel, equipment, and other resources to enforce restricted access and response to incidents.
- (11) Process for removal of, or denying access to persons who are not authorized or are a threat to order, security, and discipline.
- (12) Annual exercise of contingency plans, including systems for alerting and evacuation of personnel.
- (13) A mechanism to keep appropriate personnel informed of the plan and their responsibilities.
- (14) The number, design, and placement of IACPs, to include gatehouses, approach routes, barriers, sentry posts, and vehicle control devices will be constructed per the Army Access Control Point Standard Definitive Design.
- (15) The number of vehicular IACPs should be kept to a minimum, and plans should consider—
  - (a) Traffic volume.
  - (b) Traffic patterns to limit high-speed approaches to IACPs.
  - (c) The IACP designated for employees only, with others reserved for visitors and delivery vehicles.
  - (d) Perimeter protection measures adjacent to IACPs.
  - (e) Response planning for gate runners.
  - (f) Protection against reverse entry and ramming attacks.
  - (g) Protected guard positions.
  - (h) Controlled parking areas for visitor parking and use in vehicle inspections that are inside jurisdictional boundaries, but preferably outside the perimeter fencing and barriers.
  - (i) Road patterns to enable vehicle queuing, and turnaround of unauthorized vehicles outside of the final vehicle barrier system in such a way as to prevent them from gaining access.
  - (j) Vehicle by-pass control.
  - (k) Gate area lighting.
  - (l) Pass office location.
- (16) Use of temporary traffic lanes outside the installation perimeter for traffic congestion resulting from business rush hours and increased security measures implemented during heightened threat conditions.
- (17) Conduct annual exercises of entry control contingency plans, including—
  - (a) Response to gate runners.
  - (b) Procedures for alerting emergency dispatch and command personnel.
  - (c) Transition to heightened FPCON.
  - (d) Implementation of RAM.
- (18) Response to natural and manmade disasters that include—
  - (a) Commuting procedures and entry requirements for critical personnel.

# FOR OFFICIAL USE ONLY

(b) Phased and rapid evacuation of personnel from facilities and installations.

(c) Response to sabotage or unintentional deactivation of installation and restricted area perimeter electronic security system (where required) or automated entry control system.

(19) Conduct random vehicle inspections (frequency to be determined by the Garrison commander) of all privately owned vehicles and commercial vehicles that enter onto the installation for prohibited items by utilizing explosives detecting devices and equipment such as hand-held vapor tracers, vehicle and cargo inspection systems, or MWDs.

c. The use of RAM, in conjunction with site-specific FPCON measures in a manner that portrays a robust, highly visible and unpredictable security posture from which security patterns or routines cannot be easily discerned.

## **8–11. Installation access control point security forces**

a. The IACPs will be manned by armed security force personnel (Soldiers, DA civilian police, DA security guards, or contract guards) as permitted by applicable Federal, state, and territorial statutes, and SOFA.

b. Commanders will use HQDA (DAPM–MPP–PS) IACP staffing guidance for manpower considerations to determine the appropriate manpower for primary and secondary IACPs.

c. Security forces will be provided with—

(1) Adequate means of communications.

(2) Appropriate weapons and ammunition and trained in their care and use per AR 190–14.

(3) Personal protective equipment.

d. Procedures will be established for each IACP, and will be reviewed at least annually and revised, as necessary.

e. Training and weapons qualification of security force personnel will be in accordance with applicable directives, AR 190–56 for all assigned DA police and DA guards, and the statement of work for contract security guards.

f. Training will also include—

(1) Recognition of sabotage-related devices and equipment that might be used against the installation.

(2) Use of devices to identify sabotage-related devices and equipment such as hand-held vapor tracers and vehicle and cargo inspection systems.

(3) Authorized forms of identification for access to the installation.

## **8–12. Outside the continental United States provisions**

The OCONUS commanders may continue to use current forms of identification, and continue background checks to allow installation access to foreign nationals, contractors, and vendors per SOFA and other theater regulations.

## **8–13. Controlling entry of privately owned arms and ammunition**

a. Privately owned arms and ammunition on Army property is prohibited unless authorized by the installation commander per AR 190–11.

b. Signs announcing this prohibition will be posted at IACPs.

c. This prohibition does not apply to the lawful performance of official duties by a sworn officer, agent, or employee of the United States, a state, or a political subdivision thereof, or host nation who is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law or security duties.

d. Procedures will be established and punitive measures will be publicized to regulate privately owned arms and ammunition on the installation to include—

(1) Mandatory registration and storage of weapons belonging to personnel living on the installation.

(2) Carrying and use of weapons by hunters, and recreational and marksmanship shooters using installation firing ranges.

(3) Identification of prohibited weapons (for example, nunchucks and throwing stars).

## **Chapter 9**

### **Physical Security Equipment Planning**

#### **9–1. System certifications**

a. The PSE that physically or logically connects to the global information grid (GIG) will comply with DIACAP and other certifications, as required.

b. The PSE configured as a stand-alone system does not require DIACAP but should undergo a recurring vulnerability test to validate operational security. For the purpose of this policy, a stand-alone system is one that is operational without requiring external support except for power, and does not connect to or interact with the GIG. Standards for a recurring vulnerability test will be determined in coordination with the supporting Network Enterprise Center and equipment manufacturer.

c. The PSE sustainment is the responsibility of the organization operating the equipment.

# FOR OFFICIAL USE ONLY

## 9-2. Intrusion Detection System

*a.* The IDS is a technology substitute for continuous armed surveillance required for certain assets (for example, AA&E stored in certain configurations), or for constant manning (for example, an information processing facility, or facility where controlled medical substances are stored). In general, IDS is required for assets that are dangerous or are of unique importance to national defense or to the Army mission. The IDS and electronic security system are not routine requirements for Army facilities or areas, but rather for assets when specifically prescribed in policy.

*b.* The HQDA centrally plans IDS replacement based on asset criticality and system age. The IDS will be replaced on a 10-year life cycle to the greatest extent possible and continuously sustained.

*c.* The ICIDS is the standardized DOD IDS intended for use by organizations where technically feasible. The initial installation of ICIDS is centrally managed by product manager, force protection systems. The using organization or supporting garrison per memorandum of agreement is thereafter responsible for system sustainment.

*d.* Commercial IDS may be used if ICIDS does not satisfy a specific technology requirement. The IDS design and installation of IDS will be per unified facilities guide specification (UFGS) 28 20 01.00 10.

*e.* For specific IDS or electronic security system capabilities and system configuration, refer to the governing policy for the assets under consideration (for example, AA&E, nuclear, chemical) for design, installation, monitoring, and sustainment criteria.

*f.* An inspection will be conducted by qualified technical personnel to ensure the system meets all minimum acceptable standards before a new IDS is accepted for operation. DA Form 4604 (Security Construction Statement) will be used to record acceptance by the commander or designated representative.

*g.* A record of all alarms received will be maintained for at least 90 days. DA Form 4930 (Alarm/Intrusion Detection Record) may be used as an option to record alarm activations if the IDS does not provide an automated report with sufficient information.

*h.* Keys to IDS components will be safeguarded and accounted for per AR 190-51. Keys to IDS components used to protect AA&E will be safeguarded and accounted for per AR 190-11.

*i.* The IDS signs.

(1) Areas with IDS will have warning signs prominently displayed. Whenever possible, IDS signs will be mounted at eye level on the outside of each interior and the outside of each exterior door leading into the protected area.

(2) An example of IDS warning sign is provided in figure 9-1. The sign is flat with shape, size, and with a legend as shown. The sign face should consist of reflectorized sheeting bonded to an aluminum backing. The sign backing is flat, degreased, etched, and unpainted aluminum alloy, type 6061T6, not less than 1/16-inch thick. Plastic or wood may be used for interior posting.

(3) The IDS signs will be posted in English and in the host nation language. Other languages predominant in the area are also encouraged as a safety and legal precaution.

(4) For assets requiring a perimeter IDS (see asset specific regulations), warning signs will not be affixed to sensor fences to avoid false and nuisance alarms.

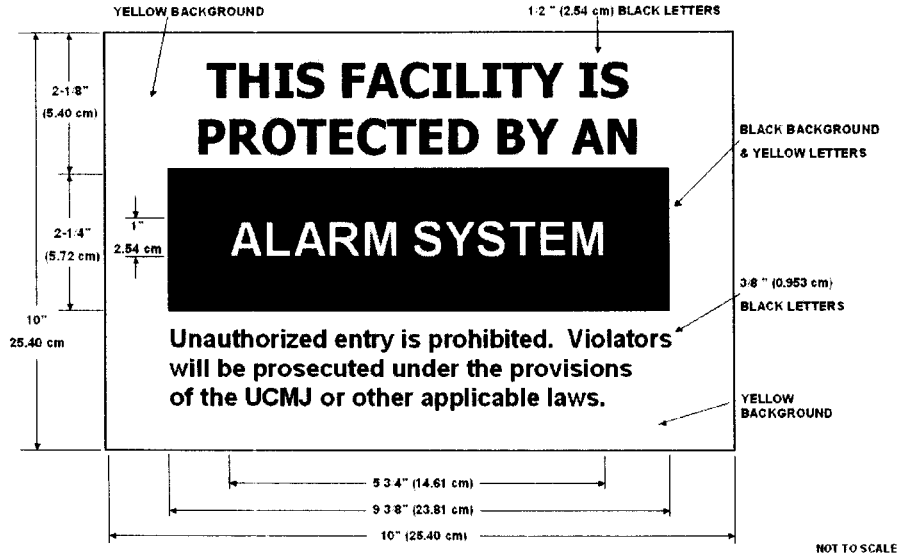


Figure 9-1. IDS warning sign

## Chapter 10 Security Forces

### 10-1. General

A security patrol, guard patrol, or unit personnel will periodically check facilities and areas used to store sensitive or critical items or equipment.

*a.* Security checks will be conducted on an irregular basis during non-duty 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.

*b.* Security patrols will physically inspect doors and locks on all storage structures in their area of responsibility during periods of increased vigilance because of a threat situation.

*c.* Selection of personnel to perform guard duties will be closely monitored by commanders or designated representatives to ensure only properly trained and reliable persons are assigned duty. Supervisory checks will be conducted to ensure guard duties are properly performed.

*d.* Security patrols may be conducted by military personnel, civilian security personnel, contracted personnel, the U.S. Marshal Service, or state, local, or campus police.

*e.* Department of the Army controlled security forces will be provided with adequate means of communication.

*f.* Security forces may be armed with appropriate weapons and ammunition at the discretion of the commander concerned. Provisions in AR 190-14 apply if personnel are armed.

### 10-2. Personnel selection and training

For DA civilian personnel, provisions for selection, hiring, and minimum training requirements will be per AR 190-56

### 10-3. Procedures

Guard procedures will be reviewed at least annually and revised as needed to provide greater application of security measures. Special emphasis will be placed on guard post locations and guard orientation concerning required duties.

### 10-4. Inspections and guard checks

Inspections and checks of guards will be increased during nights, weekends, and holidays based on local threat and as determined by the commander to provide for deterrence of violations and for the early detection of asset loss. Checks

# FOR OFFICIAL USE ONLY

will be recorded and will consist of an inspection of the building, facility or area, including all doors and windows. Records of checks will be maintained for a minimum of 90 days.

## **10-5. Patrol plans**

Security patrol plans will be coordinated and integrated with the guard plan or other security plans and programs to the maximum extent. When facilities are located in civilian communities, liaison will be established with local civil police for periodic surveillance and to coordinate a security plan.

# FOR OFFICIAL USE ONLY

## Appendix A References

### Section I Required Publications

#### AR 190-5

Motor Vehicle Traffic Supervision (Cited in paras 8-2*d*, 8-4*b*(1), 8-4*c*(3).) (Available at <http://www.apd.army.mil/>.)

#### AR 190-11

Physical Security of Arms, Ammunition, and Explosives (Cited in paras 2-14*d*(3), 2-15*b*(1), 8-13*a*, 9-2*h*.) (Available at <http://www.apd.army.mil/>.)

#### AR 190-51

Security of Unclassified Army Property (Sensitive and Nonsensitive) (Cited in paras 1-24*j*(4), 6-1*c*, 9-2*h*.) (Available at <http://www.apd.army.mil/>.)

#### AR 215-8

Army and Air Force Exchange Service Operations (Cited in para 4-3*c*(1).) (Available at <http://www.apd.army.mil/>.)

#### DA Pam 190-51

Risk Analysis for Army Property (Cited in paras 1-24*j*(4), 2-5*a*, 2-7*a*, 2-7*b*(8), 2-11*a*, 2-18*a*(5).) (Available at <http://www.apd.army.mil/>.)

#### DODD 5105.55

Defense Commissary Agency (DeCA) (Cited in para 4-3*c*(2).) (Available at <http://www.dtic.mil/whs/directives/>.)

### Section II Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

#### AR 1-1

Planning, Programming, Budgeting, and Execution System

#### AR 10-87

Army Commands, Army Service Component Commands, and Direct Reporting Units

#### AR 25-2

Information Assurance

#### AR 25-55

The Department of the Army Freedom of Information Act Program

#### AR 37-49

Budgeting, Funding, and Reimbursement for Base Operations Support of Army Activities

#### AR 70-1

Army Acquisition Policy

#### AR 71-9

Warfighting Capabilities Determination

#### AR 190-14

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

#### AR 190-17

Biological Select Agents and Toxins Security Program



# FOR OFFICIAL USE ONLY

**AR 190-30**

Military Police Investigations

**AR 190-54**

Security of Nuclear Reactors and Special Nuclear Materials

**AR 190-56**

The Army Civilian Police and Security Guard Program

**AR 190-59**

Chemical Agent Security Program

**AR 340-21**

The Army Privacy Program

**AR 380-5**

Department of the Army Information Security Program

**AR 380-10**

Foreign Disclosure and Contacts with Foreign Representatives

**AR 380-86**

Classification Of Former Chemical Warfare, Chemical And Biological Defense, And Nuclear, Biological Chemical Contamination Survivability Information

**AR 381-12**

Subversion And Espionage Directed Against The U.S. Army (SAEDA)

**AR 420-1**

Army Facilities Management

**AR 525-13**

Antiterrorism

**AR 530-1**

Operations Security (OPSEC)

**AR 600-8-14**

Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel

**AR 600-20**

Army Command Policy

**AR 690-950**

Career Management

**AR 700-127**

Integrated Logistic Support

**DA General Order 2003-09**

Establishment of the Office of the Provost Marshal General

**DeCA Directive 30-18 (C5)**

Defense Commissary Agency Security Programs (Available at <https://www.us.army.mil/suite/doc/13937758>.)

**DOD 5200.1-R**

Information Security Program (Available at <http://www.dtic.mil/whs/directives/>.)

**DOD 5200.08-R**

Physical Security Program (Available at <http://www.dtic.mil/whs/directives/>.)

# FOR OFFICIAL USE ONLY

## **DODD 1000.25**

DOD Personnel Identity Protection (PIP) Program (Available at <http://www.dtic.mil/whs/directives/>.)

## **DODD 8190.3**

Smart Card Technology (Available at <http://www.dtic.mil/whs/directives/>.)

## **DODI 3224.03**

Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E) (Available at <http://www.dtic.mil/whs/directives/>.)

## **DODI 5200.08**

Security of DOD Installations and Resources and The DOD Physical Security Review Board (PSRB) (Available at <http://www.dtic.mil/whs/directives/>.)

## **EOP 16-1**

Exchanges operating procedures: AAFES Security (Available at <https://www.us.army.mil/suite/doc/13783119>.)

## **FED-STD-809A**

Federal Standard: Neutralization and repair of GSA approved containers (Available at <https://assist.daps.dla.mil/quicksearch/>.)

## **FIPS 201**

Federal Information Processing Standards 201 (Available at <http://www.itl.nist.gov/fipspubs/>)

## **MIL-STD-3007F**

Department of Defense Standard Practice For Unified Facilities Criteria And Unified Facilities Guide Specifications (Available at <https://assist.daps.dla.mil/quicksearch/>.)

## **SDDCTEA Pam 55-15**

Traffic and Safety Engineering for Better Entry Control Facilities (Available at <http://www.tea.army.mil/pubs/dod.asp>.)

## **International Security Act of 1950**

War And National Defense (Available at <http://uscode.house.gov/search/criteria.shtml>.)

## **STD 872-90-03**

Standard Drawing: FE6 Chain-Link Security Fence Details for Non-Sensored Fence (Available at <https://pdc.usace.army.mil/library/drawings/fence>.)

## **UFC 4-010-01**

Unified Facilities Criteria: DOD Minimum Antiterrorism Standards for Buildings (Available at [http://www.wbdg.org/references/pa\\_dod.php](http://www.wbdg.org/references/pa_dod.php).)

## **UFC 4-010-02**

Unified Facilities Criteria: DOD Minimum Antiterrorism Standoff Distances for Buildings (FOUO) (Available at [http://www.wbdg.org/references/pa\\_dod.php](http://www.wbdg.org/references/pa_dod.php).)

## **UFC 4-020-01**

Unified Facilities Criteria: DOD Security Engineering Facilities Planning Manual (Available at [http://www.wbdg.org/references/pa\\_dod.php](http://www.wbdg.org/references/pa_dod.php).)

## **UFC 4-022-01**

Unified Facilities Criteria: Security Engineering: Entry Control Facilities/Access Control Points (Available at [http://www.wbdg.org/references/pa\\_dod.php](http://www.wbdg.org/references/pa_dod.php).)

## **UFGS 28 20 01.00 10**

Unified facilities guide specification: Electronic Security System (Available at [http://www.wbdg.org/ccb/browse\\_org.php?o=70](http://www.wbdg.org/ccb/browse_org.php?o=70).)

## **18 USC 795**

Photographing and sketching defense installations (Available at <http://uscode.house.gov/search/criteria.shtml>.)

# FOR OFFICIAL USE ONLY

## **18 USC 797**

Publication and sale of photographs of defense installations (Available at <http://uscode.house.gov/search/criteria.shtml>.)

## **18 USC 1382**

Entering military, naval, or Coast Guard property (Available at <http://uscode.house.gov/search/criteria.shtml>.)

## **18 USC 3041**

Penalty for violation of security regulations and orders (Available at <http://uscode.house.gov/search/criteria.shtml>.)

## **50 USC 797**

War And National Defense (Available at <http://uscode.house.gov/search/criteria.shtml>.)

### **Section III**

#### **Prescribed Forms**

Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the Army Publishing Directorate Web site at <http://www.apd.army.mil>.

#### **DA Form 2806**

Physical Security Survey Report (Prescribed in para 2–14c.)

#### **DA Form 2806–1**

Physical Security Inspection Report (Prescribed in para 2–15a.)

#### **DA Form 4261 and DA Form 4261–1**

Physical Security Inspector Identification Card (Prescribed in para 3–5.)

### **Section IV**

#### **Referenced Forms**

Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the Army Publishing Directorate web site (<http://www.apd.army.mil>). DD Forms are available from the OSD Web site (<http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>).

#### **DA Form 11–2**

Internal Control Evaluation Certification

#### **DA Form 1602**

Civilian Identification

#### **DA Form 2028**

Recommended Changes to Publications and Blank Forms

#### **DA Form 4604**

Security Construction Statement

#### **DA Form 4930**

Alarm/Intrusion Detection Record

#### **DD Form 2A (ACT)**

Active Duty Military Identification Card (Available through normal forms supply channels.)

#### **DD Form 2 (ACT)**

Armed Forces of the United States-Geneva Conventions Identification Card (Active) (Available through normal forms supply channels.)

#### **DD Form 2 (RES)**

Armed Forces of the United States-Geneva Conventions Identification Card (Reserve) (Available through normal forms supply channels.)

#### **DD Form 2 (RET)**

United States Uniformed Identification Card (Retired) (Available through normal forms supply channels.)

# FOR OFFICIAL USE ONLY

## **DD Form 2S (ACT)**

Armed Forces of the United States-Geneva Conventions Identification Card (Active) (Available through normal forms supply channels.)

## **DD Form 2S (RES)**

Armed Forces of the United States-Geneva Conventions Identification Card (Reserve) (Available through normal forms supply channels.)

## **DD Form 2S (RET)**

United States Uniformed Identification Card (Retired) (Available through normal forms supply channels.)

## **DD Form 2S (RES RET)**

United States Uniformed Identification Card (Reserve) (Retired) (Available through normal forms supply channels.)

## **DD Form 1173**

Uniform Services Identification and Privilege Card

## **Appendix B Physical Security Plan**

### **B-1. General**

The following will be used in the preparation of a physical security plan. Portions may not be applicable to a specific location or organization, and local requirements may require inclusion of additional material. Care will be taken to mark pertinent portions for classification per applicable policy.

### **B-2. Classification and authority**

Cite the overall security classification of the plan and the authority for the classification.

### **B-3. Name and location of the facility**

Self-explanatory.

### **B-4. Mission of the facility**

Self-explanatory.

### **B-5. Purpose**

Cite a brief purpose of the plan. The plan should integrate all forces, devices, and equipment into an effective security system.

### **B-6. Objectives**

Cite the objectives of the plan (for example, protection of chemical assets from sabotage or unauthorized access).

### **B-7. Analysis of external and internal threat**

Analyze threats against assets. Review and consider the postulated threat. Consider the tactics and associated weapons, tools, and explosives that aggressors are likely to use. Review and evaluate local threat information obtained from intelligence, counterintelligence, and law enforcement sources. Consider any recent related or unrelated security incidents that may bear on the overall threat analysis.

### **B-8. Vulnerabilities**

Review results of the latest site vulnerability assessment. Identify critical structures, containers, buildings, and work areas in which assets require protection. Consider their location, size, function, and contents even if they are only occasionally used. Consider aggressor tactics included in the threat analysis.

### **B-9. Priorities**

Establish priorities for protecting various asset areas.

### **B-10. Controlled, limited, and exclusion areas**

Delineate these areas.

# FOR OFFICIAL USE ONLY

## **B-11. Equipment and devices to detect or delay intrusion**

Identify equipment and devices to detect or delay intrusion.

*a. Perimeter boundary.*

- (1) Type.
- (2) Construction.

*b. Clear zones.*

- (1) Widths.
- (2) Surface undulations and ditches.
- (3) Obstacles such as poles, trees, boulders, structures that could not be relocated or removed.
- (4) Culverts, utility tunnels, and other structures.

*c. Gates.*

- (1) Type and construction of personnel and vehicle gates.
- (2) Locations.
- (3) Hours of operation.
- (4) Locking means and procedures.

*d. Signs.*

(1) Types such as no trespassing, persons and vehicles subject to search, use of deadly force, and bilingual when appropriate.

(2) Location.

*e. Inspection or maintenance.* Identify types of inspection or maintenance.

## **B-12. Security lighting**

Identify types of lighting used and current procedures.

*a.* Types such as area, glare projection, controlled, and portable.

*b.* Type of light source such as low or high pressure sodium vapor, mercury vapor, or incandescent.

*c.* Use, control, and standards (foot candles or lumens).

- (1) Perimeter.
- (2) Gates.
- (3) Interior areas and structures.

*d.* Inspections and maintenance.

*e.* Emergency actions for power failure.

*f.* Emergency generator type, location, fuel supply, operating instructions, testing procedures, and maintenance requirements.

*g.* Emergency backup lighting operating instructions.

## **B-13. Intrusion Detection System**

Identify the system to be used and required procedures.

*a.* Types.

*b.* Locations.

*c.* Procedures for operation, monitoring, and activation or deactivation.

*d.* Tests and antitamper procedures.

*e.* Inspections and maintenance.

*f.* Record logs.

*g.* Actions by security force when alarms occur or when the alarm system, or any part of the system, becomes inoperative.

*h.* Duress system.

*i.* Warnings and alarms.

*j.* Emergency or backup power sources.

## **B-14. Communications**

Identify communication system procedures.

*a.* Types.

*b.* Locations.

*c.* Use.

*d.* Tests.

*e.* Inspections and maintenance.

*f.* Record logs.

# FOR OFFICIAL USE ONLY

- g. Emergency or backup power sources.

## **B-15. Locks and keys**

Identify locks, keys, and procedures.

- a. Types.
- b. Use.
- c. Locations.
- d. Maintenance and rotation.
- e. Controls, logs, accountability.
- f. Two-person control keys.

## **B-16. Delay systems**

Identify delay systems and procedures.

- a. Types.
- b. Locations.
- c. Total delay time provided (for example, aggressor time needed to gain access to protected assets).
- d. Inspections and maintenance.

## **B-17. Security procedures during construction, renovation, or extensive maintenance**

Provide instruction when applicable.

## **B-18. Measures to control personnel vehicles and material**

Determine what personnel and vehicle movement restrictions are required for each critical area or structure (for example, limited area, exclusion area, material access area).

- a. Personnel access controls.
  - (1) Assigned personnel.
  - (2) Visitors.
  - (3) Maintenance personnel (government and contractors).
- b. Escort requirements.
- c. Search and seizure procedures.
- d. Duress system.
- e. Nonoperational hours access procedures.
- f. Emergency entrance procedures for fire, security, asset disposal, and medical personnel.

## **B-19. Personnel identification system**

Personnel recognition and identification cards or badges for assigned personnel, visitors, and maintenance personnel.

- a. Identification cards.
- b. Badges.
- c. Entry control rosters.

## **B-20. Vehicle control**

Identify delay systems and procedures.

- a. Search and seizure procedures.
- b. Parking locations during duty and non-duty hours (include security requirements).
- c. Restrictions and control on privately owned, government, contractor, maintenance, and commercial vehicle.
- d. Procedures for emergency vehicles for security, fire, and medical.
- e. Registration, if applicable.

## **B-21. Material control**

Identify requirements for controlling material.

- a. *Incoming.*
  - (1) Requirements for admission, to include restrictions.
  - (2) Inspection, search, and seizure.
  - (3) Sealed packages and containers.
- b. *Outgoing.*
  - (1) Documentation required.
  - (2) Inspection, search, and seizure.

# FOR OFFICIAL USE ONLY

*c. Classified.* Classified documents or materials, controls, and procedures for incoming and outgoing, to include emergency destruction.

## **B-22. Security forces**

Identify procedures for the security force.

- a.* Type—military, civilian, and contractor (U.S. and foreign).
- b.* Composition and organization.
- c.* Authority and jurisdiction.
- d.* Weapons, ammunition, and equipment.
- e.* Rules of engagement and use of deadly force (include fixed wing aircraft and helicopter assault).
- f.* Training.
- g.* Actions to be taken under adverse weather and limited visibility conditions.
- h.* Posts.
  - (1) Locations.
  - (2) Areas of responsibility.
  - (3) Hours.
  - (4) Duties and functions, including general patrol routes (vary patrol routes and rotate stationary posts to combat boredom).
  - (5) Reporting procedures.
  - (6) Employment of MWD (if applicable).
- i.* Response force.
  - (1) Purpose and mission.
  - (2) Size, composition, and organization.
  - (3) Weapons, ammunition, and equipment.
  - (4) Location and call-out procedures.
  - (5) Reaction times.
  - (6) Protection of response vehicles from sabotage.
  - (7) Protected response means and alternate routes.
  - (8) Actions for multiple site intrusions.
  - (9) Training, including frequency of testing.
- j.* Augmentation force.
  - (1) Purpose and mission.
  - (2) Size, composition, and organization.
  - (3) Weapons, ammunition, and equipment.
  - (4) Location and call-out procedures.
  - (5) Response time.
  - (6) Tactical plan (attach as an appendix).
  - (7) Other supporting security forces. Identify procedures.

## **B-23. Emergency actions of general nature**

Actions not covered by this plan required for serious emergencies such as fire, bomb threats, and serious injury.

## **B-24. Coordination**

Provide contact names and telephone numbers of agencies with whom the plan was coordinated.

- a.* Integration of the plan with installation supporting agencies.
- b.* Liaison and coordination with nearby military units, police, and intelligence agencies, and with civil agencies including civil police and FBI, as appropriate.

## **B-25. Appendixes**

- a.* Guard orders.
- b.* Communications plan.
- c.* Recapture/recovery plan.
- d.* Rules of engagement and use of deadly force (include rules for air or helicopter assault).
- e.* Threat analysis.
- f.* Site vulnerability assessment documentation.
- g.* Contingency defense plan.
- h.* Disaster control plan.

# FOR OFFICIAL USE ONLY

- i.* Demonstration control plan.
- j.* Civil disturbance plan.

## Appendix C Internal Control Evaluation Checklist

### C-1. Function

This checklist covers basic administration of the Army Physical Security Program.

### C-2. Purpose

This checklist helps commanders evaluate key management controls outlined below. It is not intended to cover all processes and procedures.

### C-3. Instructions

Answers must be based on the actual testing of key management controls such as by document analysis, direct observation, sampling, and simulation. Answers indicating deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

### C-4. Test questions

- a.* Does the ACOM, ASCC, DRU, ARNG by formal process—
  - (1) Maintain a physical security program to plan and coordinate physical security matters and to ensure practical, effective, and common sense measures are used? What documents support the program, such as a command plan?
  - (2) Appoint a command PSO on orders?
  - (3) Review, approve and maintain copies of subordinate organizations PS plans?
  - (4) Identify and forward resource requirements to DAPM-MPP-PS?
  - (5) Execute funds per OPMG resource guidance?
  - (6) Coordinate new PSE performance requirements with TRADOC?
  - (7) Use the SMS for inspections, surveys, cost analysis, trend analysis, and loss expectancy analysis?
  - (8) Ensure physical security, antiterrorism, and engineering personnel coordinate design criteria for new construction projects?
  - (9) Ensure physical security personnel track construction projects at every milestone of the planning, design, and construction process, and document the tracking process?
  - (10) Ensure forces deploying to overseas areas designate personnel to carry out physical security responsibilities to safeguard personnel, facilities, equipment, operations, and materiel against hostile intelligence, terrorists, and criminal, dissident, or other disruptive activity?
  - (11) Ensure deployed PSIs are provided with inspector credentials for the duration of their deployment tour, and to ensure issued credentials are recovered and accounted for after deployment?
  - (12) Record, track, and resolve deficiencies found during inspections and surveys?
  - (13) Manage maintenance contracts for PSE on a regional basis to the greatest extent feasible?
  - (14) Ensure the contract structure that supports PSE sustainment promotes competition?
  - (15) Issue, control, account for, and properly destroy inspector credentials?
  - (16) Ensure inspections and surveys are conducted per this regulation and against the minimum standards of asset-specific regulations?
  - (17) Appoint a voting member or nonvoting advisor, as applicable, to the DAPSRB and APSEAG?
- b.* Do commanders of posts, camps, stations, and installations, including Army-managed Armed Forces Reserve Centers, Army Reserve Centers, Army National Guard Armories, and other Army facilities subject to DA jurisdiction or administration, or in DA custody, by formal process—
  - (1) Appoint a command PSO on orders?
  - (2) Use SMS?
  - (3) Conduct inspections and surveys per this regulation and against the minimum standards of asset-specific regulations?
  - (4) Designate restricted areas in writing?
  - (5) Post warning signs at restricted areas?
  - (6) Designate MEVAs in writing?
  - (7) Ensure engineers and physical security personnel coordinate in the formulation of design criteria for new



# FOR OFFICIAL USE ONLY

construction projects, and that physical security personnel review all plans and specifications at every step of the planning, design, and construction process?

- (8) Issue written appointment orders establishing a PSC chaired by the senior installation law enforcement officer?
- (9) Pass threat information to all military activities on/off the installation?
- (10) Have an installation or activity physical security plan?
- (11) Include physical security as an annex to all applicable orders and plans?
- (12) Ensure supporting military intelligence elements are given all the information relating to the organization and its activities needed to support the force protection mission?
- (13) When requested by tenant activities, provide physical security support per AR 37-49?

## **C-5. Supersession**

This is an initial evaluation for The Army Physical Security Program.

## **C-6. Comments**

Help make this a better tool for evaluating management controls. Submit comments to Headquarters, Department of the Army, (DAPM-MPP-PS), Office of the Provost Marshal General, 2800 Army Pentagon, Washington, DC 20310-2800.

# FOR OFFICIAL USE ONLY

## Glossary

### Section I

#### Abbreviations

**AA&E**

arms, ammunition, and explosives

**AAFES**

Army and Air Force Exchange Service

**ACOM**

Army command

**ACSIM**

Assistant Chief of Staff for Installation Management

**AIE**

Automated Installation Entry

**APSEAG**

Army Physical Security Equipment Action Group

**AR**

Army regulation

**ARNG**

Army National Guard

**ARSTAF**

Army staff

**ASA (ALT)**

Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

**ASA (CW)**

Assistant Secretary of the Army for Civil Works

**ASA (IE&E)**

Assistant Secretary of the Army (Installations, Energy and Environment)

**ASA (M&RA)**

Assistant Secretary of the Army (Manpower and Reserve Affairs)

**ASCC**

Army service component command

**ASI**

additional skill identifier

**ASI H3**

additional skill identifier, physical security inspector

**CAC**

common access card

**CE**

civilian equivalent

**CIO/G-6**

Chief Information Officer/G-6

# FOR OFFICIAL USE ONLY

**CG**

commanding general

**COE**

Chief of Engineers

**CONUS**

continental United States

**DA**

Department of the Army

**DAPSRB**

Department of the Army Physical Security Review Board

**DBIDS**

Defense Biometric Identification System

**DCS, G-1**

Deputy Chief of Staff, G-1

**DCS, G-2**

Deputy Chief of Staff, G-2

**DCS, G-3/5/7**

Deputy Chief of Staff, G-3/5/7

**DCS, G-4**

Deputy Chief of Staff, G-4

**DeCA**

Defense Commissary Agency

**DES**

Director of Emergency Services

**DIACAP**

Department of Defense Information Assurance Certification and Accreditation Process

**DOD**

Department of Defense

**DODD**

Department of Defense directive

**DODI**

Department of Defense instruction

**DRU**

direct reporting unit

**ESC**

Electronic Security Center

**FBI**

Federal Bureau of Investigation

**FIPS**

Federal Information Processing Standards

# FOR OFFICIAL USE ONLY

**FPCON**

force protection condition

**GIG**

global information grid

**GSA**

General Services Administration

**HQDA**

Headquarters, Department of the Army

**HRC**

Human Resources Command

**IACP**

installation access control point

**ICIDS**

Integrated Commercial Intrusion Detection System

**IDS**

Intrusion Detection System

**IDSWG**

Intrusion Detection Systems Working Group

**III**

Interstate Identification Index

**JRWG**

Joint Requirements Working Group

**MDEP**

management decision evaluation package

**MEVA**

mission essential and vulnerable area

**MWD**

military working dog

**NCIC**

National Crime Information Center

**NDA**

National Defense Area

**O-4**

major

**O-5**

lieutenant colonel

**OCONUS**

outside the continental United States

**OPMG**

Office of the Provost Marshal General

# FOR OFFICIAL USE ONLY

**PDC**

Protective Design Center

**PIN**

personal identification number

**PM**

provost marshal

**PMG**

Provost Marshal General

**PSC**

physical security council

**PSE**

physical security equipment

**PSEAG**

Physical Security Equipment Action Group

**PSEWG**

Physical Security Equipment Working Group

**PSI**

physical security inspector

**PSO**

physical security officer

**RAM**

random antiterrorism measures

**RDT&E**

research, development, test, and evaluation

**SMS**

Security Management System

**SOFA**

status of forces agreement

**TRADOC**

U.S. Army Training and Doctrine Command

**TTP**

Trusted Traveler Program

**UFC**

Unified Facilities Criteria

**UFGS**

unified facilities guide specification

**USACE**

U.S. Army Corps of Engineers

**USACIDC**

U.S. Army Criminal Investigation Command

# FOR OFFICIAL USE ONLY

## **USAR**

U.S. Army Reserve

## **USC**

United States Code

## **USDB**

U.S. Disciplinary Barracks

## **Section II**

### **Terms**

#### **Access (relating to a restricted area)**

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 a controlled cryptographic item through uncontrolled physical possession. External viewing or escorted proximity to a controlled cryptographic item does not constitute access.

#### **Access control**

Permitting or denying the use of a particular resource by a particular entity.

#### **Access control point**

Points at the outermost boundary of the installation (or cantonment area of large installations) where security checks can be performed on personnel, vehicles, and materials before potential threats can gain close proximity to Army assets.

#### **Army Access Control Points Standard Definitive Design**

Provides standards to meet access control functions on active Army installations and Reserve Component prime installations (<https://www.us.army.mil/suite/page/441649>).

#### **Army standard for access control points**

Provides standards for Army access control points (ACPs) (<https://www.us.army.mil/suite/doc/8912967>).

#### **Army Standard (Part I) and System Specifications (Part II) for Automated Installation Entry**

Provides standards for Army AIE (<https://www.us.army.mil/suite/doc/9647105>).

#### **Automated installation entry**

A system of software and hardware designed to read and compare vehicle and personnel identification media. The results of the media comparison are used to permit or deny access according to set criteria. The AIE is intended to expedite entry of authorized personnel.

#### **Charette**

A collaborative session in which a group of designers drafts a solution to a design problem.

#### **Common access card (CAC)**

An identification card displaying the cardholder's name, photo, and organization. The CAC is the DOD implementation of Homeland Security Presidential Directive 12 that requires Federal Executive Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal facilities and information systems and designates the major milestones for implementation.

#### **Contractor**

One who enters into a binding agreement to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, goods or services, during a specific time. Contractors may require logical access to Army computers in addition to physical access to a site. Sub-contractors are included in this category.

#### **Contractor Verification System**

A web-based system established by the Defense Manpower Data Center to automate the application, validation, and approval process for issuance of a CAC to eligible DOD contractors.

#### **Controlled area**

A type of restricted area in which access to the general public is denied unless certain entry controls are met. This type

# FOR OFFICIAL USE ONLY

of area has the least restrictive conditions. Usually the required controls for entry include a military identification card or proof of identification by another Federal or state government document, and a need for access. Once authorized to enter, movement within the area is not controlled. An example of a controlled area is an Army installation or facility where entry is granted at the IACP. A controlled area may also be a building that is not accessible by the general public because entry is controlled by proof of identification that the individual is an active or retired member of the military (for example, commissary, post exchange).

## **Crime prevention**

The anticipation, recognition, and appraisal of a crime risk, and initiation of some action to remove or reduce the risk. 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.

## **Entry control**

In terms of this policy, entry control are security actions, procedures, equipment, and techniques, employed in restricted areas to ensure persons who are present in the areas at any time have authority and official reason for being present.

## **Exception**

An approved permanent continuation of a deviation from this regulation in which the requirements are not being met and the approving authority determines it is inappropriate to meet the requirements. Compensatory security measures are required to provide adequate security for the deviation.

## **Exclusion area**

A type of restricted area that contains a security interest or other material of such vital importance that proximity resulting from entry into the area constitutes access to such security interest or material. Therefore entry into an exclusion area is more restrictive than into a limited area. An exclusion area is usually located within a limited area. In addition to conditions required for entry into the limited area, further entry into an exclusion area is disqualified from everyone unless they are identified through an entry control roster, electronic access control system, or exchange badge system for the exclusion area and can meet two conditions: (1) The person must be a current member of the Personnel Reliability Program, and (2) the person is a participant in a two-person access requirement within the area. Movement within an exclusion area is controlled by the two-person rule. All other individuals allowed entry into an exclusion area must be escorted by person who can satisfy the previous two conditions. Persons under escort cannot satisfy the two-person requirement and are not considered to have access to the security interest.

## **Global information grid (GIG)**

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. The GIG supports the DOD, the National Security Agency, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

## **Independent power source**

A power source (usually a battery) that is independent of any other source.

## **Installations**

A grouping of facilities located in the same vicinity that support particular functions.

## **Installation access control point**

A point along an installation boundary that represents an initial security screening point for vehicles and personnel entering the installation.

## **Interstate Identification Index (III)**

The III is an index-pointer system for the interstate exchange of criminal history record information. The FBI maintains an index of persons arrested for felonies or serious misdemeanors under state or Federal law.

## **Intrusion Detection System (IDS)**

Electronic components including sensors, control units, transmission lines, and monitoring units that are integrated to

# FOR OFFICIAL USE ONLY

be capable of detecting one or more types of intrusion into the area protected by the system and reporting to a central monitoring station.

## **Limited area**

A type of restricted area that is more restrictive than a controlled area because in addition to the need for access and proof of positive identification, entry is limited to only those individuals whose names have been previously placed on an entry control roster signed by the controlling authority (installation/activity commander) or who have been enrolled in an electronic access control system, or are part of an approved exchange badge system. Entry is granted to those limited individuals listed on the entry control roster, enrolled in the electronic access control system, or members of an exchange badge system after verification at the entry control facility. Movement within a limited area is not controlled for those authorized unescorted entry. A limited area is normally a buffer zone for an exclusion zone because access to the security interest contained within the exclusion area remains prohibited. Commanders may require escorts for uncleared personnel with a need for entry into the limited area.

## **Locks**

A mechanical or electro-mechanical fastening device intended to control access. Locks are devices designed to delay intruders, rather than means to fully stop unauthorized entry since any lock can eventually be defeated by expert manipulation or by force. Refer questions 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) (<https://portal.navfac.navy.mil/go/locks>).

## **Management Decision Package (MDEP)**

A funding source that describes a particular organization, program, or function, and records the resources associated with the intended output. An individual MDEP applies uniquely to management areas for the active Army, Guard, and Reserve. During programming for resource requirements, MDEPs provide useful visibility to assist Army managers, decision makers, and leaders to assess program worth, confirm compliance, and rank resource claimants. During budgeting, MDEPs help convey approved programs and priorities into budget estimates and assist in recording program changes caused by budget decisions and approved funding. During execution, MDEPs help track program and financial performance, and help determine future requirements.

## **Mission essential or vulnerable areas**

An area or a structure determined to be essential to the mission, or as being unusually vulnerable to the prevailing threat, or both, and that it deserves priority status for protection resources. The MEVAs can be areas that house information, equipment, property or personnel. They are recommended for MEVA status by the PM/DES/SO and approved by the commander. The terms mission essential and vulnerable are not synonymous. An area or structure may be essential to the mission, but not particularly vulnerable to a known threat due to a well layered security-in-depth posture. In contrast, an area or structure may be vulnerable to a threat, but not contain mission essential resources or functions. This critical distinction can help commanders prioritize the application of security resources.

## **National Crime Information Center (NCIC)**

A computerized index of criminal justice information such as criminal record history information, fugitives, stolen properties, and missing persons. The NCIC is operated by the FBI. It is a continuous operation available to Federal, state, and local law enforcement and other criminal justice agencies. An NCIC III check searches these databases: Wanted Person File, Foreign Fugitive File, Violent Gang and Terrorist Organization File, U.S. Secret Service File, Convicted Persons on Supervised Release File, Threat Against Peace Officer Alert File, Protection Order File, Missing Person File, State Criminal Investigation Division Only Wanted Person File, Concealed Handgun License File, Drivers License Record File, Convicted Sexual Offender Registry File, Deported Felon File, and the Unidentified Persons File.

## **National Incident Management System**

A system that provides a consistent nationwide template to enable all government, private sector, and nongovernmental organizations to work together during domestic incidents.

## **Personal identity verification**

A process to verifying a person's identity.

## **Physical security**

Using risk analysis as a decision basis, physical security is a combination of physical protective measures and security procedural measures employed to safeguard personnel, property, operations, equipment, facilities, materiel, and information against loss, misuse, theft, damage or destruction by disaffected persons (insiders), vandals, activists, extremist



# FOR OFFICIAL USE ONLY

protesters, criminals (individuals and organized groups), terrorists (domestic, state-sponsored, and transnational), saboteurs and spies.

## **Physical security equipment**

A broad term used to describe items, devices, and systems used primarily to protect resources to include nuclear, chemical, biological, 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.

## **Physical security inspection**

A formal, recorded assessment of physical protective measures and security procedures measures implemented by a unit or activity to protect its assets.

## **Physical protective measures**

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. In contrast with security procedural measures that often involve personnel, these measures are usually permanent and involve expenditure of funds. Examples of physical protective measures are barriers, IDSs, and locks and keys.

## **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 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**

A plan developed by the PSO, and approved by the responsible commander that identifies physical security needs and shows proposed, prioritized procurement of those needs.

## **Physical security survey**

A formal, recorded assessment of the installation physical security program.

## **Restricted area**

An area defined by an established boundary to prevent admission unless certain conditions or controls are met to safeguard the personnel, property or material within. These areas are not to be confused with those designated Federal Aviation Administration areas over which aircraft flight is restricted. All restricted areas will be marked and have the ability to control access to the area. Restricted areas are identified by the different types of conditions required to permit entry. Conditions for entry vary depending on the nature and degree of importance of the security interest or government assets contained within a restricted area. The three types of restricted areas are controlled, limited, and exclusion.

## **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.

# FOR OFFICIAL USE ONLY

## **Security badge**

A security credential, worn on the outer garment, used to validate a person's authority to be in a restricted area.

## **Security identification card**

An official, distinctive identification (pass or card) that identifies and authorizes a person to be present in a restricted area.

## **Security engineering**

The application of engineering principles to the protection of assets against various threats through the application of construction and equipment.

## **Security procedural measures**

Practices followed to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. In contrast with physical protective measures that usually involves equipment, these measures can usually be changed within a short amount of time and usually involve manpower. Examples of security procedural measures are key and lock inventory controls, use of badge systems, and guard patrols.

## **Tenant activity**

A unit or activity of a agency, military department, or commercial entity that occupies facilities on an installation and that receives supplies or other support services from that installation.

## **Teslin card**

A type of identification card made of synthetic, waterproof material used in some DOD identification and privilege cards and also widely used for vehicle operator licenses, voter identification cards, and other forms of identification card. As examples, DD Form 2S (RET) and DD Form 1173 are teslin cards.

## **Trusted traveler**

A person enrolled in the TTP.

## **Trusted Traveler Program (TTP)**

A process by which a uniformed Servicemember or government employee with a valid CAC, driver's license, and clear NCIC check, presents their identification token for automated authentication at an IACP, and simultaneously vouches for other vehicle occupants.

## **Unified Facilities Criteria (UFC) 4-010-01**

Provides minimum construction standards for all DOD buildings to mitigate mass casualties from the terrorist threat.

## **Unified Facilities Criteria (UFC) 4-010-02**

Provides minimum standoff distances for all DOD buildings to mitigate mass casualties from the terrorist threat.

## **Unified Facilities Criteria (UFC) 4-020-01**

Supports the planning of DOD facilities that include requirements for security and antiterrorism.

## **Unified Facilities Criteria (UFC) 4-022-01**

Provides construction standards for these for entry control facilities/access control points.

## **Vendor**

A supplier of goods or services who might not require logical access to Army computers but does require physical access to a site.

## **Waiver**

Temporary relief from specific regulatory standards issued while pending completion of actions that will bring the matter into regulatory conformance. Compensatory measures are required.

## **Section III**

### **Special Abbreviations and Terms**

This section contains no entries.

**FOR OFFICIAL USE ONLY**

**PIN 002202-000**