

**USAREUR Regulation 190-13**

**Military Police**

# **The USAREUR Physical Security Program**

**Headquarters  
United States Army, Europe,  
and Seventh Army  
Unit 29351  
APO AE 09014  
25 August 1995**

# SUMMARY of *CHANGES*

USAREUR Regulation 190-13  
The USAREUR Physical Security Program

1 May 2003

This revision changes table C-2, section IV.

25 August 1995

This revision—

- Establishes and implements the USAREUR Physical Security Program.
- Identifies the key components of the USAREUR program (chap 2).
- Eliminates "activity priorities."
- Consolidates existing USAREUR physical-security guidance into a single document, thereby eliminating USAREUR Regulations 190-3, 190-11, 190-17, 190-51, and 190-56.

Military Police

The USAREUR Physical Security Program

For the Commander in Chief:

DAVID L. BENTON, III  
Major General, USA  
Chief of Staff

Official:



DALE E. PEYTON  
Colonel, GS  
Deputy Chief of Staff,  
Information Management

**Summary.** This regulation establishes the USAREUR Physical Security Program and provides supplemental guidance to DA physical-security publications. The USAREUR Physical Security Program is a component of the USAREUR Force Protection Program. This regulation will be used with ARs 190-11, 190-13, 190-16, 190-50, 190-51, 190-56, and DA Pamphlet 190-51.

**Applicability.** This regulation applies to every USAREUR assigned and attached unit (incl U.S. Army tenant units in USEUCOM that are subject to local requirements).

**Supplementation.** Commanders will not supplement this regulation without Commander in Chief, USAREUR, approval.

**Forms.** Appendix D lists forms prescribed by this regulation. Only -R forms may be reproduced locally on 8½- by 11-inch paper through the servicing forms management office. Other forms will not be reproduced; they will be ordered by the unit or organization publications officer from the United States Army Printing and Publications Center, Europe, or as stated in the prescribing directive.

**Interim Changes.** Interim changes to this regulation are not official unless authenticated by the Deputy Chief of Staff, Information Management, USAREUR. Interim changes will be destroyed on their expiration dates unless sooner superseded or rescinded.

**Suggested Improvements.** The proponent of this regulation is the Office of the Provost Marshal, HQ USAREUR/7A (AEAPM-O-PS, 380-7379). Users may send suggestions to improve this regulation on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086.

**Distribution.** Distribute according to DA Form 12-88-E, block 0235, command level A.

CONTENTS

Chapter	Paragraph	Page	Chapter	Paragraph	Page
1. GENERAL			2. USAREUR PHYSICAL SECURITY PROGRAM		
	Purpose	1-1	Section I		
	References	1-2	PROGRAM PRINCIPLES		
	Abbreviations and Terms	1-3	Purpose	2-1	2-1
	Responsibilities	1-4	Objectives	2-2	2-1
	Format	1-5	Program Requirements	2-3	2-1

**USAREUR Reg 190-13**

<b>Chapter</b>	<b>Paragraph</b>	<b>Page</b>	<b>Chapter</b>	<b>Paragraph</b>	<b>Page</b>
<b>Section II</b>			Inventory and Accountability	5-4	5-1
<b>PROGRAM COMPONENTS</b>			IDS	5-5	5-1
Commander Responsibilities	2-4	2-1	K&LC	5-6	5-1
Assessing the Threat	2-5	2-1	Reporting Missing and Recovered AA&E	5-7	5-2
Duty Assignments	2-6	2-1	Transporting AA&E	5-8	5-2
Planning	2-7	2-2	AE Form 190-13I	5-9	5-2
Risk Analysis	2-8	2-2			
MEVA	2-9	2-2			
Restricted Areas	2-10	2-2	<b>6. ELECTRONIC SECURITY SYSTEMS</b>		
Coordination	2-11	2-2	Purpose	6-1	6-1
Physical-Security Councils	2-12	2-3	Physical-Security Equipment Overview	6-2	6-1
Security Measures	2-13	2-3	Planning Guidelines	6-3	6-1
Inspections and Surveys	2-14	2-3	Priorities	6-4	6-2
			Risk Analysis	6-5	6-2
<b>3. UNIT- AND INSTALLATION-LEVEL SECURITY OF ARMY PROPERTY</b>			Forecasting	6-6	6-2
Purpose	3-1	3-1	Identification and Verification of Requirements	6-7	6-3
Security Standards	3-2	3-1	Coordination	6-8	6-3
Security Guidance	3-3	3-1	Request Packet (J-SIIDS)	6-9	6-3
Essential Warfighting Facilities	3-4	3-1	Request Packet (Commercial ESS)	6-10	6-4
Transition and Sustainment Facilities	3-5	3-1	Technical Review for Commercial ESS	6-11	6-4
Other Facilities	3-6	3-1	IDS Acquisition Procedures	6-12	6-4
			Physical-Security Plans	6-13	6-5
<b>4. INSTALLATION ACCESS</b>			IDS Categories	6-14	6-5
Purpose	4-1	4-1	Recommended Sensors	6-15	6-5
Applicability	4-2	4-1	Description of System Components	6-16	6-5
Entry Authorization	4-3	4-1	Location of IDS Components	6-17	6-5
USAREUR Passes and Badges	4-4	4-2	System Wiring Diagram	6-18	6-6
Issuing Authorities	4-5	4-2	Transmission Lines and Backup Power	6-19	6-6
AE Forms 190-13A and 190-13B	4-6	4-3	Installation	6-20	6-6
AE Form 190-13C	4-7	4-4	Personnel Checks	6-21	6-7
Alternate Installation Access Procedures	4-8	4-5	IDS Operating Procedures	6-22	6-7
AE Forms 190-13E, 190-13F, and 190-13G	4-9	4-6	Recordkeeping	6-23	6-8
Confiscating ID Cards, Passes, and Badges	4-10	4-7	Maintenance	6-24	6-8
Reporting Persons Barred From Installations	4-11	4-7	Logistics Procedures	6-25	6-8
Specified-Country Citizens	4-12	4-7	Response to Alarms	6-26	6-8
Installation Access by German Police	4-13	4-7	Inspections	6-27	6-9
DA Form 1818	4-14	4-8	Operational Checks	6-28	6-9
Recording Entry Into Controlled Areas	4-15	4-9	Access Roster	6-29	6-10
			Key Control	6-30	6-10
<b>5. PHYSICAL SECURITY OF AA&amp;E</b>			Signs	6-31	6-10
Purpose	5-1	5-1	Movement of IDS	6-32	6-10
Structure Standards	5-2	5-1			
Waivers and Exceptions	5-3	5-1	<b>7. USAREUR SECURITY GUARD PROGRAM</b>		
			Purpose	7-1	7-1
			Applicability	7-2	7-1
			Objectives	7-3	7-1

Chapter	Paragraph	Page	Chapter	Paragraph	Page
Guard Authority	7-4	7-1	<b>Appendixes</b>		
Types of Guards	7-5	7-1	A. References		A-1
Policy	7-6	7-1	B. Responsibilities		B-1
Guard Force Standards	7-7	7-1	C. Minimum Security Standards		C-1
Individual Reliability			D. Forms		D-1
Program	7-8	7-2	E. Waivers and Exceptions		E-1
Drug Screening	7-9	7-2	F. Inspection Checklist		F-1
Training	7-10	7-2	G. Inspector Credentials		G-1
Uniform and Equipment	7-11	7-3			
Establishing and Filling					
Requirements	7-12	7-4	<b>Glossary</b>		<b>Glossary 1</b>
Guard Orders	7-13	7-4			
Evaluations	7-14	7-5	<b>Index</b>		<b>Index 1</b>

**CHAPTER 1  
GENERAL**

**1-1. PURPOSE**

a. This regulation implements the requirement in AR 190-13 for major Army command commanders to establish a Physical Security Program.

b. This regulation provides policy and procedures for the USAREUR Physical Security Program.

c. The guidance in this regulation will help commanders formulate, plan, and coordinate physical-security matters. The goal of this regulation is to establish practical and effective measures that will be used and tested as part of the overall physical-security program.

d. This regulation will be used to integrate physical-security efforts into force-protection plans and procedures.

**1-2. REFERENCES**

Appendix A lists required references, related publications, and forms.

**1-3. ABBREVIATIONS AND TERMS**

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

**1-4. RESPONSIBILITIES**

The security of the force is an operational concern with overall security responsibility remaining within operational channels. Responsibilities are consolidated and listed in appendix B. Responsibilities in appendix B include not only those developed to support this regulation, but also those responsibilities listed in the various Army regulations (ARs) that deal with physical security.

**1-5. FORMAT**

a. This regulation is published in loose-leaf format to facilitate the creation of a physical-security guide in a 3-ring binder. Because of the loose-leaf format, specific portions of this regulation can be changed when necessary without the need to republish the whole document.

b. Where possible, individual chapters have been designed to relate to specific ARs. In those chapters are required clarifications and supplementation needed for that specific AR.

c. It is recommended that the applicable AR be maintained in the 3-ring binder at the end of the pertinent chapter in this regulation.

**CHAPTER 2**  
**USAREUR PHYSICAL SECURITY PROGRAM**

**SECTION I**  
**PROGRAM PRINCIPLES**

**2-1. PURPOSE**

This chapter establishes and defines the principles of the USAREUR Physical Security Program.

**2-2. OBJECTIVES**

The USAREUR Physical Security Program—

a. Is an integral part of the USAREUR Force Protection Program.

b. Incorporates guidance from various DA publications dealing with physical security.

c. Provides commanders with guidelines and standards for planning efficient and cost-effective local physical-security programs to protect USAREUR assets from damage or loss.

d. Provides physical-security measures to counter—

- (1) Criminals.
- (2) Disaffected persons.
- (3) Hostile intelligence.
- (4) Paramilitary forces.
- (5) Protesters.
- (6) Saboteurs.
- (7) Terrorists.

**2-3. PROGRAM REQUIREMENTS**

The USAREUR Physical Security Program—

a. Will follow the guidance in AR 190-13, chapter 2.

b. Will operate from HQ USAREUR/7A through area support groups (ASGs) and base support battalions (BSBs) to the unit level. Each level has specific responsibilities that allow the program to direct functions at the appropriate level.

c. Is an integrated process made up of the following components, which are discussed in section II:

- (1) Assessing the threat.
- (2) Assigning specific physical-security duties.
- (3) Conducting security planning.
- (4) Conducting risk analysis.
- (5) Identifying mission-essential or vulnerable areas (MEVAs).
- (6) Designating restricted areas.
- (7) Coordinating security efforts.
- (8) Establishing physical-security councils.
- (9) Employing physical- and procedural-security measures.
- (10) Conducting inspections and surveys.

**SECTION II**  
**PROGRAM COMPONENTS**

**2-4. COMMANDER RESPONSIBILITIES**

Physical security is a commander's program. An effective physical-security program uses an approach that is methodical, deliberate, and ongoing at each command level. Commanders at all levels will establish programs that include the components prescribed by this regulation. Commanders will periodically review and be prepared to adjust their programs to the changing threat.

**2-5. ASSESSING THE THREAT**

Threat statements must be developed, updated as necessary, and included as annexes to physical-security plans (AR 190-13).

**2-6. DUTY ASSIGNMENTS**

a. Physical-security officers will be designated according to AR 190-13, chapters 1 and 3. ASG and BSB commanders will designate individuals to serve on a joint action working group (JAWG), which fulfills the requirement to establish physical-security councils (AR 190-13) and the AR 525-13 requirement for a force-protection committee.

b. ASGs must also have a fusion cell (AR 525-13, para 3-3).

c. Key-and-lock control (K&LC) will be a designated duty in every organization (para 5-6). K&LC custodians will be appointed in writing to control keys to arms, ammunition, and explosives (AA&E).

## USAREUR Reg 190-13

### 2-7. PLANNING

a. The physical-security plan will tie security measures together. The plan will be written using the guidance in AR 190-13 and Field Manual (FM) 19-30. It will integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other.

b. The physical-security plan must have reasonable and affordable protective measures. Reliance on security guards should be a measure of last resort, with alternatives considered when possible. Associated costs should be in proportion to the value or criticality of the property being protected and the existing level of risk.

c. Because security requirements will change with each threat condition (THREATCON), it is important these changes be identified in the plan. A separate annex of the plan will identify where and what security changes must occur for each THREATCON level. The annex should include a list of resources that are required and the source of those resources.

### 2-8. RISK ANALYSIS

a. Risk analyses are critical to security planning. With the exception of AA&E storage, risk analyses are explained in DA Pamphlet 190-51 and in the Security Management System (SMS). Risk analyses are used to adapt physical protective measures and security procedures to local conditions.

b. Risk analyses must be performed on MEVAs. Risk analyses will be considered when scheduling follow-on inspections and surveys. Analyses will be kept on file until the next risk analysis is conducted.

### 2-9. MEVA

a. The MEVA list helps commanders concentrate protection on the most important assets and prioritize the physical-security effort. The MEVA list will include only areas and activities that have been determined to be mission-essential or highly vulnerable based on a total assessment of the specific mission, environment, and threat.

b. To develop a MEVA list, commanders will begin by identifying assets that are critical to national security, mission essential, or subject to attack, based on inclination shown by current threat groups.

c. Based on their analyses, commanders at each level will develop a MEVA list and submit it through their next higher

command to the BSB commander for consideration as a MEVA. BSB commanders will send approved MEVA lists to the local provost marshal (PM) by 30 September each year for scheduling of risk analyses and physical-security inspections.

d. JAWGs will consider and approve MEVA lists (para 2-12). AR 190-13 has a more detailed discussion of MEVA.

### 2-10. RESTRICTED AREAS

a. One way commanders can safeguard Army assets is by declaring an area restricted and, thereby, limiting access to that area. Restricted areas will be posted according to AR 190-13.

b. Authority for USAREUR to declare and enforce restricted areas is based on the NATO Status of Forces Agreement (SOFA). The NATO SOFA may be supplemented by individual host countries. Countries subject to the NATO SOFA are responsible for seeking legislation to ensure there is adequate security for U.S. installations and property.

c. Commanders will contact the local judge advocate general (JAG) when questions arise about jurisdiction over restricted areas. Violations of restricted areas will be brought to the attention of the local PM and intelligence officials. Violations include entering a restricted area, receiving or trying to gather sensitive or classified information, and other offenses.

d. Violations that may involve espionage or sabotage will be reported according to AR 381-12. In Germany, the servicing PM will be immediately provided with details of restricted area violations. The PM will inform German police authorities and local intelligence officials.

### 2-11. COORDINATION

a. Commanders will coordinate appropriate physical-security plans with adjacent ASGs, BSBs, and units. Coordination and liaison will also be established with host nation (HN) authorities.

b. Construction projects require continuous security coordination between engineers and security personnel from planning through completion of the project. The link between physical-security requirements for military construction projects and funding for physical-security systems is vital.

c. Commanders must ensure physical-security requirements are identified during construction planning, and funding for security systems is established at the beginning.

**2-12. PHYSICAL-SECURITY COUNCILS**

a. ASGs and BSBs will establish a force-protection JAWG. The JAWG meets the requirements in AR 190-13 and AR 190-16 for physical-security councils and the requirement in AR 525-13 for force-protection councils.

b. The force-protection JAWG will meet at least once every 3 months to ensure attention is being given to physical security and force protection. The force-protection JAWG agenda will address all issues directly related to physical security. The ASG or BSB commander will schedule additional meetings when appropriate.

c. The JAWG will direct routine actions into normal staff channels and expedite action on critical or time-sensitive issues requiring a coordinated response.

d. As a minimum, the JAWG should be made up of the following:

- (1) ASG, BSB, or separate community commander.
- (2) Directorate of plans, training, mobilization, and security (DPTMS) personnel.
- (3) Directorate of engineering and housing (DEH) officer.
- (4) Resource management (RM) officer.
- (5) PM.
- (6) Representatives of subordinate commands, major installations, and tenant commands.

e. Issues appropriate for JAWG meetings include, in addition to those listed in AR 190-16 and AR 525-13—

- (1) Considering and prioritizing projects for Command Security Upgrade Program (CSUP) funding, and reviewing the status of existing projects.
- (2) Coordinating force-protection measures for units with United States Army Intelligence Command Continental (United States) Operations (CONOPS) missions.
- (3) Ensuring maintenance plans for clear zones are included in the ASG or BSB land-management plan, and reviewing the status of clear zones.
- (4) Monitoring the effectiveness of crime-prevention programs.
- (5) Prioritizing—
  - (a) The MEVA list.

(b) Funding requirements for waivers and exceptions.

(c) Funding for correction of deficiencies noted during physical-security inspections and surveys.

(6) Reviewing and approving the MEVA list.

(7) Reviewing—

(a) Intrusion detection system (IDS) failures (incl causes), downtime, and repair problems.

(b) ASG and BSB modernization plans, status of proposed construction, and integration of security requirements.

(c) Crime trends and conditions conducive to crime.

(d) Threat assessments and the THREATCON status.

(e) Force-protection plans, orders, exercises, and resource issues.

**2-13. SECURITY MEASURES**

There are two broad categories of security measures: physical and procedural. Measures should deter, detect, delay, or defeat the threat. Deterrence can be improved by using highly visible measures and randomness. This is cost-efficient and complicates the threatening person, group, or force ability to plan. Security measures should be integrated and layered by using a combination of fences, lights, electronic security systems (ESSs), guards, and reaction forces.

**2-14. INSPECTIONS AND SURVEYS**

a. USAREUR inspections and surveys will conform to the requirements of AR 190-13, chapter 2, for physical-security surveys, physical-security inspections, and security engineering surveys. References in AR 190-13 to "installation-level" responsibilities apply to ASGs and separate commands in USAREUR. ASGs may delegate responsibilities to the BSBs for execution.

b. Inspections are primarily of MEVAs; the frequency is every 24 months for non-AA&E facilities and every 18 months for AA&E facilities. The ASG or BSB commander may, however, direct inspections of other facilities.

c. Physical-security offices will send a copy of completed DA Forms 2806-1-R (Physical Security Inspection Report) that resulted in a "not adequate" rating and every DA Form 2806-R (Physical Security Survey Report) to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086. Commanders will also send reports of corrective action taken in response to physical-security surveys to the above address.

**CHAPTER 3  
UNIT- AND INSTALLATION-LEVEL SECURITY OF  
ARMY PROPERTY**

**3-1. PURPOSE**

a. This chapter—

(1) Provides policy and procedures for safeguarding Army equipment at the USAREUR unit and installation levels.

(2) Will be used with AR 190-51 and DA Pamphlet 190-51.

b. The objectives of this chapter are to—

(1) Provide guidance to reduce loss, theft, and damage of USAREUR resources in an efficient and cost-effective manner.

(2) Clearly establish the minimum security standards that must be met to safeguard USAREUR assets.

**3-2. SECURITY STANDARDS**

a. Security standards are the collective measures that must be taken to safeguard assets. Measures include both procedural and physical means. Access controls, duty appointments, and security checks are examples of procedures. Fences, locks, lights, alarm systems, and cameras are examples of physical means.

b. Appendix C prescribes the minimum security standards for protecting selected USAREUR assets. More information is available in ARs and security-classification guides for specific equipment.

**3-3. SECURITY GUIDANCE**

a. Not all assets can or should be given the same level of security. Efficient and cost-effective security is achieved by using resources based on risk analyses (DA Pam 190-51 and SMS explain how to conduct a risk analysis). Security resources (manpower and money) are limited and must be used in response to the criticality of the asset and the risk to or vulnerability of the protected asset.

b. When employing security measures, use a mix of measures, layer the protection, and employ measures at random, to the extent possible.

**3-4. ESSENTIAL WARFIGHTING FACILITIES**

a. The following are examples of facilities considered essential to the USAREUR warfighting mission:

(1) AA&E bulk storage sites.

(2) Active air defense artillery (ADA) sites.

(3) Critical facilities on airfields from which combat aviation assets routinely operate.

(4) Major headquarters (corps and above) and other special units designated by the Deputy Chief of Staff, Operations (DCSOPS), USAREUR.

b. Appendix C prescribes minimum security standards for the facilities in a above. These assets will be secured, as a minimum, at risk level III standards.

**3-5. TRANSITION AND SUSTAINMENT FACILITIES**

a. The following are examples of facilities that are critical to the USAREUR war-sustainment mission and transition-to-war operations:

(1) AA&E storage, minus bulk storage and unit arms rooms.

(2) Army airfields not covered in paragraph 3-4a(3).

(3) Combat and combat support headquarters headed by a colonel or above.

(4) Direct support (DS) and general support (GS) supply, maintenance, and transportation facilities.

(5) Headquarters designated by the DCSOPS.

(6) Petroleum, oils, and lubricants (POL) bulk storage facilities (not incl those supporting only administrative-use vehicles, unless specifically designated as war reserves).

(7) Stockpiled material, such as prepositioned materiel configured to unit sets (POMCUS).

b. Appendix C prescribes minimum security standards for the facilities in a above. These types of assets will be secured, as a minimum, at risk level II standards.

**3-6. OTHER FACILITIES**

Facilities not identified in paragraphs 3-4 and 3-5 will be protected, as a minimum, at risk level I (app C).

**CHAPTER 4  
INSTALLATION ACCESS**

**4-1. PURPOSE**

This chapter—

- a. Prescribes policy, responsibilities, and procedures on installation access in USAREUR.
- b. Gives procedures for preparing, accounting for, turning in, and disposing of USAREUR installation-access passes and restricted-area badges.
- c. Will be used with AR 600-8-14.

**4-2. APPLICABILITY**

- a. This chapter applies to commanders of commands listed in USAREUR Regulation 10-5, appendix A; members of the U.S. Forces, National Guard, or Reserve on active duty and their eligible family members; DOD civilian employees and their eligible family members; and persons who are authorized to use appropriated fund (APF) and nonappropriated fund (NAF) facilities and have a legitimate need for access to USAREUR facilities and installations.
- b. This chapter does not apply to personnel identification (ID) documents used at sensitive compartmented information facilities (SCIFs).

**4-3. ENTRY AUTHORIZATION**

- a. Any of the documents listed in c and d below may be used to gain access to installations not designated as restricted areas. Documents in e below will be used to control access to restricted areas.
- b. Documents without photographs may be used as access authorization; however, the bearer must still have a form of ID with a photograph (for example, a military ID card, passport).
- c. The following ID cards have photographs:

- (1) DD Form 2(RET), United States Uniformed Services Identification Card (Retired).
- (2) DD Form 2A(ACT) (Army), Active Duty Military ID Card.
- (3) DD Form 2A(RES), Armed Forces of the United States Identification Card (Reserve). This card may be used when the holder is authorized logistic or mission support according to AR 600-8-14 and USAREUR Regulation 600-700. Installation or facility policy may impose restrictions on the use of DD Form 2A(RES) when such support is not

authorized. Access to Reserve training facilities, however, should not be denied.

- (4) DD Form 2AF(ACT) (Air Force), Active Duty Military ID Card.
- (5) DD Form 2MC(ACT) (Marine Corps), Active Duty Military ID Card.
- (6) DD Form 2N(ACT) (Navy), Active Duty Military ID Card.
- (7) DD Form 1173, Uniformed Services Identification and Privilege Card. This card is used for non-U.S. NATO Forces and for DOD civilians. It is valid only overseas.
- (8) DA Form 1602, Civilian Identification.
- (9) DA Form 5431, Army Guard/Reserve Family Member Identification Card. Family members may use DA Form 5431 to enter an installation only when their sponsor is on one of the following training duties ((3) above):
  - (a) Active duty (AD) or active duty for training (ADT).
  - (b) Annual training (AT).
  - (c) Inactive duty training (IDT).
  - (d) Temporary tour of active duty (TTAD).
- (10) AE Form 190-13A, Permanent U.S. Army, Europe, Installation Pass. To receive AE Form 190-13A, applicants must complete AE Form 190-13B (Application for Permanent U.S. Army, Europe, Installation Pass) (para 4-6).
- (11) AE Form 600-410C, USAREUR Civilian Support Identification Card.
- (12) AE Form 600-700A, USAREUR Privilege and Identification Card.
- d. The following may be used as ID or access documents:
  - (1) DD Form 1172, Application for Uniformed Services Identification Card and DEERS Enrollment. DD Form 1172 may be used to gain access to the installation only for obtaining another entry authorization document (for example, DD Form 1173).
  - (2) DD Form 1610, Request and Authorization for TDY Travel of DOD Personnel. Civilians must present DD Form 1610 with a passport.

## USAREUR Reg 190-13

(3) AE Form 190-13C, Temporary U.S. Army, Europe, Installation Pass. Paragraph 4-7 discusses this form.

e. The following are restricted-area access-control documents (badges):

- (1) AE Form 190-13E, Security Badge (Red).
- (2) AE Form 190-13F, Security Badge (Green).
- (3) AE Form 190-13G, Security Badge (Black).

f. For installations without "open" access, persons who are not directly associated with USAREUR or its subordinate elements and who require access to USAREUR installations must be sponsored by a HQ USAREUR/7A staff agency or a USAREUR command. The agency or unit must meet the requirements of a sponsoring agency as defined in the glossary.

g. Solicitation permits do not grant installation access to the holder. These permits are issued and controlled according to AR 210-7 and USAREUR Regulation 210-70, and give authorization only to sell merchandise. Individuals must obtain access and solicitation authority from each installation or community as a separate action.

### 4-4. USAREUR PASSES AND BADGES

a. Appendix D lists forms prescribed by this regulation and provides samples of them. The following are accountable forms and will be issued and controlled by serial number:

- (1) AE Form 190-13A (permanent pass).
- (2) AE Form 190-13C (temporary pass).
- (3) AE Form 190-13E (badge).
- (4) AE Form 190-13F (badge).
- (5) AE Form 190-13G (badge).

b. To order the accountable forms in a above, requesters will use DA Form 4569 (USAPC Requisition Code Sheet).

c. Issuing authorities (para 4-5) will keep a record of each pass and badge issued or destroyed. Records will be maintained on AE Form 600-700C-R (Accountability Register for Privilege and Identification Cards).

d. Passes and badges are U.S. Government property and may not be transferred or altered after they are issued. Lost passes or badges will be reported promptly to the issuing authority. When the need for a pass or badge ends, the commander, supervisor, or sponsor will ensure the pass or

badge is voided and returned to the issuing authority. The issuing authority will destroy the pass or badge by cutting it into small pieces or shredding it, and recording its final disposition. The commander will report passes and badges that cannot be recovered as "lost."

e. Lost or stolen installation passes will be reported to the appropriate issuing authority and to the local PM.

f. ASG and BSB commanders may revoke installation passes. This authority may be delegated to installation coordinators (ICs) when installation access involves only their areas of responsibility.

### 4-5. ISSUING AUTHORITIES

a. AE Form 190-13A issuing authorities are the persons in (1) through (5) below. The commanders in (2) through (4) below may delegate authority for issuing USAREUR-wide passes to regional management level to meet operational requirements.

(1) ASG commanders may issue AE Form 190-13A to persons requiring access to installations in their areas of responsibility. BSB commanders or ICs may issue passes for their local access requirements.

(2) The Commander, Army and Air Force Exchange Service, Europe (AAFES-Eur), may issue AE Form 190-13A to persons requiring access to installations throughout USAREUR to service AAFES-Eur facilities.

(3) The Commander, United States Army Materiel Command, Europe (USAMC-E), may issue AE Form 190-13A to persons requiring access to installations throughout USAREUR to perform services.

(4) The Commander, United States Army Engineer Division, Europe (USAEDE), may issue AE Form 190-13A to persons requiring access to installations throughout USAREUR to perform services.

(5) The PM, USAREUR, may issue AE Form 190-13A to persons requiring access to nonrestricted areas throughout USAREUR and who are not sponsored by a commander in (1) through (4) above. The following procedures apply to passes issued by the PM, USAREUR:

(a) Sponsoring organizations not listed in (1) through (4) above may request an installation pass by sending the following items to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, Bin 154, APO AE 09086:

1. The applicant's completed AE Form 190-13B.

2. Two 1- by 1½-inch photographs of the applicant submitting the AE Form 190-13B.

3. A *Polizeiliches Führungszeugnis* (Police Good Conduct Certificate) when required (para 4-6d(3)(a)). A comment should be entered in block 8 of the AE Form 190-13B that the sponsor has reviewed the Police Good Conduct Certificate.

(b) The PM, USAREUR, or a designated representative, will approve or disapprove issuing an AE Form 190-13A and return the request through command channels to the sponsoring organization.

b. The issuing authority for AE Form 190-13C is the commander of the ASG or installation being visited.

c. The issuing authority for AE Forms 190-13E, F, and G is the commander of the installation or facility where the badge will be used.

d. To control and account for passes and badges, issuing authorities will—

(1) Control procurement, storage, processing, issue, turn-in, recovery, expiration, and destruction.

(2) Establish measures to reduce the possibility of theft, loss, counterfeiting, and improper use.

(3) Establish a uniform method of wearing security badges.

(4) Arrange entry-control points so arriving and departing personnel must pass in single file in front of access-control personnel.

(5) Position racks or containers holding security badges and passes so they are accessible only to access-control personnel.

(6) Authenticate records.

(7) Appoint a responsible custodian to perform control procedures required by AR 600-8-14 and this regulation. As a minimum, standing operating procedures (SOPs) will prescribe instructions on—

(a) Maintaining written records that show forms on hand and those issued, and the disposition of lost, stolen, and destroyed forms. Information will be recorded on AE Form 600-700C-R. AE Forms 600-700C-R will be maintained and destroyed according to AR 25-400-2, file number 640-3c, or on automated data files that include the same data elements as the AE form.

(b) Safeguarding AE forms.

(c) Recovering mutilated or defective AE forms. Sponsoring agencies will collect mutilated or defective forms from discharged, transferred, and deceased personnel, as well as from personnel whose employment or access has been terminated. Collected passes will be returned to the issuing authority with a note explaining circumstances of the action. Collected forms will be destroyed by shredding or by being cut into pieces small enough to make them unusable. Disposition of the forms will be noted.

(d) Conducting unannounced inspections and inventories of issuing procedures and on-hand AE forms. These inspections and inventories will be conducted by a disinterested officer (sergeant first class or above) at least once a quarter. The inspector will document inspection or inventory results and provide a copy of the results to the custodian of the installation pass documents inspected. Discrepancies will be brought to the attention of the commander of the issuing authority.

(e) Inventorying temporary badges daily or at changes in shifts by access-control personnel.

(f) Promptly invalidating lost or stolen security badges and passes and maintaining a current roster of invalidated badges and passes at access-control points.

(g) Recovering permanent and temporary badges at the exit point of the sensitive restricted area where the badges were issued.

(h) Maintaining records at access-control points that enable access-control personnel to determine promptly and accurately the number and identity of persons in the area at any time.

#### 4-6. AE FORMS 190-13A AND 190-13B

a. AE Form 190-13A may be issued—

(1) To U.S. and non-U.S. personnel employed for more than 90 days by USAREUR or other U.S. Government agency, who require continued access to nonrestricted areas and who do not have other valid entry documents (paras 4-3c and d).

(2) As USAREUR-wide access when—

(a) The requester needs routine access to installations in three or more USAREUR ASGs.

(b) The requester and sponsor justify visits in writing through the IC to the issuing authority. Justifications should show that access is needed to support a USAREUR mission or contracted service and is not simply as a convenience.

## USAREUR Reg 190-13

b. AE Form 190-13A will never be issued in place of AE Form 210-70E (USAREUR/USAFE Commercial Solicitation Permit) for vending and solitation. Vendors must coordinate access requirements with individual installations.

c. AE Form 190-13B will be used to request initial issue and renewal of permanent passes, and for replacement of lost passes. AE Form 190-13B will be maintained by the issuing authority and destroyed according to AR 25-400-2, file number 190-21a. When used to replace a lost or stolen pass or badge, the application will include the following information:

- (1) A statement of the circumstances of loss.
- (2) What was done to recover the pass or badge.
- (3) The number of the lost or stolen pass or badge.

d. Application procedures for AE Form 190-13A are as follows:

(1) Applicants must complete blocks 1 through 4, and sign block 9 of AE Form 190-13B.

(2) The supporting civilian personnel service center (CPSC) or the sponsoring unit or organization must complete AE Form 190-13B, blocks 5 through 8, and enter the verifying official's information and signature.

(3) Before submitting the application to the issuing authority, the verifying official must ensure the following actions are completed according to USAREUR Regulation 604-1:

(a) Review the applicant's *Polizeiliches Führungszeugnis* (Police Good Conduct Certificate). A review of this certificate is not required for persons hired through the CPSC or for employees of German local or Federal Government agencies. For initial issue of an AE Form 190-13A, the supporting personnel office or sponsoring organization will attach a copy of the *Polizeiliches Führungszeugnis* as an enclosure to the applicant's AE Form 190-13B.

(b) Submit AE Form 604-1A (Personnel Data Request). AE Form 604-1A will not be submitted for persons hired through the CPSC.

(c) Check the Defense Clearance and Investigation Index on foreign national applicants who have worked for the U.S. Forces in the past.

(d) Enter statements verifying completion of applicable actions ((a) thru (c) above) in block 8 (Remarks) of AE Form 190-13B.

e. AE Forms 190-13A and 190-13B will be prepared as follows:

(1) Issuing authorities must do the following when completing AE Form 190-13B:

(a) Ensure applicant data is complete.

(b) Ensure the checks required by USAREUR Regulation 604-1 (d(3) above) have been completed, annotated, and verified.

(c) Ensure the sponsoring official authentication block is completed (incl the official's signature). The sponsoring official authenticating the application must be a lieutenant colonel, GS-12, or higher-ranking individual.

(d) Enter the pass number, effective date, expiration date, and limitations in the "For Use by Issuing Authority" block.

(e) Complete and sign the issuing-authority authentication block.

(f) Staple one applicant photograph on the front of the completed AE Form 190-13B.

(g) Affix a photograph of the applicant on the AE Form 190-13A to be issued.

(2) Applicants and issuing authorities will sign the AE Form 190-13A.

(3) Completed AE Forms 190-13A will be laminated before they are issued to applicants.

(4) Applicants will sign AE Form 190-13B, block 10, acknowledging receipt of AE Form 190-13A.

(5) Issuing officials will record the issuance on AE Form 600-700C-R.

f. AE Forms 190-13A will not supersede other entry authorization documents needed for access to a restricted area (for example, AE Form 190-13E, F, or G) as required by the responsible commander.

### 4-7. AE FORM 190-13C

#### a. Issue.

(1) AE Form 190-13C may be issued for recurring visits for up to 90 days within an ASG, BSB, or specific installation. AE Form 190-13C will not be valid for more than

90 days, should not be used for a one-time requirement, and will not be issued for USAREUR-wide access.

(2) Pass-issuing authorities will verify access needs with the sponsoring agency.

(3) ASG commanders will determine escort requirements for persons who are issued an AE Form 190-13C. ASG commanders may delegate this authority to BSB commanders or ICs.

(4) ASG commanders may waive AE Form 190-13C requirements for a specific group of contract employees. However, authorities should grant waivers only individually, always keeping in mind that granting waivers may create vulnerable situations.

(5) When a waiver is granted, commanders will ensure an access roster, used in place of the pass requirements, is posted at respective installation-access points. The guards or entry-control personnel will verify each worker's ID (for example, a passport or German *Ausweis* (ID card)) with the posted roster. Commanders will further ensure access rosters are posted for specific times and are collected from access-control points when no longer required.

(6) Organizations sponsoring social functions should provide a guestlist to the IC. On receipt of the guestlist, the IC should brief the sponsoring officials that their guests and their guests' possessions (incl vehicles) will be subject to search according to AR 190-22. The IC should attach a memorandum to the guestlist stating that it has been accepted in place of AE Form 190-13C. The IC will provide the memorandum and guestlist to access-control supervisors, who will provide copies to access-control personnel. The memorandum should indicate a point of contact (POC) from the sponsoring organization, how that person may be contacted, where the function will take place, and time-period the guestlist will be valid. Access-control supervisors will collect the guestlists from access-control points when they are no longer required.

(7) A process server (a court-appointed bailiff) must obtain written authorization from the Commander in Chief, USAREUR, ATTN: AEAJA-IL-I, Unit 29351, APO AE 09014, to perform each service. In these cases, the guard or other entry-control person will admit the process server without an AE Form 190-13C.

(8) AE Form 190-13C is required for employees of the *Technischer Überwachungsverein (TÜV)*. The TÜV is a German agency that inspects U.S. Government high-pressure boilers.

(a) TÜV employees must carry a special pass issued by the appropriate German State in addition to AE Form 190-13C.

(b) Each special pass will be validated for 2 years by a German State. When the pass expires, the German State may revalidate the pass two more times. Revalidations are marked by a stamp on the pass.

(c) The POC for TÜV employees will be a U.S. military or DA civilian employee representative of the sponsoring U.S. engineer office.

**b. Recording Issuance.** Issuing authorities will use AE Form 190-13H(G)-R or 190-13H(I)-R (Personnel/Vehicle Record of Admission) to record the issuance and turn-in of AE Form 190-13C.

**c. Liability To Be Searched.** Issuing authorities will inform the visitors who are issued AE Form 190-13C that they and their possessions (incl vehicles) are subject to search in accordance with AR 190-22. Persons issued AE Form 190-13C will also be informed that the pass must be returned after the visit. The back of AE Form 190-13C has information in English, German, and French about returning the pass. If one of these languages is not the predominant language of the area, the notice should be written in the appropriate language. Access-control personnel will be provided an ample supply of these supplemental notices to present to visitors, as appropriate.

**d. Restrictions.** AE Form 190-13C will not supersede other entry authorization documents needed for access to a restricted area (for example, AE Form 190-13E, F, or G) as required by the responsible commander.

#### 4-8. ALTERNATE INSTALLATION ACCESS PROCEDURES

Conditions may exist where the use of AE Form 190-13C is impractical, such as a facility with a large volume of transient traffic. ASG and BSB commanders may waive the requirement to use AE Form 190-13C for temporary access if an approved local procedure is implemented. The procedure must comply with the following:

a. Commanders must verify local conditions are such that using AE Form 190-13C as outlined in paragraph 4-7 is not practical because of resource limitations or operational necessity. Local procedures will be approved in writing by the ASG commander.

b. Exceptions will apply to a single installation or facility.

c. Local procedures will require use of an access device (pass or access roster) that distinctly indicates the applicable installation or facility and the individual's full name, place of duty, and ID (passport or *Ausweis*) number.

## USAREUR Reg 190-13

d. Each individual will be required to present ID to the guard at the point of entry. The guard will verify the photograph on the ID is that of the bearer, and will check the number on the ID against the local access device. Individuals will not be required to surrender personal ID to be granted access.

e. Local procedures will be augmented during periods of increased THREATCONs by using a sign-in/sign-out system.

### 4-9. AE FORMS 190-13E, 190-13F, AND 190-13G

#### a. General.

(1) AE Forms 190-13E (Red), F (Green), and G (Black) will be used only at USAREUR sensitive restricted areas and other sensitive areas that require special access controls. Badges will be worn at each area as determined by the commander. The position in which worn (such as, on the left lapel or the right shoulder) should not interfere with the normal work of the wearer.

(2) Commanders may use AE Form 190-13E, F, G, or any combination of the forms to suit their access-control needs, except as otherwise provided in this regulation. Commanders may elect to use a commercially designed security badge or pass or a combination thereof to meet special security needs in place of AE Forms 190-13E, F, or G. If commercially designed badges or passes are used, they will meet standards in AR 600-8-14 and this regulation.

**b. Permanent Pass.** AE Form 190-13E, F, or G may be issued as a permanent pass to a person requiring continual access to sensitive restricted areas. The following conditions apply to such passes:

(1) A clear photograph of the person with a title board that includes the name of the person will be put over the letter "T" on the front of AE Form 190-13E, F, or G.

(2) The form will be completed in its entirety, except the social security number (SSN) will not be entered in the "NAME, SN, OR CATEGORY" block. Fingerprints are not required.

(3) The form will be signed by the badge custodian or designated representative and will be laminated to prevent tampering.

(4) The permanent pass will be presented to access-control personnel at the entrance to sensitive restricted areas. Access-control personnel will compare the ID data and photograph on the permanent pass with the person presenting the pass.

**c. Permanent Badge.** AE Form 190-13E, F, or G may be issued as a permanent badge to a person requiring continual access to highly-sensitive restricted areas. The permanent badge will be prepared in the same manner as the permanent pass, except it will have a clip-on attachment allowing it to be worn at all times on an outer garment while the bearer is in the restricted area.

**d. Temporary Badge.** AE Form 190-13E, F, or G may be issued as a temporary ID document for visitors who require entry to a sensitive restrictive area. AE Form 190-13E, F, or G also may be used by personnel requiring continual access while a permanent badge is being prepared. Custodians may require visitors to release personal identification documents in exchange for a temporary badge or pass. When temporary badges are used, they will—

(1) Include information on the issuing unit and be signed by the issuing authority. Photographs and personal information about the bearer are not required.

(2) Be laminated and have a clip allowing them to be worn on outer garment while in the restricted area.

(3) Be easily distinguishable from permanent security badges and passes. Visitors will be escorted at all times while in a restricted area. Entry and exit of visitors will be recorded.

**e. Exchange for Other Documents.** AE Form 190-13E, F, or G may be issued in exchange for another entry authorization document. When used as an exchange document, it will have the same descriptive information as the form it replaces. A photograph meeting the requirements of AR 600-8-14 is required. The SNN is not required. The exchange document will be a different color from the document for which it is exchanged. The permanent badge may be issued in exchange under one of the following situations, as directed by the installation commander:

(1) The holder of AE Form 190-13A may exchange it for a permanent AE Form 190-13E, F, or G at the point of entry to the sensitive restricted area. The access controller will compare the photograph and descriptive data on the AE Form 190-13A with the bearer at the time of exchange and when the bearer leaves the area.

(2) The holder of a permanent or temporary AE Form 190-13E, F, or G may exchange it for another permanent or temporary AE Form 190-13E, F, or G at the access-control point to a sensitive restricted area different from the area for which the badge was issued.

**f. Reissue.** AE Forms 190-13E, F, and G will be reissued individually every 3 years after the date of initial issue or reissue. AE Forms 190-13E, F, and G will be reissued completely when 5 percent of all forms currently in use are unaccounted for.

**g. Preparation.** AE Forms 190-13E, F, and G will be prepared as follows:

(1) The custodian of AE Forms 190-13E, F, and G will enter the local control number by stamp or typewriter in the "BADGE NO" block on the front of the form. (A serial number is preprinted on the back of each form.)

(2) The "VALID FOR AREA(S)" block may be used for a block numbering system, a lettering system, or a system based on the card's color.

(3) Fingerprints and classification markings are not required.

(4) Access-control personnel will be familiar with the signature of the issuing officer on the front of AE Forms 190-13E, F, and G.

(5) Effective dates will not exceed 3 years from the date of issue. A person whose assignment is expected to be less than 3 years will be issued AE Form 190-13E, F, or G with an effective date for the duration of the expected assignment.

(6) Fingerprints and classification markings are not required on AE Forms 190-13E, F, and G.

(7) AE Forms 190-13E, F, and G do not need to be reissued when the issuing officer departs.

**4-10. CONFISCATING ID CARDS, PASSES, AND BADGES**

a. Commanders and issuing authorities will strictly follow the provisions of AR 600-8-14 and USAREUR Regulation 600-700.

b. Access-control personnel will avoid embarrassing situations and disturbances, but will deny access to persons with expired, severely damaged, or altered ID or installation-access documents. If access is denied, access-control personnel will confiscate installation-access passes and badges if that document is expired, severely damaged, or altered. Access-control personnel will inform the supporting law enforcement activity when a passbearer refuses to surrender an expired, altered, or severely damaged ID or installation-access document.

c. Access-control personnel (except military police (MP) personnel) who confiscate ID documents (b above) will complete AE Form 190-13D (Receipt for Confiscated ID Card) and give the completed form to the person surrendering the document. MPs will provide a receipt for confiscated ID documents with DA Form 4137 (Evidence/Property Custody Document). The confiscated ID card, pass, or badge will be turned over to the nearest issuing agency or authority, or to the MP office when the document is needed for evidence.

d. Access-control personnel will not require individuals to surrender personal ID devices to be granted access to USAREUR installations unless special requirements are specified in the policy on special-access programs.

**4-11. REPORTING PERSONS BARRED FROM INSTALLATIONS**

a. ASG commanders will report persons barred from USAREUR installations to the Commander, 1st Personnel Command, ATTN: AEUPE-PSSD-PAD, Unit 29058, APO AE 09081, according to AR 600-20.

b. The Commander, 1st Personnel Command (1st PERSCOM), will regularly publish a list of persons barred from USAREUR installations. Commanders or their designated representatives will review this list before issuing access-authorization documents.

**4-12. SPECIFIED-COUNTRY CITIZENS**

USAREUR Supplement 1 to AR 380-67 defines specified-country citizens and prescribes policy and procedures for their entry onto USAREUR access-controlled installations.

**4-13. INSTALLATION ACCESS BY GERMAN POLICE**

**a. Purpose.**

(1) This paragraph provides guidance for the entry of German police (GP) onto U.S. accommodations for the purpose of criminal investigation, hot pursuit, and apprehension.

(2) This paragraph does not include policy on GP access in cases of hostage taking, terrorist acts, armed violence, or similar criminal incidents; demonstrations; catastrophes; or accidents. These conditions are covered by the SOP for Community Commanders-Installations Commanders of U.S. Forces Accommodations in Germany, subject: Procedures for Entry Onto U.S. Forces Accommodations by the German Police and Cooperation With the U.S. Forces in Cases of Major Disturbances, 8 November 1989; and agreements on this subject reached between appropriate German State (*Land*) Governments and USAREUR *Land* liaison offices.

## USAREUR Reg 190-13

**b. Jurisdiction.** The U.S. Forces may exercise the police jurisdiction (NATO SOFA, art VII, para 10(a)) on the accommodations made available to the U.S. Forces for exclusive use (SA to NATO SOFA, art 53, para 1). Exercise of German jurisdiction, however, is not excluded, because an extraterritoriality of accommodations of foreign armed forces stationed in Germany is not provided for in the NATO SOFA. To safeguard the security and protect the property of the U.S. Forces and, for the protection of German interests, the GP have an inherent need for access onto U.S. accommodations.

**c. Procedures.** The local PM or designated representative will support the GP to the greatest extent possible in accordance with the NATO SOFA, supplements to it, and applicable U.S. and HN laws, directives, and regulations. To do this, the local PM or designated representative will—

(1) Establish and conduct liaison with the GP having jurisdiction for each respective U.S. accommodation and establish procedures for installation access by GP. The PM or a designated representative will not, however, conclude any agreements with the GP or other German authority other than establishing administrative working procedures to implement the provisions of this regulation. The liaison should ask GP to—

(a) Use blue lights when entering U.S. accommodations in hot pursuit (defined in the glossary). Plain-clothes GP should identify themselves by showing their badges or credentials. U.S. guard personnel will not delay GP in hot pursuit; but, will immediately notify the MP desk sergeant, who will request all gates to the installation be closed and remain closed until the suspects are apprehended. MP patrols will be dispatched to close unguarded gates if possible.

(b) Coordinate with the local PM office or MP station before entering the installation to conduct routine investigations. The MP may accompany GP during routine investigations on a U.S. installation.

(c) Coordinate with the local PM when entrance to buildings or quarters in U.S. housing areas is required. On notification by the PM, MP will accompany GP to help deal with residents. This coordination requirement does not apply during hot pursuit.

(2) During emergencies, provide GP with a liaison who is familiar with the area. The U.S. Forces will provide a qualified interpreter if required.

**d. Entry to Restricted Areas.** Unless specifically permitted by the U.S. representative in charge (for example, PM, officer in charge (OIC), noncommissioned officer in charge (NCOIC)), do not allow the GP to enter areas, buildings, or portions of buildings designated "restricted." In hot-pursuit

situations, the OIC, NCOIC, or staff duty officer (SDO) may grant this permission and immediately notify the PM. Entry will be granted only in accordance with applicable security regulations and only when it would otherwise be impossible to conduct an investigation.

**e. Cost and Claims.** Waivers of costs for the services provided will be in accordance with HN laws and regulations. Claims for personal injuries and property damage, resulting from GP actions on U.S. installations will be resolved according to applicable provisions of the NATO SOFA and supplemental agreements.

### 4-14. DA FORM 1818

a. Commanders will issue DA Form 1818 (Individual Property Pass) to authorize personnel to carry Government or personal property onto or out of restricted areas. Commanders may use DA Form 1818 on other installations requiring controlled access as a crime-prevention and physical-security tool.

b. A temporary DA Form 1818 will be issued to persons who have a one-time need to carry authorized items onto or out of an installation.

c. A permanent DA Form 1818 will be issued to persons who require continual access to an installation and possession of articles described on the pass (for example, maintenance toolkit).

d. DA Form 1818 will be prepared as follows:

(1) Custodians will complete DA Forms 1818 in 2 copies. Entries on the form may be handwritten in ink or typed. SSNs will not be put on the forms.

(2) Temporary forms will include an expiration date, not to exceed 1 week from date of issue.

(3) Permanent forms will have an expiration date not to exceed 3 months after the date of issue. A new permanent DA Form 1818 may be issued for an additional 3 months.

e. Custodians will issue the original DA Form 1818 to the person authorized to carry the articles described onto or out of the installation. The custodian will keep the second copy of DA Form 1818 at the point of issue.

f. When the bearer of a temporary DA Form 1818 leaves the area for which the pass was issued, the bearer will return the original pass to the custodian. The custodian will examine the property to ensure only authorized property is removed from the installation. The custodian will attach (for example, with a paperclip) the original and duplicate passes and keep

them in custodial unit files. The custodian will hold the forms for 3 months and then destroy them.

g. The bearer of a permanent DA Form 1818 will return the pass to the custodian when the pass expires. The custodian will attach (for example, with a paperclip) the original and duplicate forms, keep them in the custodial unit files for 3 months, and then destroy them.

**4-15. RECORDING ENTRY INTO CONTROLLED AREAS**

Access-control personnel will use AE Form 190-13H(G)-R or 190-13H(I)-R to document the entrance and exit of visitors to installations and activities requiring controlled access, and to sensitive restricted areas. AE Forms 190-13H(G)-R and 190-13H(I)-R will be maintained and destroyed according to AR 25-400-2, file number 190-13b.

## CHAPTER 5 PHYSICAL SECURITY OF AA&E

### 5-1. PURPOSE

This chapter establishes responsibilities and procedures for the physical security of AA&E in USAREUR. This chapter will be used with AR 190-11.

### 5-2. STRUCTURE STANDARDS

a. Structural standards for AA&E storage facilities must be verified on DA Form 4604-R (Security Construction Statement) by qualified engineer personnel (AR 190-11). If qualified engineer personnel are unable to provide verification, they will explain why the structural standards cannot be verified. It is not sufficient to merely state construction standards "could not be verified." The nature of the structural deficiencies must be explained so that it can be determined what is required to correct the deficiencies or whether or not it is possible to request a waiver or exception.

b. Verification of structural standards of AA&E storage facilities on DA Form 4604-R does not apply to U.S. Army units occupying facilities on some joint-use installations. Specifically, joint-use installations where HN authorities have primary control of the installation and are responsible for construction, maintenance, and general administration of the storage facilities are exempt from AR 190-11 verification requirements.

### 5-3. WAIVERS AND EXCEPTIONS

Only HQDA (DAMO-ODL-S) may approve waivers and exceptions to physical-security standards. Appendix E prescribes procedures for processing these requests.

### 5-4. INVENTORY AND ACCOUNTABILITY

a. Unit commanders will ensure—

(1) A serial-number inventory is conducted each month of all weapons and ammunition.

(2) Records are maintained according to AR 190-11; AR 710-2, paragraphs 2-12, 2-42, and 3-29; and DA Pamphlet 710-2-1, paragraphs 9-10 and 9-11b.

b. Weapons assigned to soldiers will be issued and controlled per AR 190-11 and DA Pamphlet 710-2-1, paragraph 5-5b.

### 5-5. IDS

a. Chapter 6 provides guidance on operating, maintaining, procuring, and using IDS.

b. Every AA&E storage facility that contains category I or II AA&E will be equipped with IDS (AR 190-11). If an IDS fails, armed guards will be posted until the IDS is restored. In bulk storage facilities, guards will be posted where they can maintain constant, unobstructed observance to the entrances of a row, section, or column of affected storage facilities (structures). Additionally, when an IDS fails, the interval between security patrol checks will not exceed 1 hour for category I AA&E, and 2 hours for category II AA&E.

c. IDS response forces will be tested by ASG and BSB commanders not less than once each quarter to determine the adequacy of training, procedures, and equipment. These tests will be recorded in writing. During scheduled physical-security inspections of AA&E facilities, the inspector will verify that the response force for that facility has undergone such tests.

### 5-6. K&LC

a. Keys providing access to category I or II AA&E that are not in use or are not attended will be stored in a class 5 General Services Administration (GSA) security container or equivalent. Commanders will establish K&LC procedures according to AR 190-11, paragraph 3-8.

b. Spare keys will not be kept with operational keys. The next higher headquarters will keep spare keys. When the higher headquarters is far from the storage site, the keys will be stored in a depository per agreement between the user and a host unit (such as a BSB, ASG, or other major headquarters on the casern).

c. Maintenance keys for high-security padlocks will not be used as primary access keys. Maintenance keys will be secured as in b above and will be kept separate from spare keys. Placing maintenance keys in a separate, sealed envelope in a container with the spare keys constitutes acceptable separation.

d. The next higher headquarters must inventory and sign for the spare keys and maintenance keys, or sign for a locked sealed container on DA Form 2062 (Hand Receipt/Annex Number) (for example, "Container protected by seal #12345 that contains arms room keys."). If keys are stored in a locked, sealed container, the custodian of the keys will keep the key for the container lock and a copy of the receipt for the container. Key containers weighing less than 500 pounds will be fastened to the structure with bolts or chains equipped with secondary padlocks to preclude easy removal.

e. Keys to the IDS control-unit door and monitoring cabinet will be kept separate from other IDS keys, and access will be limited to authorized maintenance personnel. These

## USAREUR Reg 190-13

keys may be signed out to DEH maintenance personnel; however, they must be accounted for at all times and inventoried at least twice a year.

### 5-7. REPORTING MISSING AND RECOVERED AA&E

When AA&E is lost, missing, stolen, or recovered, PMs or designated representatives will initiate a DA Form 3056 (Report of Missing/Recovered Firearms, Ammunition, and Explosives) within 72 hours and send 1 copy to each of the following addresses:

a. Commander in Chief, USAREUR, ATTN: AEAPM-OPS, Unit 29931, APO AE 09086.

b. Commander, 5th Military Police Detachment (CID), ATTN: CIRCE-ZA, Unit 29201, APO AE 09102.

c. HQDA (DAMO-ODL-S), Suite 225, 4401 Ford Ave, ALEX, VA 22302-1432.

d. Director, Crime Records Center, 2301 Chesapeake Avenue, Baltimore, MD 21222-4099.

### 5-8. TRANSPORTING AA&E

Appendix C prescribes minimum security requirements for transporting AA&E in Europe by rail and by noncommercial motor vehicle. For other types of unit movement and for commercial movement, see AR 190-11. Movement of AA&E must be coordinated with the HN to ensure no conflicts exist in providing the required security measures.

### 5-9. AE FORM 190-13I

a. AE Form 190-13I (Issue of Weapons and Ammunition) will be used to issue weapons (incl privately owned weapons). If, however, a military weapon is issued for less than 24 hours, AE Form 190-13I is not required, unless ammunition is issued with the weapon.

b. Before issuing a weapon using AE Form 190-13I, the armorer must receive a DA Form 3749 (Equipment Receipt) for the weapon from the individual. After the soldier returns the weapon, the armorer will return the DA Form 3749.

c. AE Form 190-13I will be kept until the monthly inventory is completed. The form may be destroyed after the monthly inventory unless the monthly inventory reveals a discrepancy (for example, weapon still signed out), in which case the form will be kept until the discrepancy is resolved.

d. DA Form 2062 may be used instead of a weapons card (DA Form 3749).

e. AE Form 190-13I will be completed as follows:

**(1) Block 1, UNIT OR STATION.** Self-explanatory.

**(2) Block 2, RACK NUMBER.** The unit armorer or issuing authority should print the rack number (also known as the weapon number, assigned by the unit) from which the weapon is taken. If the weapon is not from a rack, the number of the secure storage container should be printed in this block.

**(3) Block 3, TYPE OF WEAPON.** The unit armorer will list the nomenclature of the weapon (for example, M16A1). Bayonets issued with weapons should also be listed (for example, M16A1w/B).

**(4) Block 4, SERIAL NUMBER.** Self-explanatory.

**(5) Block 5, NUMBER ROUNDS.** Self-explanatory. If no rounds were issued, then "0" goes in this block. Block 5 should never be blank.

**(6) Block 6, TIME OUT.** The person accepting the weapon will enter the date and time the weapon was issued.

**(7) Block 7, TO (SIGNATURE).** The person accepting the weapon will sign his or her name.

**(8) Block 8, BY (INIT).** The issuing armorer will enter his or her initials after ensuring that all weapon information is correct.

**(9) Block 9, TIME IN.** The person turning in the weapon will enter the date and time the weapon is turned in.

**(10) Block 10, NUMBER ROUNDS.** The armorer will enter the number of rounds being turned in. If no rounds were turned in, "0" will be entered. Block 10 should never be blank.

**(11) Block 11, TO (SIGNATURE).** The armorer receiving the weapon will sign for the weapon.

**(12) Block 12, BY (INIT).** The person turning in the weapon will enter his or her initials.

**CHAPTER 6  
ELECTRONIC SECURITY SYSTEMS**

**6-1. PURPOSE**

This chapter—

a. Prescribes policy, responsibilities, standards, and procedures for selecting, acquiring, and using ESSs in USAREUR.

b. Will be used to develop IDS programs.

c. Does not include procedures for special weapons storage facilities.

d. Does not include ESS procedures for cryptological facilities (SCIFs). SCIF procedures are in AR 380-5 and Director of Central Intelligence Agency Directive 1/21.

**6-2. PHYSICAL-SECURITY EQUIPMENT OVERVIEW**

a. As defined in Technical Manual (TM) 5-853-4, ESSs include IDSs, closed-circuit televisions (CCTVs), and entry-control systems (ECSs). These systems can be used as measures to improve a facility's physical-security posture.

b. When properly designed, installed, and maintained, ESSs are valuable additions to USAREUR and individual command physical-security programs. Effective use of an ESS requires a "total-system approach" that integrates policy, procedures, equipment, protective construction, and awareness. This requires a coordinated effort by the unit and the supporting PM office, DEH, directorate of information management (DOIM), and directorate of logistics (DOL).

c. Electronic systems may reduce guard requirements by providing cost-effective, continual surveillance, detection, assessment, delay, response, and access-control protection.

d. A basic IDS consists of a sensor connected to a control unit. This control unit is linked to a monitored annunciator console. The IDS is supported by a security response force. IDS is useless unless it is properly operated, monitored, and supported by prompt security-force action when the system is activated.

**6-3. PLANNING GUIDELINES**

AR 190-13, paragraph 4-15, discusses planning for ESS and IDS. IDS and other ESS applications will be planned, budgeted, procured, and initiated the same as other Army systems. AR 190-13, paragraph 4-16, and this regulation, paragraphs 6-6 through 6-12, explain project submission and acquisition procedures.

a. ESS equipment projects will be initiated—

(1) As the result of a physical-security survey, risk analysis, or inspection identifying vulnerabilities that can be reduced by the installation of an ESS.

(2) To comply with regulatory requirements.

(3) To meet security requirements identified during the design of Military Construction, Army (MCA), projects.

(4) To meet security requirements identified during the design of Operation and Maintenance, Army (OMA), funded renovation projects. These projects may require programming Other Procurement, Army (OPA), funds if new equipment must be purchased.

(5) To employ ESS as an alternative to guards to ensure continuous surveillance or to maintain access control.

(6) To consolidate alarm monitors to conserve manpower.

b. Use of other than joint-services interior intrusion detection system (J-SIIDS) components to meet IDS requirements requires approval from the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086. HQ USAREUR/7A will not consider approval of a commercial intrusion detection system (CIDS) unless—

(1) The system requirements exceed the capabilities of the alarm monitor group (AMG) 25 to 64 zones.

(2) The system supplements an existing commercial system.

(3) The proposed system requires exterior sensors.

(4) There is an architectural or technical problem with installing J-SIIDS.

(5) CIDS would be more cost-effective than J-SIIDS.

(6) A low-priority NAF requirement is involved.

(7) The project involves HN requirements that stipulate the use of CIDS.

c. When an MCA project requires a J-SIIDS or CIDS—

(1) Provide an estimate of the required installation funds as a line item on the front page of DD Form 1391 (FY##, Military Construction Project Data) submitted to HQDA for approval. If IDS installation funds were omitted from DD Form 1391, a user change request for the IDS will be submitted to the Commander, United States Army Engineer District, Europe, Unit 25727, APO AE 09242.

## USAREUR Reg 190-13

(2) Include OPA funds to purchase CIDS.

d. Programming IDS for NATO projects will be as follows:

(1) NATO supports IDS (CIDS or NATO IDS) when specified in the applicable NATO Criteria & Technical Standards for an approved infrastructure category. Any U.S. requirement for IDS that exceeds, either wholly or in part, NATO criteria must be paid from the appropriate U.S. national fund sources (OMA or OPA).

(2) If the applicable NATO Criteria & Technical Standards does not require IDS at a U.S.-used NATO facility, the U.S. Government must supply both the IDS, as Government-furnished equipment (GFE) to be forecasted through OPA funds, and OMA funding for design and installation.

(3) If the U.S. Government requires a GFE IDS (J-SIIDS) to be installed in place of a NATO IDS, the U.S. Government will receive a "credit" from NATO equal to the value the IDS NATO would have installed. Both the credit size and a cost-share formula will be agreed on at a NATO construction project "phase" (design) meeting. A credit may be applied at the same location toward another item of construction that exceeds NATO Criteria & Technical Standards, or that amount will be credited to the U.S. NATO Infrastructure Budget. The credit cannot be applied towards the purchase of a U.S. (GFE) IDS.

(4) Although preliminary construction measures normally required for IDS installation (regardless of the system) (such as wall conduits, cable trenching, J-boxes) usually are funded and executed by NATO when part of a larger project, installation of a U.S.-procured system may be done by NATO, but usually will be performed by the responsible DEH. DEH documentation of project costs to the U.S. Government must include real property improvements required to support the system that were not NATO funded.

(5) More detailed information on IDS program funding of construction in excess of NATO Criteria & Technical Standards, referred to as "conjunctive funding," is in USAREUR Regulation 415-22, paragraph 4-3.

e. Except for MCA projects, IDS installation must be done with OMA funds. Budget activity 11 (BA11) mission funds may be used for J-SIIDS installation only with PM, USAREUR, approval.

### 6-4. PRIORITIES

Priorities for IDS or other ESS installations will depend on the asset, type of facility, and degree of protection required. AA&E IDS requirements are listed in AR 190-11. Guidance on other facilities where IDS should be integrated into the total security system is in AR 190-13, paragraph 4-10. Pri-

orities for installation will be consistent with the guidance in AR 190-13, paragraph 4-9.

### 6-5. RISK ANALYSIS

PM offices will conduct risk analyses in coordination with local security managers, organization commanders, or facility managers. Integral to the risk analyses are threat assessments, normally provided by supporting military intelligence units and criminal investigation divisions (CIDs). Units will request risk analyses according to AR 190-51, paragraph 2-2. The results of risk analyses will be used during planning to identify, assess, and validate physical-security requirements (incl the need for IDS or other physical-security equipment (PSE)).

### 6-6. FORECASTING

a. Units must forecast IDS and other ESS technology applications before acquisition. Forecasting ensures components and funds will be available when the IDS is required. Forecasts will cover a 7-year period by fiscal year. This is mandated by law, and it supports the Program Objective Management (POM) Program and Future-Year Defence Plan (FYDP). The forecast must identify the project; the location and unit the project supports; fiscal year required; justification; priority code (AR 190-13, para 4-9); OMA funds to reimburse design, site preparation, and installation costs; and OPA funds for equipment procurement. The forecast must include a consolidated equipment list that indicates, by fiscal year, the quantity of each J-SIIDS component required.

b. The user unit will coordinate forecasts with the supporting DEH and DOIM and submit them through servicing PM channels. ASGs will consolidate, review, and prioritize forecast requirements (AR 190-13, para 4-9) before submitting them to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086.

c. Forecast submissions are not approvals for IDSs. A site survey is required before approval for funding. The results of the site survey are required to support the project request packet, which must be submitted to the PM, USAREUR, as specified in paragraphs 6-12 and 6-13.

d. On annual forecasts, ASGs will note—

- (1) Previously forecasted projects no longer required.
- (2) Installations suspended to another fiscal year.
- (3) Changes in funding or equipment requirements.

e. J-SIIDS should be programmed for replacement between 10 and 15 years after initial installation or the last life-cycle replacement date. The service life varies from system to

system. The servicing DEH will determine the re-placement date.

f. IDS PSE technologies not forecasted but required immediately may affect forecasted projects. A project request packet, prepared according to paragraphs 6-12 and 6-13, must be sent to the PM, USAREUR, to obtain funding approval. When submitting unforecasted requirements, document the extenuating circumstances that prevented forecasting.

**6-7. IDENTIFICATION AND VERIFICATION OF REQUIREMENTS**

Users will identify and verify IDS requirements based on the following:

- a. Requirements and priorities from applicable regulations (for example, AR 190-11, AR 190-13, AR 190-51).
- b. Latest physical-security inspections, surveys, and risk analyses (AR 190-51).
- c. Crime statistics.

**6-8. COORDINATION**

a. Site surveys must be conducted and submitted to the PM, USAREUR, for approval. Site surveys are required before approval of funding. Users will coordinate a site survey according to the U.S. Army Corps of Engineers (Huntsville District) Site Survey Procedures Guide for Intrusion Detection Systems or other applicable ESS survey guides. Site survey coordination requests will be in writing and include a request for—

- (1) PM office assistance in conducting a risk analysis. Risk analyses are used in planning stages to identify, assess, and validate physical-security requirements.
- (2) DEH assistance for design, estimates, and installation (submitted on DA Form 4283 (Facilities Engineering Work Request)).
- (3) DOIM representative assistance in coordinating communications media.
- (4) DOL assistance for equipment procurement and property book accountability.

b. Extensive or complex commercial technology projects may require the expertise and participation of the Huntsville Division IDS Technical Center of Expertise (IDS MCX) to properly complete the survey. Users must coordinate their request for IDS MCX technical assistance with the PSE Program Manager, USAREUR.

**6-9. REQUEST PACKET (J-SIIDS)**

A J-SIIDS project request packet with the following information must be sent through the ASG PM, with review and endorsement by the DEH, DOIM, and DOL, to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086:

- a. Request for system approval.
- b. Copies of all equipment requisitions (DA Forms 2765-1 (Request for Issue or Turn-In) or DD Forms 1348-6 (DOD Single Line Item Release/Receipt Document) completed per DA Pam 710-2-1).

**NOTE:** J-SIIDS end-item components are furnished free as initial issue to user installations. The components are paid for with OPA funds from the U.S. Army Aviation and Troop Command (ATCOM). J-SIIDS replenishment components and repair parts, however, must be funded by the user installation from OMA funds.

c. Statement identifying the basis for project submission. The statement should clearly identify that the project was submitted to—

- (1) Meet a regulatory requirement (incl citing the applicable AR number and paragraph down to the lowest subparagraph that has the requirement).
- (2) Reduce a vulnerability identified during a risk analysis or physical-security survey.
- (3) Produce manpower savings.

d. Designated security level of the facility as defined in AR 190-13, paragraph 4-10.

e. List of materials (incl cost estimate for system installation). (See DEH automated IDS cost estimator CEHND-SP-93-268-ED-ME.)

f. A completed site survey and engineer blueprints or drawings of the protected area and component locations.

g. Projected fiscal year for system installation.

h. A request for USAREUR OMA funds to reimburse design, site preparation, and installation of the system.

i. A statement that ASG base operations (BASOPS) funds are available for maintenance of the system.

j. Other information supporting the IDS requirement (for example, physical-security inspections, surveys).

## USAREUR Reg 190-13

### 6-10. REQUEST PACKET (COMMERCIAL ESS)

If conditions of paragraph 6-3b exist, send a commercial ESS project request packet through ASG PM channels to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086. The packet must include the following information:

a. A request for system approval and funding (incl cost estimates for purchase and installation).

b. POC and telephone number, and a funding authority (to receive DD Form 448 (Military Interdepartmental Purchase Request (MIPR)) from ATCOM.

c. Statement identifying the basis for project submission. The statement should clearly identify that the project was submitted to—

(1) Meet a regulatory requirement (incl citing the applicable AR number and paragraph down to the lowest subparagraph that has the requirement).

(2) Reduce a vulnerability identified during a risk analysis or physical-security survey.

(3) Produce manpower savings.

d. Designated security level of facility as defined in AR 190-13, paragraph 4-10.

e. Justification as to why J-SIIDS GFE security equipment cannot meet requirements.

f. Justification as to why an existing system cannot be expanded, if the selected CIDS requires an additional monitor panel.

g. A completed site survey, technical specifications of proposed components, and engineer blueprints or drawings to scale of the system (protected area and component locations).

h. Projected fiscal year for system installation.

i. A statement that ASG BASOPS funds are available to maintain the system.

j. Other information supporting the requirement (for example, physical-security inspections, surveys).

k. Security engineering surveys for projects that are beyond the local capability. These surveys may be requested through the PM, USAREUR, and conducted on a reimbursable basis by the United States Army Corps of Engineer (Protective Design or IDS MCX).

### 6-11. TECHNICAL REVIEW FOR COMMERCIAL ESS

a. Requests for purchase, lease, or lease renewal of commercial ESS (incl electronic entry-control devices and CCTVs (if connected to an IDS and used in a surveillance or assessment mode)) will be sent through PM channels to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086. The PM, USAREUR, will forward technology designs to the Physical Security Equipment Management Officer (PSEMO), ATTN: AMSAT-I-WTP, Fort Belvoir, VA. The PSEMO will review the designs to ensure they integrate compatible equipment components to produce an operating unit capable of providing total, reliable, and continuous monitoring. The review will include the following:

(1) Evaluation of physical-security requirements to determine if the system or equipment will significantly improve protection.

(2) Evaluation of the technical specifications and design of requested CIDS or commercial PSE technologies to determine suitability for use with other DOD standardized systems or commercial systems already in use or under development.

(3) Evaluation to ensure the requested system counters the threat without unnecessary expenditure.

b. Commercial ESS technologies may be approved if it is determined that DOD standardized equipment is not reasonably available, is not cost-effective, or does not meet the requirements of a particular facility.

c. Technical criteria for planning, designing, and procuring CIDS are prescribed in USAREUR Regulation 420-43. These criteria will be used for either direct (in-house) or for indirect (ABG-75) projects.

d. A technical review of standardized PSE (for example, J-SIIDS) is not required.

### 6-12. IDS ACQUISITION PROCEDURES

a. Under no circumstances will the user procure or allow security technologies to be installed without PM, USAREUR, approval. The PM, USAREUR, will review system-request-submission packets in coordination with the Deputy Chief of Staff, Engineer (DCSENGR), USAREUR, and, if approved, will assign a control number and notify the user and supporting ASG PM. The PM, USAREUR, will require ASG PMs to revalidate approved requirements at least once each year.

b. For J-SIIDS, users will prepare requisitions according to AR 725-50 and submit requisitions, with PM, USAREUR approval, through the appropriate DOL property book officer (PBO). Initial-issue items are funded by ATCOM and cost users nothing for new installations. Users will pay for replacement of nonexpendable components.

c. Users will send requests for ESS funding, with supporting documents, through ASG PM channels to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086.

d. For commercial ESS that have been approved by HQ USAREUR/7A, DEH will initiate procurement using negotiated procurement procedures (if more than six zones).

### 6-13. PHYSICAL-SECURITY PLANS

a. ASG and BSB physical-security plans will identify IDS locations and include the type of—

- (1) Area or structure being protected.
- (2) Sensors used.
- (3) Response forces required and source providing the response forces.

b. An annex to the force-protection plan will include detailed instructions on—

- (1) Monitoring procedures.
- (2) Response-force procedures.
- (3) Testing and inspection requirements.
- (4) Actions to be taken in the event of a power failure.
- (5) Identification of auxiliary power sources.

c. Associated with the physical-security plan, the ASG will maintain a database that includes the following:

- (1) Using unit.
- (2) Casern, building, room number, and type of facility protected.
- (3) Date of installation or life-cycle replacement.
- (4) Facility priority code according to AR 190-13, paragraph 4-9.
- (5) Monitor location.

(6) Monitor personnel.

(7) Type of system.

(8) Manufacturer name.

(9) Type of sensors in use.

(10) Source providing response force.

### 6-14. IDS CATEGORIES

IDS consists of intrusion sensors connected to a monitor cabinet backed by a security response force. Intrusion sensors detect through sound, vibration, motion, electrostatic emissions, and light beams. Information on categories of sensors and their recommended use is in FM 19-30, chapter 7; TM 5-853-4 provides technical criteria. The following are the categories of sensors:

**a. Penetration Sensors.** Sensors that detect penetration of a protected area, including entry through doors, windows, walls, floors, ceilings, or other openings in a room.

**b. Volumetric Sensors.** Sensors that detect the movement of an object inside a protected area.

**c. Duress Switches.** Switches that are activated by an armorer, employee, duty person, guard, or protected person to call for assistance.

**d. Point Sensors (Magnetic Sensors, Capacitance Proximity Sensors).** Sensors designed to detect the attempted removal of an item from its normal position within the protected area (for example, weapons racks, storage cabinets, safes, security containers, desks).

### 6-15. RECOMMENDED SENSORS

a. Balanced magnetic switches are the recommended primary sensors for detecting the opening of doors and windows. These switches are used with passive ultrasonic or passive infrared sensors secured to ceilings, walls, and floors.

b. Grid-wire sensors or vibration sensors may be used for securing floors, walls, and ceilings, and openings such as doors and windows.

c. Ultrasonic motion sensors are the recommended primary sensors for detecting movement inside a facility. Passive infrared and microwave motion sensors are other types of sensors used for detecting movement in a facility.

d. Capacitance proximity sensors and magnetic weapon sensors may be used for detection inside a facility and are recommended to protect class-5 weapon containers.

## USAREUR Reg 190-13

e. The alarm-latching switch (duress alarm) should be used with balanced magnetic switches and motion sensors, if required, to provide a means of signaling a response-force during a robbery or duress. Arms rooms will be equipped with this type of sensor.

### 6-16. DESCRIPTION OF SYSTEM COMPONENTS

TMs 5-6350-264-14-1 and 5-6350-264-14&P-2 through 5-6350-264-14&P-13 identify the individual components that form a J-SIIDS. TMs 5-6350-280-10 and 5-6350-280-23&P address the AMG. Comparable CIDS components must meet or exceed the criteria in applicable TMs. Listings and applications of other available Government-furnished PSE components and systems can be obtained from the PSEMO, USAREUR.

### 6-17. LOCATION OF IDS COMPONENTS

J-SIIDS will be selected and applied as prescribed in Technical Bulletin (TB) 5-6350-264. ESS must meet or exceed the criteria in TB 5-6350-264 and TM 5-853-4.

a. Sensors should be positioned in protected areas at locations that will provide maximum protection. Enough sensors should be used to ensure the entire area is protected without operating the sensors at maximum sensitivity.

b. The control unit normally will be mounted on the inside wall of the protected facility (excl class-5 weapons containers) as close as possible to the main entrance. Control units may be mounted on the outside of ammunition and explosive storage structures if they are secured inside a locked security container.

c. The monitor cabinet should be positioned to ensure the status displayed is not obstructed from the continual view of monitor personnel. A required location for the monitor station is not specified because IDS locations must be evaluated individually and locations approved by the respective commander.

d. The alarm-latching switch (duress alarm) will be positioned inside the protected area at a location where it is readily available to on-duty personnel and can be operated without being observed by an intruder. The preferred location is on the floor under issue windows. If issue windows are not used, the switch should be located under the armorer's desk or on the floor next to the main entrance doorframe.

e. The audible alarm should be located on the outside of the protected area and mounted as high as possible on the protected structure wall or on utility poles. This will prevent tampering and increase the sound effect. The audible alarm must be accessible to maintenance personnel.

### 6-18. SYSTEM WIRING DIAGRAM

If grid-wire sensors are installed, a system installation wiring diagram and grid-wire dimensional diagram will be made for each protected area. The diagrams will indicate which sensors are installed and show color-coded interconnections between each sensor and the control unit. System options (for example, alarm option, length of time delays, type of monitor to which the module system reports, signal transmission option) should be indicated on the diagram. The diagram will help maintenance personnel when repairs are needed. Wiring diagrams or other instructions developed by the installer for maintenance personnel will be kept inside the control unit. System wiring diagrams and associated site-specific information must be classified at the classification of the level of the area protected. The minimum classification level will be For Official Use Only.

### 6-19. TRANSMISSION LINES AND BACKUP POWER

In USAREUR, line supervision will be provided if undetected access to transmission lines between the control unit and monitor cabinet is possible. Signal transmission line supervision is a technical electronic safeguard to monitor whether an electrical circuit has been broken, grounded, or shorted. If undetected access between the sensors and control unit is possible, wiring will be enclosed in a rigid conduit. Class-B lines, lines that are not supervised, and systems that do not conform to the above will be upgraded. A backup power source or uninterruptable power supply will be provided for each control unit and monitor cabinet and must be capable of lasting at least 4 hours.

### 6-20. INSTALLATION

a. Planning ESS technology applications must include coordination with the local DOIM representative to ensure data transmission have line compatibility and comply with USAREUR Regulation 25-22. Coordination will ensure the dedicated transmission media are available when installation begins.

b. Trained or certified DEH personnel will install IDS and PSE technologies unless installation is to be performed by contract. TMs 5-6350-264-14-1 and 5-6350-264-14&P-2 through 5-6350-264-14&P-13 explain how to install J-SIIDS components.

c. Contractor-installed IDS or PSE technologies will be inspected by trained or certified DEH personnel before the installed system is accepted. Performance criteria required for acceptance of CIDS and commercial security technologies will meet or exceed the criteria in applicable TBs and TMs.

d. A post-completion evaluation (AR 190-13, paras 4-14b and c) may be requested from the IDS MCX to ensure the IDS was properly installed and is being maintained at the appropriate level. This evaluation is required for CIDS and commercial PSE projects. Funding for this evaluation must be programmed through the PM, USAREUR, and will be included in OMA forecasts.

## 6-21. PERSONNEL CHECKS

a. Personnel whose duties will involve designing, operating, or maintaining IDS or PSE and who operate monitoring stations must have a favorable National Agency Check (NAC) or National Agency Check with written inquiry (NACI) or, in the case of local national (LN) personnel, be screened according to USAREUR Regulation 604-1.

b. A security clearance is not required to maintain or install IDSs.

c. Requirements for personnel suitability checks and clearances will be clearly stated in contracts.

d. Commanders may develop command-oriented background-check requirements consistent with HN policy, the local threat situation, sensitivity of the facilities protected, and the vulnerability of the facilities served. Additional commander-developed background check requirements involving foreign national personnel (other than those authorized by USAREUR Reg 604-1) must be coordinated with the Commander in Chief, USAREUR, ATTN: AEAGB-CI(S), Unit 29351, APO AE 09014.

e. United States Army Criminal Investigation Command (USACIDCS) special agents may be available to conduct proper personnel background checks (criminal records verification) on personnel who have access to vulnerable or mission-essential areas. This assistance may be received by written request to the local supporting USACIDC resident agency.

## 6-22. IDS OPERATING PROCEDURES

a. Two people are usually required to operate an IDS; one at the control unit and the other at the monitor cabinet. The monitor-station operator must be a responsible person who can alert a security or response force during an alarm. The control-unit operator should be the person designated to unlock and lock the protected area. The operator will contact the monitor-station operator to verify the protected area is being opened or secured.

b. The three basic modes of IDS operation are—

**(1) Secure.** IDSs are operated in the secure mode when a protected area is secured or is not open to authorized personnel. Alarms (intrusion, tamper, and duress) are processed and routed to the status modules. Alarms, except the duress alarm, are routed to an audible alarm, if used. An exit time-delay is provided to allow authorized personnel to turn the control-unit mode switch to secure and leave the protected area without creating a latched alarm.

**(2) Access.** IDS are operated in the access mode when a protected area is open to authorized personnel. IDSs are set to prevent intrusion alarms from being routed to the status modules and the audible alarm. Tamper and duress alarms are routed to the status modules, but only tamper alarms are routed to an audible alarm. An entrance time-delay is provided to allow authorized personnel to enter the protected area and turn the control-unit mode switch to access without triggering an audible alarm or activating the status module alarm.

**(3) Test/Reset.** The test/reset mode is used when maintenance is being performed on a system. In this mode IDS are set to prevent alarms from being routed to the audible alarm, rather they are routed to status modules. On receiving alarm input, an audible signal in the control unit is activated for 10 seconds as an aid to IDS testing. If the mode switch is placed momentarily in the test/reset position, the audible alarm is reset and silenced. If the mode switch is switched from the test/reset position to the secure position, all processed alarms are cleared if the sensor inputs have ceased to be alarmed.

c. AE Form 190-13J-R (Monitoring Station Emergency Information) and AE Form 190-13K-R (Protected Area Emergency Information) will be affixed or posted as close to each monitor cabinet or control unit as appropriate.

d. The monitor cabinet operator and control-unit operator will use duress procedures. Supervisory personnel will establish duress procedures for use at the monitor-cabinet location. Procedures should be changed at least each quarter or when a security compromise is suspected. Only personnel involved in opening or securing the protected area and monitor personnel should have access to duress procedures.

e. IDS sensors will activate at the monitor station. A duress alarm at the monitor cabinet will be relayed to response forces by the monitor operator using the fastest means available (preferably direct, voice communication). If possible, the monitor station should be located with the response force.

f. Monitor stations will be staffed continuously to ensure there is a quick response to alarms. Monitor personnel will not be assigned any additional duty that diverts their attention from the monitor cabinet.

## USAREUR Reg 190-13

### 6-23. RECORDKEEPING

In USAREUR, DA Form 4930-R (Alarm/Intrusion Detection Record) will—

a. Be used to log daily IDS operations. For computer-driven monitors that provide a printout of system activity, only information not on the printout need be entered on the DA Form 4930-R (for example, weather, patrol dispatch, time to clear).

b. Include at least the following information:

- (1) Time.
- (2) Date.
- (3) Location of alarm.
- (4) Identity of the person receiving the alarm.
- (5) Cause of the alarm.
- (6) Action taken in response to the alarm.

c. Be maintained at the monitor station for 90 days after the last entry.

d. Be sent to the supporting DEH electrical engineer branch after being maintained at the monitor station for 90 days.

### 6-24. MAINTENANCE

Trained or certified DEH personnel will perform maintenance of ESS unless maintenance is performed by contract. TM 5-6350-264-14-1 provides guidance on maintenance of J-SIIDS components. (See USAREUR Reg 420-43.)

a. Unit-level maintenance will be restricted to general cleaning type maintenance (for example, dusting and wiping the exterior portion of IDS components with a dry cloth). IDS components will not be painted.

b. Contractor-installed ESS will be maintained as specified in the Government maintenance contract. The contractor should be required to perform routine maintenance inspections not less than once each year.

c. Organizational personnel will perform periodic preventive maintenance checks and services (PMCS). Conditions requiring repair will be reported to DEH within 2 hours for corrective action. The DEH will make repairs as soon as possible. IDS required by regulation should be repaired within 24 hours to avoid excessive security manpower requirements.

### 6-25. LOGISTICS PROCEDURES

a. BSB DEHs are responsible for maintaining, repairing, and stocking expendable repair parts for IDSs.

b. Supporting maintenance activities will order and stock only those expendable repair parts needed to perform J-SIIDS maintenance and repair.

c. Initial requisitions for new GFE IDS accountable components will be submitted through the servicing installation PBO.

d. GFE IDS users will initiate requests to replace unserviceable GFE IDS equipment sets declared as nonexpendable items (coded "N" in the Army Master Data File (AMDF)). Users will submit requests for supply action and provide applicable fund cites. After receipt, GFE IDS users (requisitioner of the end item) will submit a request to the DEH for quality surveillance (bench-check) and installation of the equipment.

e. If J-SIIDS components fail on initial installation, procedures in AR 702-7-1 will be used, and an SF 368 (Product Quality Deficiency Report) will be submitted by the DEH. Each end-item or repair-part failure is an individual action and must be treated as such. Procedures in AR 710-2, DA Pamphlet 710-2-2, and AR 725-50 will be used by DOLs to requisition replacement parts for faulty components.

f. GFE users will maintain PM, USAREUR, approval documents; requisitioning information (such as complete requisition numbers, date of order, listing of components); and other information necessary to track the procurement process effectively. Requesters will make periodic checks with their servicing DOL to check the status of ordered equipment.

g. IDS component accountability will be maintained according to AR 710-2, DA Pamphlet 710-2-1, and AR 735-5.

### 6-26. RESPONSE TO ALARMS

**a. General.** The ASG commander will set alarm response policy; the BSB commander will implement the policy. The policy, implemented through local physical-security and emergency plans, must include designation of response-force type, size, and armament. Use of MP as the primary or sole force for response to alarms in military communities is discouraged. Procedures will be in place to ensure local MP stations are notified of all alarms and response-force deployments to alarms. Additionally, organizations owning facilities in which an alarm has activated must be notified.

**b. Use of Force.** ASG commanders will establish procedures on the use of force according to AR 190-14 and HN laws.

**c. Duties.** The response force will observe, report, and take action as directed by the response-force commander. The response force must—

(1) Be located so it can respond promptly to an activated alarm. In no case will arrival at the scene exceed 15 minutes from alarm activation.

(2) Go to the protected area and determine the cause of the alarm. A telephone call to the protected area is not an acceptable response when an alarm sounds.

(3) Neutralize an actual alarm condition of any alarm in the protected area (d below).

**d. Response Procedures.** The procedures in (1) through (6) below are recommended when an alarm is received from a protected area. ASG commanders will develop specific procedures to fit the needs of their areas.

(1) When an alarm is announced at the monitor station, the operator will notify the response-force commander and the MP desk sergeant and give the location and time of the alarm.

(2) The response force will be sent to the building where the alarm has been activated.

(3) The response force will block all entrances and exits. One or more members of the response force will be posted at each entrance as they arrive or as instructed by the senior response-force member. No one will be allowed to enter or exit the building.

(4) The senior response-force member will supervise a search of the protected area to determine whether or not an intrusion or attempted intrusion has occurred. If there are no signs of a break-in, the senior response-force member will inform the monitor-station operator and MP desk sergeant, and normal duties will be resumed.

(5) If an intrusion has occurred or was attempted, the senior response-force member will inform the monitor station operator and the MP desk sergeant, and temporarily detain witnesses or suspects until informed of the action to be taken by the response-force OIC or NCOIC. The response-force OIC or NCOIC will secure the area and request MP assistance to summon the appropriate investigative agency (for example, CID, MP). In Germany, affiliated and nonaffiliated civilians (glossary) may be taken into temporary custody until released to local police authorities if one or more of the following occurs:

(a) German authorities request the person be detained.

(b) The person is caught in the act of committing a crime and either the identity of the person cannot immediately be established or there is reason to believe the person may flee.

(6) Notify local law enforcement authorities immediately of any detention. USAREUR ASG PMs outside Germany will consult their servicing staff judge advocate (SJA) for guidance on authority to detain suspects.

## 6-27. INSPECTIONS

Physical-security inspectors will—

a. Conduct an IDS check during security inspections and surveys required by ARs 190-11 and 190-13.

b. Conduct operations-and-functions inspections of IDS during scheduled physical-security surveys and inspections to ensure sensors, signal processors, control units, and monitor cabinets work. Inspectors will use installation manuals, contract statements of service, and modification work orders for this purpose.

c. Visually inspect components and conduits for evidence of tampering.

d. Conduct inspections jointly with security and maintenance personnel.

e. Review copies of inspection reports and maintenance records and perform spotchecks to confirm the accuracy of the reports.

f. Make checks of unit IDS-log entries and records on operation, maintenance, and inspection of IDS.

## 6-28. OPERATIONAL CHECKS

Unit security personnel must make and log periodic system-operations checks. An operations check is an active check of sensors (for example, activation of sensors) and not a remote test. Checks will be conducted quarterly for arms rooms, ammunition storage facilities, and class-1-explosives storage facilities. Checks will be conducted for other protected facilities as follows:

a. Twice a year for bulk AA&E storage facilities with less than 200 protected structures.

b. Once a year for bulk AA&E storage facilities with over 200 protected structures.

c. At least twice a year for high-risk personnel quarters.

## USAREUR Reg 190-13

### 6-29. ACCESS ROSTER

A roster of personnel authorized to open and secure the protected area and to perform maintenance on IDS will be provided as follows:

a. A roster of personnel authorized to open and secure the protected area will be provided to the monitor station. The roster will indicate name, SSN or equivalent HN ID-card number, and telephone number of personnel at the protected area. The commander of the protected area will sign the roster. The roster will be kept where it is readily available to the monitor-station operator and out of sight to unauthorized personnel.

b. The DEH will provide a roster of authorized IDS installation and maintenance personnel to the monitor station and to the commander of the protected area. The ASG security manager will verify the roster. The roster will indicate name, SSN or HN ID-card number, and telephone number of authorized personnel. Only personnel who have had favorable checks according to paragraph 6-21 will be included on the roster. To prevent unauthorized tampering with IDS, only personnel listed on the roster will be permitted to perform maintenance.

### 6-30. KEY CONTROL

DEHs will maintain control and accountability of IDS keys during the initial installation and test phase. On completion of the final test and acceptance of the IDS, control and accountability of IDS keys becomes the responsibility of the unit or activity commander. Keys will be controlled according to AR 190-11, paragraph 3-8, and AR 190-51, appendix D.

### 6-31. SIGNS

Two signs, one in English and the other in the HN language, prominently indicating the presence of the IDS will be posted at facilities protected by IDS. These signs are identified in AR

190-11, appendix F, and the USAREUR Real Property Maintenance Activity Supply Catalog. Signs may be obtained through the servicing DEH.

### 6-32. MOVEMENT OF IDS

a. Installed IDS is installation property and must be accounted for on community property books.

b. Activity and facility closure and organization moves and inactivations may invalidate the need for certain IDSs. Commanders, in coordination with the supporting DEH, will identify inactive IDSs, which may be transferred to other locations. IDS components removed from closing installations will be turned in to the PBO. ASGs may keep removed components, if needed, to backfill outstanding requisitions or to fill ASG DEH maintenance-float densities. Disposition of excess components will be coordinated through the DOL. The PM, USAREUR, and the Deputy Chief of Staff, Logistics (DCSLOG), USAREUR, will be informed of final disposition of removed components.

c. For approval to transfer IDS to a new location, the user will send a request through PM channels to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086, with the following information:

(1) Age of IDS.

(2) Statement from the ASG commander that—

(a) No unit requiring an IDS will occupy the facility from which the IDS is being removed.

(b) The IDS is needed in the new location.

(3) Site survey of new location that shows the IDS will meet needs at the new location.

## CHAPTER 7 USAREUR SECURITY GUARD PROGRAM

### 7-1. PURPOSE

This chapter supplements the requirements of AR 190-56. It assigns responsibilities and prescribes policy, standards, and procedures for using military and civilian guard forces in USAREUR.

### 7-2. APPLICABILITY

This chapter applies to USAREUR assigned and attached units, Civilian Support Group (CSG) guard units, guards hired through CPSCs, and contract guards. Commanders will consider local laws, international agreements, HN agreements, SOFAs, tariff agreements, and contract provisions when implementing the policy and procedures in AR 190-56 and this regulation.

### 7-3. OBJECTIVES

The objective of the USAREUR Security Guard Program is to provide a professional, high quality, and effective security guard force. It provides centralized direction while ensuring the commander retains the responsibility to manage local personnel and assets.

### 7-4. GUARD AUTHORITY

Authority for guards is based on AR 190-56, USAREUR Regulation 600-472, and this regulation.

### 7-5. TYPES OF GUARDS

**a. MP.** MP guards will be used at critical and sensitive facilities and activities as determined by the ASG commander and according to USAREUR directives on force protection. With few exceptions, MPs will be used as guards only when specifically authorized by modification table of organization and equipment (MTOE) or tables of distribution and allowances (TDA).

**b. CSG Guards.** CSG guards are LN employees who work for the U.S. Government. They are authorized on TDAs and are organized and trained as a unit. CSG guards will be used to guard only those facilities that have a regulatory requirement for such guards. The HN has placed restrictions, however, on the type of missions and training CSG guards can perform. Commanders must coordinate with the Commander, USAREUR Civilian Support Agency (CSA), before assigning CSG guards to a mission that might be interpreted as tactical or military.

**c. Contract Guards.** Security services may be contracted through competitive bids. Contracted security services must comply with the USAREUR performance work statement (PWS) and this regulation. The USAREUR PWS will be used as a model for developing contract-guard services in

USAREUR. USAREUR will fund contract guards to meet regulatory requirements when CSG guards are not available.

**d. Borrowed Military Manpower.** For the purpose of security-guard missions, borrowed military manpower (BMM) refers to soldiers used outside of their assigned military occupational specialty (MOS) for specific security duties. This includes short-duration duties that do not technically qualify as BMM by strict definition of the term. BMM will be used when other types of guard forces are not available nor appropriate for a particular security requirement.

**e. CPSC Guards.** Local-hire civilians (DA or LN civilian or family member) may be authorized on a TDA and hired through the local CPSC. Use of CPSC guards in USAREUR is discouraged. The PM, USAREUR, will approve their use as an exception only when no other alternative is practical.

### 7-6. POLICY

Guards are a valuable resource. They may be employed either in an active capacity (access control) or in a passive role (surveillance and detection). Guards are, however, a costly asset and, as such, should be employed only where alternative solutions are not practical or allowable and when the risk to the protected asset warrants such protection. Because of manpower and funding constraints, guards will be provided only to the level essential to meet minimum security standards. Security managers should seek reasonable alternatives, such as technology (for example, ESS), to the long-term employment of guards.

### 7-7. GUARD FORCE STANDARDS

**a. U.S. Hire.** Selection and qualification standards for U.S.-hire guards are in AR 190-56, chapter 2; other applicable civilian personnel directives; and this regulation.

**b. HN Hire.** Selectees for HN hire will meet the qualification and selection standards of USAREUR Regulation 600-410 and USAREUR Regulation 600-474.

**c. Contract (U.S./HN) Hire.** Personnel qualification and selection standards for contract guards are in the USAREUR PWS. The USAREUR PWS will be the model for developing contract guard services in USAREUR.

**d. Medical Reexamination.** Contract guard personnel will take a medical reexamination each year according to the USAREUR PWS. For U.S. and LN employees (hired thru servicing CPSC), the supervisor will recommend a medical reexamination at any time there is reason to believe a medical condition exists that could adversely affect job performance or jeopardize the employee's health while performing assigned duties.

## USAREUR Reg 190-13

**e. Language Proficiency.** Security guards must be able to converse in English and the HN language to a degree that enables them to understand oral and written communications and express themselves in work-related matters.

**f. Appearance.** Security guards will maintain an acceptable standard of individual and duty-area appearance. Security personnel are particularly conspicuous in the performance of their duties and must present a high standard of appearance at all times. Formal inspections will be conducted before security personnel go on duty to ensure the highest standards of appearance are maintained. Informal inspections will be part of daily supervision. The following standards of appearance apply:

(1) The prescribed uniform will be worn while on duty as directed by the supervisor.

(2) Uniforms will be clean and well-pressed. Footwear will be polished. Required insignia will be worn. Unauthorized insignia or accoutrements will not be worn with or on uniform work clothing. Uniform work clothing will not be worn off duty, except for travel to and from place of duty and while on official duty travel.

(3) Shirts, jackets, and coats will be buttoned. Shirts will be tucked into trousers, unless specifically designed to be worn outside the trousers.

(4) When boots above ankle height are worn, trousers will be tucked into the boots.

(5) Equipment (for example, pistolbelts, holsters, arm-band) will be clean. Leather, silver, and brass parts of the uniform will be polished.

(6) Personal hygiene will be maintained.

(7) Hair (incl facial hair) will be well groomed. Hair length or fullness must not interfere with wearing required headgear. Mustaches and beards will be neatly trimmed and must not interfere with the performance of duty. Hair, mustaches, and beards will not be a length that causes a safety hazard.

(8) Hands will not be kept in pockets while performing guard duty. Gloves will be issued and worn during bad weather, as appropriate.

### 7-8. INDIVIDUAL RELIABILITY PROGRAM

a. AR 190-56, chapter 3, provides guidance on the Individual Reliability Program (IRP).

b. The USAREUR IRP, established according to AR 190-56, applies to all civilian security guards. The IRP adds to the employment security-screening requirements of applicable civilian personnel and CSA policies. Civilian guard enrollment in the IRP is a condition of employment and applies to—

(1) Contract guards.

(2) CPSC direct-hire guards (U.S. and LN).

(3) CSG guards.

c. The LN surveillance contract, which is administered by the U.S. Army medical facilities preventive medicine department, will be used to screen and evaluate medical records of LN employees in Germany.

d. Commanders charged with maintaining security, law, and order in the community are responsible for the IRP. Commanders may designate any of the following as IPR-certifying officials:

(1) Local PM.

(2) Security-guard program manager.

(3) ICs.

(4) The contracting officer's representative (COR).

(5) CSG unit supervisor.

### 7-9. DRUG SCREENING

a. AR 190-56, paragraph 2-4, prescribes policy on drug screening of guard personnel.

b. LN security-guard personnel, other than contract guards, are exempt from the Civilian Employee Drug Abuse Testing Program until such testing is approved by applicable USAREUR policy. Commanders may require a contractor to drug-test contract guards if the requirement is specified in the contract and does not violate HN law. Where required, the contract terms will require the contractor to provide evidence that testing has been done.

### 7-10. TRAINING

a. AR 190-56, chapter 4, provides guidance on guard training.

b. All guards, regardless of the source, will be formally trained in their duties before performing security functions.

Military and CPSC guards will be trained by their responsible organizations. CSG and contract guards will be trained as follows:

(1) CSG guards will be trained according to USAREUR Regulation 600-474 and must successfully complete phase I and phase II, Initial Training, before being assigned a weapon. The CSG unit supervisor will ensure guard personnel have AE Form 600-410C in their possession, with the following typed or stamped on the back: "Bearer is authorized to carry a (type of weapon) while on assigned duty." CSG unit supervisors will ensure that annual refresher training is conducted according to USAREUR Regulation 600-474.

(2) Contract guards will be trained by the contractor according to the contract.

c. The items in (1) through (9) below are required training subjects for all security guards. They are in addition to the requirements in AR 190-56 and will be included in guard-post orders, as appropriate (para 7-13):

**(1) Countersurveillance Techniques.** Terrorist and other sophisticated criminal elements usually conduct extensive reconnaissance and surveillance before executing an action. Guards must be alert to unusual persons watching protected assets and areas, and should immediately report suspicious activities to supervisors. The ASG or BSB will review countersurveillance instructions and training for adequacy.

**(2) Duress Procedures.** Each guard will be trained on duress procedures and situations that might require those procedures.

**(3) First Aid.** Security guards will receive a minimum level of instruction in first-aid and basic life-saving techniques. Qualified medical personnel should conduct the training.

**(4) Guardpost Orders.** Security guards will be trained in each aspect of their assigned duties. Other aspects of a guard's functions, such as access-control procedures for gate-guards or building-security checks for roving security guards, must be included in the guard-training program.

**(5) IPR.** Security guards will be trained on the IPR according to paragraph 7-8 and AR 190-56.

**(6) Personnel, Vehicle, and Material Control.** Security guards will be trained to conduct proper searches of vehicles, personnel, and material when assigned duties requiring such action. Local PM and SJA personnel should help present this instruction.

**(7) Physical Training.** Supervisors will ensure security guards maintain an acceptable level of physical fitness so they can perform their assigned duties. Contract guards will meet requirements of the USAREUR PWS. CSG guards will comply with requirements of USAREUR Regulation 600-474. CPSC guards will meet job description performance standards.

**(8) Weapons Qualification.** Security guards will qualify with their assigned weapons before they are assigned to security duty and at least once a year after that. The USAREUR security-guard PWS or applicable regulations will establish qualification standards. CSG guards will comply with weapons training requirements in USAREUR Regulation 600-474.

**(9) Use of Force.** The decision to arm guards will be governed by the applicable physical-security standards established for the asset being guarded. Use of force will be in strict compliance with AR 190-14, USAREUR Regulation 600-472, and the USAREUR PWS, as applicable. Policy on use of force will be coordinated with the supporting office of the SJA before being implemented. Security guards will use force only when they cannot conduct their duties without it. When use of force is necessary, only the minimum amount needed to resolve the situation is justified. Guards should attempt, through verbal persuasion, to resolve conflicts. If necessary, physical detention using unarmed defense techniques should be used when possible. Guards should request assistance from supervisory personnel when a situation appears to be escalating toward use of force, if time allows. Deadly force is seldom warranted and will be used only under conditions of extreme necessity (that is, when all lesser means of action have failed or cannot reasonably be used).

## 7-11. UNIFORM AND EQUIPMENT

a. AR 190-56, chapter 6, provides appropriate guidance on guard uniforms and equipment.

b. Commanders and supervisors will ensure security guards under their control are adequately clothed and equipped to perform assigned duties. Based on the nature of the position and responsibilities of security guards, specific equipment may be required for duty. Individual and supplemental equipment considerations include inclement weather and unusual terrain.

(1) Individual equipment includes at least the prescribed uniform (seasonal and climatic), the individual's weapon (when authorized), and other individual supplies needed to perform security-guard duties.

(2) Supplemental equipment includes vehicles, communication equipment, and other accountable property required to perform security-guard duties.

## USAREUR Reg 190-13

(3) Equipment for CSG guard units and personnel is authorized by the TDA; Common Table of Allowances (CTA) 50-900, CTA 50-909, and USAREUR Regulation 600-440.

(4) Uniform and equipment requirements will be included in guard-service contracts.

### 7-12. ESTABLISHING AND FILLING REQUIREMENTS

a. The security manager for the facility or activity being protected will identify guard requirements in accordance with the supporting BSB PM. Essentially, guard requirements are generated in one of two ways: first, guards are required by law or regulation; second, the commander, based on risk analysis, determines a valid and prudent need exists.

b. There is no standard for determining the number of guard positions needed to secure a given asset. Local operational considerations, vulnerability of the asset, and required duties will be considered when determining an acceptable minimum number of required guards. AR 570-5 explains how to develop manpower standards.

c. After establishing valid guard requirements (b above), staffing will be done as follows:

(1) Use of BMM and MP will be approved by the ASG commander.

(2) Requests for civilian guards (CSG, contract, and CPSC), will be sent through the Office of the Provost Marshal (OPM), HQ USAREUR/7A, for endorsement before submission to the Office of the Deputy Chief of Staff, Resource Management (ODCSRM), HQ USAREUR/7A, for a final decision on funding.

d. Paragraph 7-5 will be used to determine the type of guards to meet requirements.

e. CSG and CPSC guards must be placed on the organization's manpower authorization documents. A current physical-security survey will be made available on request to ODCSRM when that organization conducts organizational surveys or functional-area assessments of authorized guard positions.

f. After guard positions in an organization have been validated and funded, ASG commanders may require short-term guard use beyond the validated level, based on an increased THREATCON or local operational necessity. A need for more guards than validated must be met by the ASG commander, normally with support of tenant units. Augmentation beyond the capability of the ASG and tenant units will be requested from the Office of the Deputy Chief of

Staff, Operations (ODCSOPS), HQ USAREUR/7A. When long-term operational requirements indicate the need for an increase of validated guard requirements, the process in b through e above will be repeated.

### 7-13. GUARD ORDERS

a. AR 190-56, paragraph 5-3, provides guidance on guard orders.

b. Each guardpost will have clear instructions in both English and the HN language that describe the scope of the post, functions to be performed, and parameters within which each guard will operate. Guardpost orders will address each aspect of the guard's duties. Orders will include at least the following information:

**(1) Area of Responsibility.** The specific area for which the guard is responsible. Use of a detailed sketch will help clarify the limits of the post.

**(2) Use of Force.** Commanders responsible for preparing guard orders will include instructions on the use of force (incl deadly force). Instructions will comply with applicable HN laws, AR 190-14, and USAREUR Regulation 600-472, as appropriate. The supporting SJA will review the instructions. Use-of-force instructions will include at least the following:

(a) The conditions justifying use of force and the appropriate level of force warranted for those conditions.

(b) The specific conditions warranting use of deadly force. Conditions should include the protection of specific items (weapons and ammunition) that, if taken, could cause deadly harm to others in the hands of unauthorized individuals.

(c) The legal protection provided to a guard who, in the most prudent application of assigned duties, uses deadly force to comply with guard orders.

**(3) Equipment.** A list of required equipment that includes items for operation in bad weather and darkness (para 7-11b). Responsibility for the use, maintenance, and accountability of property and individual items of equipment will be clearly explained.

**(4) Supervisory Control.** The supervisory chain will be defined. Conditions when a guard may be required to comply with instructions from personnel outside of their supervisory chain also will be clearly explained.

**(5) Duress Instructions.** Clear duress procedures will be prescribed for each guardpost.

**(6) Reports and Forms.** Clear instructions for using reports and forms, when such are required, will be provided; samples will be provided to each post.

**(7) Special Instructions.** Unique situations and requirements of a specific post will be clearly detailed in the guard-post orders.

#### 7-14. EVALUATIONS

Regular and routine evaluations of security-guard operations are essential to ensuring compliance with this regulation, local policy, and guardpost orders. Guard-program managers should coordinate local programs to ensure at least the following personnel conduct evaluations:

**a. Guard Supervisors.** Supervisors will evaluate security guards before posting them to ensure they are fit and prepared for duty. Supervisors will also evaluate each guard-post at least once during the scheduled shift to ensure security guards know guard policies and guardpost orders.

**b. The COR.** The COR will conduct daily evaluations of security guard performance to ensure compliance with a contract, and to protect the interests of the command. The COR will document discrepancies as specified in the contract

statement of work. Appendix F provides checklists for quickly checking compliance with physical-security requirements. Commanders should consider assigning an individual to COR duties as a full-time position.

**c. The S2/S3/DPTMS.** The proponent for security operations will regularly inspect security-guard operations as part of the organizational evaluation program to ensure compliance with this regulation, command policy, and specified guardpost orders.

**d. The PM.** As the proponent for physical security and law enforcement, the PM will advise the DPTMS on security-guard policy (incl the adequacy of guardpost orders). The PM will assist the DPTMS with military patrol operations. The PM will report noted problems and discrepancies when detected. Security-guard supervisors will be contacted when security-guard operations requiring corrective action are detected. On-the-spot corrections will be made when the situation is such that direct and immediate action is necessary to preserve law and order or to protect lives or property.

**e. Higher Headquarters.** A higher command may also be required to evaluate security-guard operations. When such evaluations are directed, the security-guard program manager will be the POC for coordinating the evaluation.

**APPENDIX A  
REFERENCES**

**A-1. DEPARTMENT OF DEFENSE MANUALS**

DOD 4525.6-M (volumes 1 and 2), DOD Postal Supply

DOD 5100.76-M, Physical Security of Sensitive Conventional Arms Ammunition and Equipment

**A-2. ARMY REGULATIONS**

AR 25-400-2, The Modern Army Recordkeeping System (MARKS)

AR 37-100-series, The Army Management Structure (AMS)

AR 37-103, Disbursing Operations for Finance and Accounting Offices

AR 55-355, Defense Traffic Management Regulation

AR 60-10, Army and Air Force Exchange Service General Policies

AR 190-11, Physical Security of Arms, Ammunition and Explosives

AR 190-13, The Army Physical Security Program

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

AR 190-16, Physical Security

AR 190-22, Searches, Seizures, and Disposition of Property

AR 190-40, Serious Incident Report

AR 190-51, Security of Army Property at Unit/Installation Level

AR 190-56, The Army Civilian Police and Security Guard Program

AR 195-5, Evidence Procedures

AR 210-7, Commercial Solicitation on Army Installations

AR 380-5, Department of the Army Information Security Program

AR 380-19, Information Systems Security

AR 380-67 and USAREUR Supplement 1, Personnel Security Program

AR 381-12, Supervision and Espionage Directed Against the U.S. Army (SAEDA)

AR 420-70, Buildings and Structures

AR 525-13, The Army Combatting Terrorism Program

AR 570-5, Manpower Staffing Standards System (MS3)

AR 600-8-14, Identification Cards, Tags, and Badges

AR 600-20, Army Command Policy

AR 702-7-1, Reporting of Product Quality Deficiencies Within the U.S. Army

AR 710-2, Inventory Management Supply Policy Below the Wholesale Level

AR 725-50, Requisition and Issue of Supplies and Equipment, Requisitioning, Receipt, and Issue System

AR 735-5, Policies and Procedures for Property Accountability

**A-3. DEPARTMENT OF THE ARMY PAMPHLETS**

DA Pamphlet 190-51, Risk Analysis for Army Property

DA Pamphlet 350-38, Standards in Weapons Training

DA Pamphlet 710-2-1, Using Unit Supply System (Manual Procedures)

DA Pamphlet 710-2-2, Supply Support Activity Supply Support System Manual Procedures

**A-4. FIELD MANUALS**

FM 5-250, Explosive and Demolitions

FM 19-30, Physical Security

FM 22-6, Guard Duty

FM 90-14, Rear Battle

**A-5. TECHNICAL BULLETINS**

TB 5-6350-264, Selection and Application of Joint-Services Interior Intrusion Detection System (J-SIIDS)

## **USAREUR Reg 190-13**

### **A-6. TECHNICAL MANUALS**

TM 5-853-4, Security Engineering Electronic Security Detection Systems

TM 5-6350-264-14-1, Operation, Organizational, Direct Support and General Support Maintenance Manual, Installation, Operation, and Checkout Procedures for Joint-Services Interior Intrusion Detection System (J-SIIDS)

TM 5-6350-264-14&P-2, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Transceiver, Ultrasonic Motion Signal, RT-1161/FSS-9(V) (NSN 6350-00-228-2566) and Processor, Ultrasonic Motion Signal, MX-9444/FSS-9(V)(6350-00-228-2581)

TM 5-6350-264-14&P-3, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Receiver, Passive Signal Ultrasonic, R-1860/FSS-9(V) (NSN 6350-00-228-2534) and Processor, Passive Signal Ultrasonic, MX-9943/FSS-9(V)(6350-00-228-2548)

TM 5-6350-264-14&P-4, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Detector, Vibration Signal, DT-546/FSS-9(V) (NSN 6350-00-228-2521) and Processor, Vibration Signal, MX-9443/FSS-9(V) (6350-00-228-2524)

TM 5-6350-264-14&P-5, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Switch, Balanced Magnetic, SA-1955/FSS-9(V) (NSN 6350-00-228-2500)

TM 5-6350-264-14&P-6, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Sensor, Grid Wire, DT-545/FSS-9(V) (NSN 6350-00-228-2504)

TM 5-6350-264-14&P-7, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Sensor, Capacitance Proximity, DT-548/FSS-9(V) (NSN 6350-00-228-2606)

TM 5-6350-264-14&P-8, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Switch, Alarm Latching, SA-1954/FSS-9(V) (NSN 6350-00-228-2510)

TM 5-6350-264-14&P-9, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Alarm, Audible, BZ-204/FSS-9(V) (NSN 6350-00-228-2514)

TM 5-6350-264-14&P-10, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Control Unit, Alarm Set, C-9412/FSS-9(V) (NSN 6350-00-228-2735)

TM 5-6350-264-14&P-11, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Cabinet, Monitor, Type A, CY-7359/FSS-9(V) (NSN 6350-00-228-2690); Type B, CY-7360/FSS-9(V) (6350-00-228-2697); and Type C, CY-7361/FSS-9(V) (6350-00-228-2705); and Monitor Module, Status, ID-1921/FSS-9(V) (6350-00-228-2661)

TM 5-6350-264-14&P-12, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Receiver, Data, R-1861/FSS-9(V) (NSN 6350-00-228-2655) and Transmitter, Data, T-1257/FSS-9(V) (6350-00-251-5749)

TM 5-6350-264-14&P-13, Operator's, Organizational, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for Sensor, Magnetic Weapon, DT-547/FSS-9(V) (NSN 6350-00-228-2590)

TM 5-6350-280-10, Operator's Manual for the Alarm-Monitor Group (AMG)

TM 5-6350-280-23&P, Units and Direct Support Maintenance Including Repair Parts and Special Tools List for Alarm-Monitor Group (AMG) OA-9431/FSS-9(R) CAGEC 97403

### **A-7. COMMON TABLES OF ALLOWANCES**

CTA 50-900, Clothing and Equipment

CTA 50-909, Field and Garrison Furnishings and Equipment

### **A-8. USAREUR REGULATIONS**

USAREUR Regulation 1-201, USAREUR Organizational Inspection Program

USAREUR Regulation 10-5, HQ USAREUR/7A Responsibilities and Functions

USAREUR Regulation 25-22, Policy and Procedures for Obtaining and Using Telecommunications Services and Systems in Europe

USAREUR Regulation 55-4, Joint Transportation of Hazardous Material

USAREUR Regulation 55-355, Joint Transportation and Traffic Management Regulation—Central Europe

USAREUR Regulation 190-6, Registration and Control of Privately Owned Firearms and Other Weapons in Germany

USAREUR Regulation 210-60, Establishment of Exterior Protective or Safety Zones (*Schutzbereich*), Germany

USAREUR Regulation 210-70, Personal Commercial Affairs

USAREUR Regulation 340-21, The Army Privacy Program in USAREUR

USAREUR Regulation 415-22, NATO Infrastructure Program

USAREUR Regulation 420-43, Electrical Services

USAREUR Regulation 600-410, Civilian Support Administration—Instatement and Transfer of Personnel

USAREUR Regulation 600-440, Civilian Support Logistics

USAREUR Regulation 600-472, Labor Service—Police Authority, Possession, Carrying, and Use of Weapons for Personnel Assigned Guard Duties

USAREUR Regulation 600-474, Civilian Support— Training and Inspection Procedures

USAREUR Regulation 600-700, Identification Cards and Individual Logistic Support

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

USAREUR Regulation 740-5, Prestock Points and Forward Storage Sites

#### **A-9. USAREUR PAMPHLETS**

USAREUR Pamphlet 405-45, USAREUR Installations

USAREUR Pamphlet 715-3, Manual for Contracting Officer's Representatives

#### **A-10. MISCELLANEOUS**

CINCUSAREUR Operation Order on Force Protection

USAREUR Performance of Work Statement for Contract Guard Services

USAREUR Abrams Tank System Security Guide

Director of Central Intelligence Agency Directive 1/21, 29 July 1995, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)

U.S. Army Corps of Engineers (Huntsville Division), Site Survey Procedures Guide for Intrusion Detection Systems (HNDS-88217-ED-ME, Oct 88)

Criminal Investigation Division Regulation 195-1, CID Operations

Defense Intelligence Agency Manual 50-3, Physical Security Requirements for Selective Compartmented Information Facilities

SOP for Community Commanders-Installation Commanders of U.S. Forces Accommodations in Germany, subject: Procedures for Entry Onto U.S. Forces Accommodations by German Police and Cooperation With the U.S. Forces in Cases of Major Disturbances, 8 November 1989

#### **A-11. FORMS**

##### **a. Standard Forms**

SF 368, Product Quality Deficiency Report

SF 702, Security Container Check Sheet

##### **b. DD Forms**

DD Form 2(RET), United States Uniformed Services Identification Card (Retired)

DD Form 2A(ACT) (Army), Active Duty Military ID Card

DD Form 2A(RES), Armed Forces of the United States Identification Card (Reserve)

DD Form 2AF(ACT) (Air Force), Active Duty Military ID Card

DD Form 2MC(ACT) (Marine Corps), Active Duty Military ID Card

## **USAREUR Reg 190-13**

DD Form 2N(ACT) (Navy), Active Duty Military ID Card

DD Form 448, Military Interdepartmental Purchase Request (MIPR)

DD Form 1172, Application for Uniformed Services Identification Card and DEERS Enrollment

DD Form 1173, Uniformed Services Identification and Privilege Card

DD Form 1348-6, DOD Single Line Item Release/Receipt Document

DD Form 1391, FY##, Military Construction Project Data

DD Form 1610, Request and Authorization for TDY Travel of DOD Personnel

### **c. DA Forms**

DA Form 410, Receipt for Accountable Form

DA Form 1602, Civilian Identification

DA Form 1818, Individual Property Pass

DA Form 2062, Hand Receipt/Annex Number

DA Form 2765-1, Request for Issue or Turn-In

DA Form 2806-R, Physical Security Survey Report

DA Form 2806-1-R, Physical Security Inspection Report

DA Form 3056, Report of Missing/Recovered Firearms, Ammunition, and Explosives

DA Form 3749, Equipment Receipt

DA Form 4604-R, Security Construction Statement

DA Form 4137, Evidence/Property Custody Document

DA Form 4261, Physical Security Inspector Identification Card

DA Form 4261-1, Physical Security Inspector Identification Card

DA Form 4283, Facilities Engineering Work Request

DA Form 4569, USAPC Requisition Code Sheet

DA Form 4930-R, Alarm/Intrusion Detection Record

DA Form 5431, Army Guard/Reserve Family Member Identification Card

DA Form 5513-R, Key Control Register and Inventory

DA Form 7281-R, Command Oriented Arms, Ammunition, & Explosives Security Screening and Evaluation Record

### **d. AE Forms**

AE Form 190-6B, Privately Owned Firearm Registration

AE Form 190-13A, Permanent U.S. Army, Europe, Installation Pass

AE Form 190-13B, Application for Permanent U.S. Army, Europe, Installation Pass

AE Form 190-13C, Temporary U.S. Army, Europe, Installation Pass

AE Form 190-13D, Receipt for Confiscated ID Card

AE Form 190-13E, Security Badge (Red)

AE Form 190-13F, Security Badge (Green)

AE Form 190-13G, Security Badge (Black)

AE Form 190-13H(G)-R and 190-13H(I)-R, Personnel/Vehicle Record of Admission

AE Form 190-13I, Issue of Weapons and Ammunition

AE Form 190-13J-R, Monitoring Station Emergency Information

AE Form 190-13K-R, Protected Area Emergency Information

AE Form 190-13L-R, Request for Waiver or Exception of Physical Security Requirements

AE Form 210-70E, USAREUR/USAFE Commercial Solicitation Permit

AE Form 600-410C, USAREUR Civilian Support Identification Card

AE Form 600-700A, USAREUR Privilege and Identification Card

AE Form 600-700C-R, Accountability Register for Privilege and Identification Cards

AE Form 604-1A, Personnel Data Request

**APPENDIX B  
RESPONSIBILITIES**

**B-1. PURPOSE**

a. This appendix consolidates responsibilities for—

- (1) Installation access.
- (2) Physical security of arms, ammunition, and explosives (AA&E).
- (3) Intrusion detection systems (IDSs).
- (4) Physical security of U.S. Army property.
- (5) USAREUR Security Guard Program.

b. This appendix also provides responsibilities in the various security-related DA regulations when inclusion is necessary for clarification. Because a totally inclusive listing would be impractical, responsible parties must familiarize themselves and comply with responsibilities in applicable ARs, USAREUR regulations, and chapters of this regulation.

**B-2. PROVOST MARSHAL, USAREUR**

The Provost Marshal (PM), USAREUR, will—

- a. Be the USAREUR command physical-security officer (AR 190-13).
- b. Establish, implement, and manage the USAREUR Physical Security Program (incl developing budgets, policies, procedures, and standards).
- c. Determine commandwide security needs and advise commanders on deficiencies that threaten high-value or sensitive Government property.
- d. Review waivers and exceptions to DA physical-security requirements and forward them to the approving authority at HQDA.
- e. Review and approve or disapprove waivers and exceptions to USAREUR requirements.
- f. Manage the Command Security Upgrade Program (CSUP).
- g. Monitor security in the command.
- h. Review DA Forms 2806 (Physical Security Survey Report) and commander reports of corrective action.

i. In coordination with the United States Army Contracting Command, Europe (USACCE), ensure adequate performance work statements (PWSs) are established so that security-related contracts clearly define the limits of authority, jurisdiction, and use of force; and that they support the specific requirements and conditions necessary.

j. In coordination with the Deputy Chief of Staff, Engineer (DCSENGR), USAREUR, coordinate involvement of the U.S. Army Corps of Engineers, Huntsville Division IDS Center of Technical Expertise (IDS MCX), to participate in required surveys.

k. Provide an annual forecast of USAREUR IDS requirements to the United States Army Aviation and Troop Command (ATCOM) and establish priorities for installing IDS in USAREUR.

l. Coordinate technical reviews of proposed commercial intrusion detection systems (CIDSS) and commercial closed-circuit television (CCTV) projects with the Product Manager, Physical Security Equipment Branch, Belvoir Research and Development Engineering Center, Fort Belvoir, Virginia. Technical reviews of CIDSS also will be coordinated with the DCSENGR. CIDSS funding and initial issue of Government-furnished equipment (GFE) IDS will be coordinated with ATCOM.

m. Manage the USAREUR guard force.

n. Program Operation and Maintenance, Army (OMA), and Other Procurement, Army (OPA), funds to support identified requirements.

o. Provide funding for installation of IDS through the Deputy Chief of Staff, Resource Management (DCSRM), USAREUR.

**B-3. DEPUTY CHIEF OF STAFF, PERSONNEL, USAREUR**

The Deputy Chief of Staff, Personnel (DCSPER), USAREUR, will—

- a. Ensure physical-security personnel (additional skill identifier H3) are available and evenly distributed.
- b. Be the principle point of contact (POC) for all civilian personnel management policy matters affecting civilian guards.
- c. Ensure policies and procedures relating to civilian guards are coordinated as necessary with appropriate works councils and are in accordance with host nation (HN) requirements.

## **USAREUR Reg 190-13**

d. Maintain a list of persons barred from USAREUR installations.

### **B-4. DEPUTY CHIEF OF STAFF, INTELLIGENCE, USAREUR**

The Deputy Chief of Staff, Intelligence (DCSINT), USAREUR, will—

a. Develop and publish USAREUR threat information and updates.

b. Help area support group (ASG) and major subordinate command (MSC) (glossary) commanders develop local threat assessments.

c. In coordination with the PM, USAREUR, and the United States Army Materiel Command, Europe (USAMC-E), develop security policy and procedures for classified materials and equipment, as well as for new classified equipment fielded in USAREUR.

d. Ensure that personnel-security policies and procedures support the USAREUR Security Guard Program.

### **B-5. DEPUTY CHIEF OF STAFF, OPERATIONS, USAREUR**

The Deputy Chief of Staff, Operations (DCSOPS), USAREUR, will—

a. Develop and distribute force-protection policy and implementing instructions according to AR 525-13.

b. Provide the PM, USAREUR, and other appropriate staff agencies with information on new ammunition or equipment items scheduled for fielding in USAREUR so that security standards can be determined.

### **B-6. DEPUTY CHIEF OF STAFF, LOGISTICS, USAREUR**

The Deputy Chief of Staff, Logistics (DCSLOG), USAREUR, will—

a. Develop procedures that allow for inventory and accountability of all types of high-value and sensitive property.

b. Project future requirements for arms and ammunition storage and other logistics storage, and coordinate with the PM, USAREUR, to ensure there are no security shortfalls.

c. Control requisition, storage, and accountability of GFE nonexpendable IDS components and replacement parts.

### **B-7. DEPUTY CHIEF OF STAFF, ENGINEER, USAREUR**

The DCSENGR will—

a. Ensure construction planning takes security requirements into consideration.

b. Ensure that construction of new or modified AA&E storage facilities meet minimum structural standards in appropriate regulations.

c. Distribute OMA funds for proposed IDS installation, design, or survey according to the Office of the Provost Marshal (OPM), HQ USAREUR/7A, distribution plan.

d. Ensure new construction designs and modifications are reviewed by the appropriate PM before a contract is awarded. The local PM will ensure that security requirements are met.

e. Establish policy and procedure for designing, installing, maintaining, and repairing IDS and for training and certifying the personnel responsible for those tasks.

f. Provide the PM, USAREUR, a 7-year forecast of IDS requirements for Military Construction, Army (MCA), and NATO construction projects once a year.

g. Coordinate support from the U.S. Army Corps of Engineers, European Division, for USAREUR command security survey requirements.

h. Ensure correct sign translations (provided by the PM, USAREUR) are used and are included in the USAREUR Real Property Maintenance Activity Supply Catalog.

i. Provide technical and staff assistance on physical-security equipment-related issues.

### **B-8. DEPUTY CHIEF OF STAFF, INFORMATION MANAGEMENT, USAREUR**

The Deputy Chief of Staff, Information Management, USAREUR, will establish policy and procedures to ensure dedicated telephone lines are available to support IDS requirements.

### **B-9. DEPUTY CHIEF OF STAFF, RESOURCE MANAGEMENT, USAREUR**

The DCSRMM will distribute OMA funds to support IDS and physical-security equipment (PSE) requirements.

### **B-10. INSPECTOR GENERAL, USAREUR**

The Inspector General (IG), USAREUR, will include a physical-security inspector when conducting inspections.

**B-11. JUDGE ADVOCATE, USAREUR**

The Judge Advocate (JA), USAREUR, will provide legal assistance to commanders on—

- a. USAREUR restricted areas.
- b. HN laws that apply to the enforcement of restricted areas.

**B-12. MSC COMMANDER**

MSC commanders will—

- a. Establish close coordination with ASGs that have MSC units as tenants to ensure that the subordinate units are included in physical-security plans.
- b. Provide necessary assets to support ASG and base support battalion (BSB) guard requirements.
- c. Designate mission-essential or vulnerable areas (MEVAs) in writing and provide copies to supporting ASG and BSB commanders.

**B-13. MSC PROVOST MARSHAL**

MSC PMs will ensure every—

- a. Identified MEVA receives required physical-security inspections.
- b. Engineer projects and work orders are reviewed for compliance with physical-security criteria.
- c. Waivers and exceptions are forwarded through the supporting ASG and BSB to the PM, USAREUR.

**B-14. ASG AND BSB COMMANDERS**

ASG and BSB commanders will—

- a. Maintain the minimum guard- and response-force level and composition necessary to secure installations, activities, property, and personnel at each threat condition (THREATCON) level.
- b. Prioritize and maintain a current MEVA list.
- c. Establish a security guard management program and designate a program manager.
- d. Ensure security-screening requirements for guard personnel are met, according to USAREUR Regulation 600-410 and USAREUR Regulation 604-1.
- e. In coordination with supporting military intelligence and criminal investigation division assets, develop and distribute ASG threat statements.

f. Ensure physical-security requirements are identified in MCA, minor construction projects, and nonappropriated fund (NAF) construction projects.

g. Institute a system to ensure security deficiencies noted during inspections, surveys, and readiness tests are programmed for correction and that adequate compensatory measures are in place.

**B-15. ASG AND BSB PROVOST MARSHAL**

ASG and BSB PMs will—

- a. Manage physical-security programs and resources.
- b. Review, evaluate, and forward requests for security waivers and exceptions to the PM, USAREUR.
- c. Conduct risk analyses of MEVAs.
- d. Ensure MEVAs receive required physical-security inspections.
- e. Monitor requirements for security guards. PMs will maintain a database that includes at least the following information:
  - (1) Manyear requirements.
  - (2) Number of guards.
  - (3) Types of guards.
  - (4) Purpose of guards.
  - (5) Location of guards.

f. Review engineer project designs and work orders to ensure they comply with physical-security criteria.

g. Manage IDSs in conjunction with directorates of engineering and housing (DEHs).

h. Ensure physical-security inspectors use the Security Management System (SMS).

i. Develop 7-year forecasts of IDS requirements and submit them to the PM, USAREUR, each year.

**B-16. ASG AND BSB DIRECTORS OF ENGINEERING AND HOUSING**

ASG and BSB DEHs will—

- a. Ensure every construction project plan includes physical-security requirements.

## USAREUR Reg 190-13

b. Establish policy and procedure for designing, installing, maintaining, and repairing IDS and for training and certifying the persons responsible for those tasks.

c. Comply with USAREUR Regulation 420-43

### **B-17. ASG AND BSB DIRECTORS OF INFORMATION MANAGEMENT**

ASG and BSB directors of information management will establish policy and procedure to ensure enough dedicated telephone transmission lines are available to support identified ASG requirements.

### **B-18. ASG AND BSB DIRECTORS OF LOGISTICS**

ASG and BSB directors of logistics (DOLs) will—

a. Establish a program to control requisition of GFE IDS nonexpendable component and replacement parts from USAREUR supply activities.

b. Notify ASG DEHs and receiving-units when GFE IDS components arrive from supply sources.

### **B-19. UNIT COMMANDERS**

Unit commanders will—

a. Identify IDS requirements.

b. Ensure IDSs are checked according to this regulation, chapter 6.

c. Ensure personnel operating IDSs are reliable and trained in operating procedures.

d. Ensure only maintenance personnel listed on the access roster provided by the DEH are authorized access to the IDS.

e. Ensure DA Form 4930-R (Alarm/Intrusion Detection Record) is maintained at the monitor station for 90 days. After 90 days, the DA Form 4930-R must be turned in to the supporting electrical engineer branch to have recurring problems monitored.

f. Ensure IDS components and keys are controlled and accounted for according to AR 190-13 and this regulation.

g. Provide response forces as required by the ASG and BSB.

h. Report nonoperational systems to the PM and DEH immediately. When the system becomes operational, the PM will be advised immediately.

i. Ensure that IDSs are monitored 24 hours a day, 7 days a week. User-units and activities with IDSs that are not being monitored will have compensatory measures to protect the facility according to applicable regulations.

### **B-20. COMMANDER, 5TH CRIMINAL INVESTIGATION DIVISION DETACHMENT**

The Commander, 5th Criminal Investigation Division Detachment, will provide OPM with copies of every investigation report involving a high-value or sensitive item.

### **B-21. COMMANDER, USAREUR CIVILIAN SUPPORT AGENCY**

The Commander, USAREUR Civilian Support Agency, will—

a. Establish policy and procedures for selecting, training, and managing Civilian Support Group (CSG) guard personnel.

b. Monitor CSG guard units to ensure initial, annual, refresher (conducted by the CSG units), and advanced training are conducted as prescribed.

### **B-22. COMMANDER, USAMC-E**

The Commander, USAMC-E, will coordinate with—

a. Supporting ASG and BSB PMs to ensure that required physical-security surveys and inspections are conducted.

b. OPM on new weapon fielding sites.

**APPENDIX C  
MINIMUM SECURITY STANDARDS**

**C-1. PURPOSE**

This appendix identifies the security requirements for various categories of Army assets.

**C-2. GENERAL**

a. Tables C-1 and C-2 list minimum security standards (requirements) for selected categories of Army property. This information has been taken from applicable regulations. USAREUR-specific requirements are also established and identified in the tables. DA requirements are in abbreviated form; users must refer to the references for a full explanation.

b. Paragraph C-3 identifies the various categories of property. A detailed list of required security measures by category is provided in tables C-1 and C-2, which, in addition to listing the requirements, identify the source of the requirement.

c. Some categories of assets are protected based on the level of risk, while others (such as arms, ammunition, and explosives (AA&E)) are protected at an absolute standard (regardless of risk). Determining appropriate risk levels requires performing a risk analysis according to DA Pamphlet 190-51. Local plans must take the existing threat condition (THREATCON) into account when determining the risk level at which protection will be provided.

d. The glossary explains abbreviations used in the tables.

**C-3. RISK LEVELS AND CATEGORIES**

**a. Risk Levels.** Risk levels are classified as either I, II, or III. Risk level III requirements are the most stringent. The following are categories of assets that are protected, based on analyses of existing levels of risk:

- (1) Aircraft (components and aviation facilities) (table C-1, sec I).
- (2) Unarmed vehicles (table C-1, sec II).
- (3) Armed vehicles and towed-weapons systems and components (table C-1, sec III).
- (4) M-1 series (Abrams) tanks (table C-1, sec IV).
- (5) Communications and electronics equipment and night vision devices (table C-1, sec V).
- (6) Headquarters (brigade and above) (table C-1, sec VI).

**b. Categories.** AA&E standards are based on AA&E categories established in AR 190-11. The following are categories of assets that are protected, based on an absolute standard that does not vary based on risk.

- (1) AA&E unit arms rooms (table C-2, sec I).
- (2) AA&E in bulk storage (table C-2, sec II).
- (3) AA&E in transit (table C-2, secs III and IV).

<b>Table C-1 Analysis-Based Protection</b>	
<b>SECTION I—AIRCRAFT (COMPONENTS &amp; AVIATION FACILITIES)</b>	
<b>a. Risk Level I</b>	
1. Lock aircraft ignition and doors.	AR 190-51, para 3-3e
2. Control ignition and door keys.	AR 190-51, para 3-3e
3. Park in most secure hanger or structure available; otherwise, park aircraft next to each other and away from perimeter.	AR 190-51, para 3-3e
4. Have a written security plan.	AR 190-51, para 3-3f
5. Appoint a physical-security officer.	AR 190-51, para 3-3f
6. Conduct security check every 4 hours.	AR 190-51, para 3-3f
7. Control access at all times.	AR 190-51, para 3-3f
8. Designate airfield as "restricted area."	AR 190-51, para 3-3f
9. Prohibit POV parking.	AR 190-51, para 3-3f
10. Secure accessory equipment (such as boarding ladders, vehicle tugs).	AR 190-51, para 3-3f
11. Coordinate closely with local HN authorities.	USAREUR Reg 190-13
12. Have communications with response- and police-forces.	USAREUR Reg 190-13
13. Have an active countersurveillance program.	USAREUR Reg 190-13
<b>(Aircraft With AA&amp;E Aboard)</b>	
14. Park in lighted area.	AR 190-51, para 3-3b

<b>Table C-1</b>	
<b>Analysis-Based Protection</b>	
15. Use IDS or continuous surveillance.	AR 190-51, para 3-3b
16. When possible, remove weapons to secure storage area or make inoperable.	AR 190-51, para 3-3b
<b>(Aircraft With Missiles/Rockets in Ready-To-Fire Configuration)</b>	
17. Provide 24-hour armed-guard surveillance.	AR 190-11, para 5-8c
<b>(Aircraft With Classified Equipment)</b>	
18. See AR 190-51, para 3-3d.	
<b>b. Risk Level II</b>	
1. Meet all requirements of level I above.	
2. Protect with perimeter fencing.	AR 190-51, para 3-3e
3. Conduct an hourly security check.	AR 190-51, para 3-3f
<b>c. Risk Level III</b>	
1. Meet all requirements of levels I and II above.	
2. Park in lighted areas.	AR 190-51, para 3-3e
3. Use IDS or continuous surveillance.	AR 190-51, para 3-3f
<b>SECTION II—UNARMED VEHICLES</b>	
<b>a. Risk Level I</b>	
1. Lock vehicles and control keys.	AR 190-51, para 3-5e
2. Post off-limits signs.	AR 190-51, para 3-5e
3. To the maximum extent possible, park in motorpools protected by a fence or by guards.	AR 190-51, para 3-5d
4. Remove and secure certain components.	AR 190-51, para 3-5e
5. Prohibit master-keyed locks.	AR 190-51, para 3-5e
6. Secure items (such as bolt cutters, torches) that could be used to violate vehicle security.	AR 190-51, para 3-5e
7. Conduct a security check every 4 hours.	AR 190-51, para 3-5f
8. Prohibit POVs from entering motorpools.	AR 190-51, para 3-5f
<b>b. Risk Level II</b>	
1. Meet all requirements of level I above.	
2. Light parking areas.	AR 190-51, para 3-5e
3. Park vehicles at least 20 feet from fence.	AR 190-51, para 3-5e
4. Control entry to and exit from motorpool.	AR 190-51, para 3-5f
5. Segregate and observe certain vehicles.	AR 190-51, para 3-5f
6. Conduct a security check every 2 hours.	AR 190-51, para 3-5f
<b>c. Risk Level III</b>	
1. Meet all requirements of levels I and II above.	
2. Use ground-anchors for trailers.	AR 190-51, para 3-5e
3. Place certain vehicles in secured garages.	AR 190-51, para 3-5e
4. Mark as "restricted area."	AR 190-51, para 3-5f
5. Provide written authorization for dispatch.	AR 190-51, para 3-5f
6. Check all drivers for dispatch and operator's permit.	AR 190-51, para 3-5f
7. Use IDS or continuous surveillance.	AR 190-51, para 3-5f
<b>SECTION III - ARMED VEHICLES AND TOWED WEAPONS SYSTEMS AND COMPONENTS</b>	
<b>a. Risk Level I</b>	
1. Meet all requirements of levels I and II in section II above.	USAREUR Reg 190-13
2. Coordinate closely with local HN authorities.	USAREUR Reg 190-13
3. Have communications with response- and police-forces.	USAREUR Reg 190-13
4. Have an active countersurveillance program.	USAREUR Reg 190-13
<b>(Vehicles/Towed Systems With Missiles/Rockets in Ready-To-Fire Configuration)</b>	
5. Provide 24-hour armed-guard surveillance.	AR 190-11, para 5-8c
<b>b. Risk Level II</b>	
1. Meet all requirements of level I above.	
2. Totally control access.	USAREUR Reg 190-13
3. Conduct hourly security checks.	USAREUR Reg 190-13
4. Mark as "restricted area."	USAREUR Reg 190-13
<b>c. Risk Level III</b>	

<b>Table C-1</b>	
<b>Analysis-Based Protection</b>	
1. Meet all requirements of levels I and II above.	
2. Maintain continuous surveillance.	USAREUR Reg 190-13
<b>SECTION IV—M-1 SERIES (ABRAMS) TANKS</b>	
<b>a. Risk Level I</b>	
1. Meet all requirements of levels I and II in section III above.	
2. Segregate to the maximum extent possible.	USAREUR ATS Security Guide
3. Maintain standby response force.	USAREUR ATS Security Guide
4. Park at least 10 meters from the fence.	USAREUR ATS Security Guide
5. When possible, park "hub to hub."	USAREUR ATS Security Guide
6. Park to allow guards easy observation.	USAREUR ATS Security Guide
7. Enclose motorpool with NATO-standard fence.	USAREUR ATS Security Guide
8. Equip gates with medium-security locks and chains.	USAREUR ATS Security Guide
9. Do not use master keys, and restrict key access.	USAREUR ATS Security Guide
10. Do not use security lights wired in a series.	USAREUR ATS Security Guide
11. Secure all hatches.	USAREUR ATS Security Guide
12. Maintain an access roster.	USAREUR ATS Security Guide
<b>(Tanks Loaded With AA&amp;E)</b>	
13. Provide 24-hour armed-guard surveillance.	AR 190-11, para 5-8c
<b>(Tanks with Classified Armor and Components)</b>	
14. See the USAREUR Abrams Tank System Security Guide.	
<b>b. Risk Level II</b>	
1. Meet all requirements of level I above.	
2. Maintain constant surveillance.	USAREUR Reg 190-13
<b>c. Risk Level III</b>	
1. Meet all requirements of levels I and II above.	
2. Maintain constant armed-guard surveillance.	USAREUR Reg 190-13
<b>SECTION V—COMMUNICATIONS AND ELECTRONICS EQUIPMENT AND NIGHT VISION DEVICES</b>	
<b>a. Risk Level I</b>	
1. Provide double-barrier protection to portable items.	AR 190-51, para 3-6b
2. Provide barrier protection to nonportable items.	AR 190-51, para 3-6b
3. Store as far from the exterior as possible.	AR 190-51, para 3-6b
4. Post "off limits" signs.	AR 190-51, para 3-6b
5. Control access to storage areas.	AR 190-51, para 3-6e
6. Control keys, locks, and seals.	AR 190-51, App D
7. Handreceipt pilferage-coded items.	AR 190-51, para 3-6f
8. Secure (by padlock) tactical communications equipment remaining on vehicles.	AR 190-51, para 3-6b
<b>b. Risk Level II</b>	
1. Meet all requirements of level I above.	
2. Store pilferage-coded items separately.	AR 190-51, para 3-6c
3. Prevent POV parking within 50 feet of storage areas.	AR 190-51, para 3-6f
4. Conduct inventories.	AR 190-51, para 3-6f
<b>c. Risk Level III</b>	
1. Meet all requirements of levels I and II above.	
2. Light the area.	AR 190-51, para 3-6d
3. Control landscaping.	AR 190-51, para 3-6d
4. Protect with IDS.	AR 190-51, para 3-6d
5. Review stock records.	AR 190-51, para 3-6g
6. Conduct a security check every 2 hours.	AR 190-51, para 3-6g
<b>SECTION VI—HEADQUARTERS (BRIGADE AND ABOVE) (note)</b>	
<b>a. Risk Level I</b>	
1. Continuously control access to mission-critical workareas and high-risk personnel when the facility is occupied.	AR 190-51, para 3-19
2. Secure all entrances when headquarters workareas are not occupied.	AR 190-51, para 3-23
3. Eliminate parking beneath facilities where possible.	AR 190-51, para 3-19
4. Keep parking as far from the facility as possible, but at least 30 feet.	AR 190-51, para 3-19

<b>Table C-1</b>	
<b>Analysis-Based Protection</b>	
5. Locate mission-critical and high-risk personnel in the interior of the facility, as far from the exterior as possible where feasible.	AR 190-51, para 3-19
6. Locate trash receptacles, landscaping features, and other features higher than 1 foot (that potentially provide concealment for aggressors or bombs) at least 30 feet from the facility.	AR 190-51, para 3-19
7. Security-force responsible for headquarters security will coordinate response procedures with local HN security and police authorities.	USAREUR requirement
8. Ensure that all critical areas (such as entrance ways) are provided adequate security lighting.	USAREUR requirement
9. Maintain an active countersurveillance program, and ensure that all headquarters staff personnel are briefed on their responsibilities.	USAREUR requirement
<b>b. Risk Level II</b>	
1. Meet all requirements of level I above.	
2. Continuously control access to the facility when occupied.	AR 190-51, para 3-19
3. Ensure that windows of mission-critical and high-risk personnel are covered with reflective, 4-mil, fragment-retention film, and backed up by heavy drapes.	AR 190-51, para 3-19
4. Ensure that windows and doors of mission-critical areas and high-risk personnel workareas are locked so that any attempt to enter them when the facility is unoccupied would require noticeably forced entry.	AR 190-51, para 3-19
5. Install duress alarms in areas occupied by mission-critical and high-risk personnel.	AR 190-51, para 3-19
<b>c. Risk Level III</b>	
1. Meet all requirements of levels I and II above.	
2. Ensure that the facility is surrounded by a perimeter fence at least 50 feet from the facility.	AR 190-51, para 3-19
3. Ensure that the facility is guarded, and access to the entire facility is controlled at all times.	AR 190-51, para 3-19
4. Ensure that personnel not assigned to the facility, who enter areas where mission-critical assets or high-risk personnel, are located are searched for weapons and explosives at least randomly.	AR 190-51, para 3-19
<b>NOTE:</b> Corps and above headquarters will be protected at risk level III at all times.	

<b>Table C-2</b>	
<b>Absolute-Standard Protection (revised 1 May 2003)</b>	
<b>SECTION I—AA&amp;E UNIT ARMS ROOMS</b>	
<b>a. Categories IV and III</b>	
1. Store in approved structure.	AR 190-11, para 4-2a
2. Protect with IDS.	AR 190-11, para 4-2a
3. Conduct security checks every 24 hours.	AR 190-11, para 4-2a
4. Light the area.	AR 190-11, para 4-2d
5. Use proper locks.	AR 190-11, para 4-2e
6. Maintain K&LC.	AR 190-11, para 3-8
7. Control access.	AR 190-11, para 4-19a
8. Emplace communications.	AR 190-11, para 3-6a
9. Designate as "restricted area."	AR 190-11, para 4-15
<b>b. Category II</b>	
1. Meet all requirements of categories III and IV above.	
2. Post armed guard if IDS fails.	AR 190-11, para 4-2f(1)
3. Conduct security checks every 8 hours.	AR 190-11, para 4-2a(3)
<b>c. Category I</b>	
1. Meet all requirements of categories II above.	
2. Implement the two-person rule.	AR 190-11, para 5-9c
<b>SECTION II—AA&amp;E IN BULK STORAGE</b>	
<b>a. Category IV</b>	
1. Store in approved structure.	AR 190-11, para 5-2

<b>Table C-2 Absolute-Standard Protection (revised 1 May 2003)</b>	
<ol style="list-style-type: none"> <li>2. Conduct security checks every 48 hours.</li> <li>3. Protect with NATO-standard fencing.</li> <li>4. Use proper locks.</li> <li>5. Maintain K&amp;LC.</li> <li>6. Emplace communications.</li> <li>7. Control entry.</li> <li>8. Designate as "restricted area."</li> <li>9. Post signs announcing IDS, if present.</li> </ol>	<p>AR 190-11, para 5-2 USAREUR Reg 190-13 AR 190-11, para 5-6a AR 190-11, para 5-6b AR 190-11, para 5-7 AR 190-11, para 5-9 AR 190-11, para 5-10 AR 190-11, para 5-11</p>
<b>b. Category III</b>	
<ol style="list-style-type: none"> <li>1. Meet all requirements of category IV above.</li> <li>2. Conduct security checks every 24 hours (if no IDS).</li> </ol>	AR 190-11, para 5-2b(2)
<b>c. Category II</b>	
<ol style="list-style-type: none"> <li>1. Meet all requirements of category III above.</li> <li>2. Protect with IDS.</li> <li>3. Provide constant protection with armed guards (if IDS fails).</li> <li>4. Conduct security checks every 24 hours (every 2 hours if IDS fails).</li> <li>5. Light the area.</li> </ol>	<p>AR 190-11, para 5-2a AR 190-11, para 5-2a(2) AR 190-11, para 5-2a(2) AR 190-11, para 5-4a</p>
<b>d. Category I</b>	
<ol style="list-style-type: none"> <li>1. Meet all requirements of category II above.</li> <li>2. Conduct security checks every hour (if IDS fails).</li> <li>3. Implement the two-person rule.</li> </ol>	<p>AR 190-11, para 5-2a(2) AR 190-11, para 5-9c</p>
<b>SECTION III—NONCOMMERCIAL MOTOR VEHICLE MOVEMENTS OF AA&amp;E</b>	
<b>a. Categories IV and III, and Uncategorized AA&amp;E</b>	
<ol style="list-style-type: none"> <li>1. Maintain under continuous control.</li> <li>2. Use only GOVs; POVs are not authorized.</li> <li>3. Use the vehicle exclusively for AA&amp;E; do not mix AA&amp;E with other cargos.</li> <li>4. Lock, seal, or band cargo by shipper.</li> </ol>	<p>AR 190-11, para 7-15d AR 190-11, para 7-15a USAREUR Reg 190-13 AR 190-11, Para 7-19</p>
<b>b. Category II</b>	
<ol style="list-style-type: none"> <li>1. Meet all requirements of categories III and IV above.</li> <li>2. Place in the custody of a sergeant (E-5) or above.</li> <li>3. Provide armed-guard surveillance; one guard may cover a maximum of three vehicles.</li> <li>4. Require favorable ENAC for driver and guards.</li> <li>5. Lock and seal cargo by shipper.</li> </ol>	<p>AR 190-11, para 7-15c USAREUR Reg 190-13 AR 190-11, para 2-11a AR 190-11, para 7-19</p>
<b>c. Category I and Classified AA&amp;E (notes 1 and 2)</b>	
<ol style="list-style-type: none"> <li>1. Meet all requirements of category II above.</li> <li>2. Require the custodian to have a security clearance at least equal to the level of classification of AA&amp;E being transported.</li> <li>3. Provide an armed guard for each vehicle.</li> <li>4. Lock and seal cargo by shipper.</li> <li>5. Maintain a continuous audit trail by serial number and/or item to consignee.</li> <li>6. Require two-person certification.</li> <li>7. Maintain two-way communications between the lead- and trail-vehicles.</li> </ol>	<p>AR 55-355, para 34-2g AR 190-11, para 7-15c AR 190-11, Para 7-19 AR 190-11, para 7-4a AR 190-11. para 7-4a USAREUR Reg 190-13</p>
<p><b>NOTES:</b> 1. For commercial transportation of AA&amp;E by motor vehicle, rail, air, or sea, see AR 190-11, chap 7; AR 55-355; and USAREUR Reg 55-4. For transportation of AA&amp;E during training, refer to AR 190-11, para 2-5. 2. The requirement for armed-guard surveillance of AA&amp;E must be coordinated with HN authorities.</p>	
<b>SECTION IV—RAIL MOVEMENT OF AA&amp;E</b>	
<b>a. Categories IV, III, and II</b>	
<ol style="list-style-type: none"> <li>1. Ship inside locked (or equivalent system), sealed containers.</li> <li>2. Where possible, place containers to deny access to their doors.</li> <li>3. Require the shipper to notify a U.S. representative immediately when the train arrives at its destination.</li> <li>4. Ensure that escort team members have been fully briefed by a safety officer on the dangers of rail movements before the start of any rail mission.</li> </ol>	<p>USAREUR Reg 190-13 USAREUR Reg 190-13 DOD 5100.76-M USAREUR Reg 190-13</p>

<b>Table C-2</b>	
<b>Absolute-Standard Protection (revised 1 May 2003)</b>	
5. Under no circumstances will escort team members disembark from the passenger car and climb onto railcars or onboard equipment (for example, to check security seals or locks) when the train is being loaded for departure, while in transit, and when unloading at the final destination.	USAREUR Reg 190-13
<b>b. Category I and Classified AA&amp;E</b>	
1. Meet all requirements of categories II, III, and IV above.	
2. Ensure constant surveillance is conducted by armed guards.	DOD 5100.76-M

**APPENDIX D  
FORMS**

**D-1. PURPOSE**

This appendix identifies the USAREUR forms prescribed by this regulation. Other forms referenced in this regulation are listed in paragraph A-11.

**D-2. USAREUR PHYSICAL-SECURITY FORMS**

This regulation prescribes the following forms:

a. AE Form 190-13A, Permanent U.S. Army, Europe, Installation Pass. This form (fig D-1) is prescribed by chapter 4.

b. AE Form 190-13B, Application for Permanent U.S. Army, Europe, Installation Pass. This form (fig D-2) is prescribed by chapter 4.

c. AE Form 190-13C, Temporary U.S. Army, Europe, Installation Pass. This form (fig D-3) is prescribed by chapter 4.

d. AE Form 190-13D, Receipt for Confiscated ID Card. This form (fig D-4) is prescribed by chapter 4.

e. AE Form 190-13E, Security Badge (Red). This form (fig D-5) is prescribed by chapter 4.

f. AE Form 190-13F, Security Badge (Green). This form is prescribed by chapter 4.

g. AE Form 190-13G, Security Badge (Black). This form is prescribed by chapter 4.

h. AE Forms 190-13H(G)-R and 190-13H(I)-R, Personnel/Vehicle Record of Admission. This form (figs D-6 and D-7) is prescribed by chapter 4.

i. AE Form 190-13I, Issue of Weapons and Ammunition. This form (fig D-8) is prescribed by chapter 5.

j. AE Form 190-13J-R, Monitoring Station Emergency Information. This form (fig D-9) is prescribed by chapter 6.

k. AE Form 190-13K-R, Protected Area Emergency Information. This form (fig D-10) is prescribed by chapter 6.

l. AE Form 190-13L-R, Request for Waiver or Exception of Physical Security Requirements. This form (fig D-11) is prescribed by appendix E. Appendix E has specific instructions for completing and processing AE Form 190-13L.

**(Front)**

<b>PERMANENT U.S. ARMY, EUROPE, INSTALLATION PASS</b> <b>(USAREUR Reg 190-13)</b>		Control No.
Name <i>(Last, First, MI)</i>		Ausweis/Passport No.
Signature	<b>NOT VALID WITHOUT PHOTO</b>	Issuing Headquarters
Issue Date		Issued By (Typed Name and Grade)
Expiration Date		
Limitations		
Signature of Issuing Official		

AE Form 190-13A, Aug 86 This edition replaces AE Form 190-3A, dtd Feb 89, which is obsolete.

**(Back)**

**NOTICE**

This pass is only valid to the extent indicated on its face. It will be surrendered on termination of employment or expiration date shown (whichever is applicable).

**ZUR BEACHTUNG**

Dieser Pass gilt nur für den auf der Vorderseite angegebenen Bereich. Er muß zurückgegeben werden bei Beendigung des Arbeitsverhältnisses oder Ablauf der angegebenen Gültigkeitsdauer (was auch immer zutrifft).

**AVIS**

Ce laissez-passer n'est valable que dans les limites indiquées au recto. Il sera rendu à la terminaison d'emploi ou à la date d'expiration indiquée (suivant le cas).

**PROPERTY OF U.S. GOVERNMENT**

Figure D-1. AE Form 190-13C

<b>APPLICATION FOR PERMANENT U.S. ARMY, EUROPE, INSTALLATION PASS (USAREUR Reg 190-13)</b>			
<b>DATA REQUIRED BY THE PRIVACY ACT OF 1974 (5 U.S. CODE 552a)</b>			
<b>AUTHORITY:</b> Article 63, Suppl Agreement to NATO SOFA; 10 USC 3012			
<b>PRINCIPAL PURPOSES:</b> For identification of U.S. and non-U.S. nationals employed by U.S. Government agencies, contractors, vendors of non-military agencies of countries in which U.S. personnel have been accommodated when these personnel require recurring access to the accommodations under U.S. control and do not possess other valid entry authorization documents.			
<b>ROUTINE USES:</b> To identify personnel authorized routine or recurring access to installations under U.S. control. See 40 Fed Register 35151 for other routine uses.			
<b>MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION:</b> Voluntary, however, failure to provide any item of information will result in denial of entry onto the U.S.-controlled installation for which the AE Form 190-13A has been validated.			
<b>TO</b>	<b>FROM</b>	<b>DATE</b>	
<b>1. EMPLOYEE NAME (Last, First, MI)/NACHNAME VORNAME DES ARBEITNEHMERS</b>	<b>2. DATE OF BIRTH (GEBURTSDATUM)</b>	<b>3. CITIZENSHIP/ NATIONALITÄT</b>	<b>4. ID/PASSPORT NO./ AUSWEIS/PASS NR.</b>
<b>5. ADDRESS/UNIT OF ASSIGNMENT/ ADRESSE/EINHEIT</b>	<b>FOR USE BY ISSUING AUTHORITY</b>		
	<b>PASS NUMBER ISSUED/AUSWEISNUMMER</b>		
<b>6. INSTALLATION/LOCATION ACCESS/NAME DER KASERNE/DES GEBÄUDES, WO ENTRITT GEWÄHRT WERDEN SOLL</b>	<b>EFFECTIVE DATE/AUSGABEDATUM</b>	<b>EXPIRATION DATE/GÜLTIG BIS</b>	
	<b>LIMITATIONS/EINSCHRÄNKUNGEN</b>		
<b>7. REASON FOR APPLICATION (CHECK APPLICABLE BOX)/ANTRAGSGRUND (ZUTREFFENDES ANKREUZEN)</b>			
<input type="checkbox"/> ORIGINAL PASS <input type="checkbox"/> EXPIRATION OF PASS <input type="checkbox"/> REPLACEMENT OF LOST OR DAMAGED PASS (Explain in Remarks Block) <small>ORIGINALAUSWEIS    GÜLTIG BIS    AUSSTELLUNG EINES NEUEN AUSWEISES WEGEN VERLUST ODER BESCHÄDIGUNG</small>			
<b>8. REMARKS (Use reverse if additional space is required.) Employee is authorized to sign for visitors to installation</b> <input type="checkbox"/> YES <input type="checkbox"/> NO <small>BEMERKUNGEN (Rückseite benutzen wenn zusätzlicher Platz benötigt wird.) Der Angestellte ist berechtigt für Besucher dieser Kaserne zu unterschreiben.</small> <input type="checkbox"/> JA <input type="checkbox"/> NEIN			
<b>CONDITIONS APPLICABLE TO RECIPIENTS OF PASS</b>			
I understand that AE Form 190-13A (Permanent U.S. Army, Europe, Installation Pass) is valid only for the period of time shown and for the activities or purposes stated in the Limitations block. I understand that the AE Form 190-13A is U.S. Government property, is not transferable, and is not to be altered in any way. I understand that I am liable to search of my person and possessions (incl. vehicles) while on the installation.			
<b>BEDINGUNGEN FÜR AUSWEISEMPFÄNGER</b>			
Ich weiß, daß das AE Formular 190-13A (Unbefristeter Kasernenausweis des US-Herres) nur für die darauf angegebene Zeit gültig ist und nur für die darauf angegebenen Dienststellen und Zwecke benutzt werden darf. Ich wurde außerdem darüber informiert, daß das AE Formular 190-13A Eigentum der US-Regierung und nicht übertragbar ist, sowie auf keine Weise verändert werden darf. Mir ist bekannt, daß ich eine Durchsuchung meiner Person und meines Eigentums (Fahrzeug miteingetragen) zulassen muß, wenn ich mich innerhalb des Geländes befinde.			
<b>9. DATE OF APPLICATION AND SIGNATURE OF APPLICANT ANTRAGSDATUM UND UNTERSCHRIFT DES ANTRAGSTELLERS</b>	<b>10. RECEIPT OF AE FORM 190-13A IS ACKNOWLEDGED ERHALT DES AE-FORMULARS 190-13A WIRD HIERMIT BESTÄTIGT</b>	<b>11. DATE/DATUM</b>	
<b>VERIFICATION BY RESPONSIBLE OFFICIAL OF APPLICANT'S UNIT/ORGANIZATION</b>		<b>AUT-IDENTIFICATION BY ISSUING AUTHORITY</b>	
The status of the above named person has been verified and a bona fide need for access to the above listed installations/locations exists. Background check has been initiated or completed IAW USAREUR Reg 190-13.		<b>TYPED NAME</b>	
<b>ORGANIZATION AND PHONE NO.</b>		<b>GRADE AND TITLE</b>	
<b>TYPED NAME AND TITLE</b>		<b>ORGANIZATION</b>	
<b>SIGNATURE</b>		<b>SIGNATURE</b>	
AE Form 190-13B, Aug 95		This form replaces AE Form 190-3C, dtd Sep 89, which is obsolete.	

Figure D-2. AE Forms 190-13B

**(Front)**

<b>TEMPORARY U.S. ARMY, EUROPE, INSTALLATION PASS</b> (USAREUR Reg 190-13)	
<b>Name (Last, First, MI)</b>	<b>Control No.</b>
<b>Signature</b>	<b>Ausweis/Passport No.</b>
<b>Limitations</b>	
<b>Issue Date</b>	<b>Expiration Date</b>
<b>Issuing Headquarters</b>	<b>Validating Officer</b>

AE Form 190-13C, Aug 95      This edition replaces AE Form 190-3B, dtd Feb 89, which is obsolete.

**(Back)**

**NOTICE**

This pass is valid only to the extent indicated on its face. It will be surrendered on termination of employment or expiration date shown (whichever is applicable).

**ZUR BEACHTUNG**

Dieser Pass gilt nur für den auf der Vorderseite angegebenen Bereich. Er muß zurückgegeben werden bei Beendigung des Arbeitsverhältnisses oder Ablauf der angegebenen Gültigkeitsdauer (was auch immer zutrifft).

**AVIS**

Ce laissez-passer n'est valable que dans les limites indiquées au recto. Il sera rendu à la terminaison d'emploi ou à la date d'expiration indiquée (suivant le cas).

**PROPERTY OF U.S. GOVERNMENT**

Figure D-3. AE Form 190-13C



AE Form 190-13E, Aug 95

T	VALID FOR AREA(S)	
NAME, SN, OR CATEGORY		ISSUING OFFICER (Name, Rank, Title, and Signature)
BADGE NO.	EFFECTIVE DATES	

This edition replaces AE Form 190-3E, Jul 88, which is obsolete.

  
  

HEIGHT	WEIGHT	HAIR	EYES	SEX	DATE OF BIRTH
CARD NO.			UNIT		
			SIGNATURE OF BEARER		
	Left Index	Right Index	FINGERPRINTS This Credential is the Property of the United States Government. Its counterfeiting is a violation of Section 132, title 18, United States Code. It shall be re- turned to the issuing office on termination or demand. IF FOUND MAIL TO:		

**There are 3 different badges:**

- AE Form 190-13E (Security Badge--Red)
- AE Form 190-13F (Security Badge--Green)
- AE Form 190-13G (Security Badge--Black)

Figure D-5. AE Forms 190-13E (Red); F (Green); and G (Black)







<b>MONITORING STATION EMERGENCY INFORMATION</b>			
(USAREUR Reg 190-13)			
THIS STATION MONITORS THE FOLLOWING ACTIVITIES: (CONTACT THE LISTED PERSONNEL IF ACCESS OR KEYS ARE REQUIRED.)			
NAME	ACTIVITY	LOCATION	TELEPHONE NO.
CONTACT THE BELOW LISTED PERSON IF THE RESPONSE FORCE IS REQUIRED:			
NAME	ACTIVITY	LOCATION	TELEPHONE NO.
CONTACT THE BELOW LISTED PERSON IF A MAINTENANCE MALFUNCTION OF EQUIPMENT OCCURS:			
NAME	ACTIVITY	LOCATION	TELEPHONE NO.

**AE Form 190-13J-R**      This edition replaces AE Form 190-17A-R-E, Jan 93,  
 Aug 95                              which is obsolete.

Figure D-9. AE Form 190-13J-R

<b>PROTECTED AREA EMERGENCY INFORMATION</b> (USAREUR Reg 190-13)			
THIS PROTECTED AREA IS MONITORED AT THE FOLLOWING LOCATION:			
ACTIVITY	LOCATION	TELEPHONE NUMBER	
CONTACT THE FOLLOWING IN CASE OF ABNORMAL CONDITIONS:			
NAME	ACTIVITY	LOCATION	TELEPHONE NO.
CONTACT THE FOLLOWING IN CASE OF MAINTENANCE MALFUNCTIONS:			
NAME	ACTIVITY	LOCATION	TELEPHONE NO.

**AE Form 190-13K-R**      This edition replaces AE Form 190-17B-R-E, Jan 93,  
 Aug 95                      which is obsolete.

Figure D-10. AE Form 190-13K-R

<b>REQUEST FOR WAIVER OR EXCEPTION OF PHYSICAL SECURITY REQUIREMENTS</b> (USAREUR Reg 190-13)		(Completed by OPM, HQ USAREUR/7A) CONTROL NUMBER: EXPIRATION DATE:										
<b>PART I</b>												
FROM (Requesting Organization):		TO (BSB):										
1. TYPE OF REQUEST: <table style="width: 100%; border: none;"> <tr> <td style="text-align: center;"><input type="checkbox"/> INITIAL</td> <td style="text-align: center;"><input type="checkbox"/> WAIVER</td> <td style="text-align: center;"><input type="checkbox"/> CHANGE</td> </tr> <tr> <td style="text-align: center;">or</td> <td style="text-align: center;">or</td> <td style="text-align: center;">or</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/> EXTENSION</td> <td style="text-align: center;"><input type="checkbox"/> EXCEPTION</td> <td style="text-align: center;"><input type="checkbox"/> CANCELLATION</td> </tr> </table>				<input type="checkbox"/> INITIAL	<input type="checkbox"/> WAIVER	<input type="checkbox"/> CHANGE	or	or	or	<input type="checkbox"/> EXTENSION	<input type="checkbox"/> EXCEPTION	<input type="checkbox"/> CANCELLATION
<input type="checkbox"/> INITIAL	<input type="checkbox"/> WAIVER	<input type="checkbox"/> CHANGE										
or	or	or										
<input type="checkbox"/> EXTENSION	<input type="checkbox"/> EXCEPTION	<input type="checkbox"/> CANCELLATION										
2. BRIEF DESCRIPTION OF SPECIFIC REQUIREMENT FOR WHICH WAIVER OR EXCEPTION IS REQUESTED (Cite specific regulatory reference.):												
3. BRIEF DESCRIPTION OF ACTUAL DEFICIENCY (Attach diagram if necessary.):												
4. PROPOSED CORRECTIVE ACTION (If requesting an extension, explain reason for delay of corrective action.):												
5. DESCRIBE COMPENSATORY MEASURES IN PLACE UNTIL DEFICIENCY IS CORRECTED												
6. ESTIMATED CORRECTION DATE:	7. WORK ORDER NO./PRIORITY:	8. ESTIMATED COST:										
9. POINT OF CONTACT (Name/Rank/Telephone Number):												
10. RANK/NAME OF CDR/DIC:	11. SIGNATURE	12. DATE:										

AE Form 190-13L-R  
Aug 95
*Continue on Reverse*

Figure D-11. AE Form 190-13L-R (Front)

PART II				
FROM (BSB):		TO (ASG):		
13. RECOMMENDATION:	APPROVE	DISAPPROVE	SEE ATTACHED COMMENTS	
14. POINT OF CONTACT (Name/Rank/Telephone No.):				
15. RANK/NAME OF BSB PM:	16. SIGNATURE:		17. DATE:	
PART III				
FROM (ASG):		TO: Provost Marshal, USAREUR ATTN: AEAPM-O-PS Unit 29931 APO AE 09086		
18. RECOMMENDATION:	APPROVE	DISAPPROVE	SEE ATTACHED COMMENTS	
19. POINT OF CONTACT (Name/Rank/Telephone No.):				
20. RANK/NAME OF ASG PM:	21. SIGNATURE:		22. DATE:	
PART IV				
FROM: Provost Marshal, USAREUR ATTN: AEAPM-O-PS Unit 29931 APO AE 09036		TO: HQDA ATTN: DAMO-CDL-S Suite 225, 4401 Ford Ave. Alexandria, VA 22302-1432		
23. RECOMMENDATION:	APPROVE	DISAPPROVE	SEE ATTACHED COMMENTS	
24. POINT OF CONTACT (Name/Rank/Telephone No.):				
25. SIGNATURE:		26. DATE:		
PART V				
FROM: HQDA ATTN: DAMO-CDL-S 430 Army Pentagon WASH, DC, 20310-0400	THRU: Provost Marshal, USAREUR ATTN: AEAPM-O-PS Unit 29931 APO AE 09086	THRU (ASG):	THRU (BSB):	TO (REQUESTOR):
27. ACTION BY HQDA:	APPROVED	DISAPPROVED	SEE ATTACHED COMMENTS	
28. HQDA POINT OF CONTACT (Name/Rank/Telephone No.):				
29. HQDA APPROVAL AUTHORITY (Name/Rank/Title):	30. SIGNATURE:		31. DATE:	
32. CONTROL NUMBER (Provided by OPM, HQ USAREUR/JA):			33. EXPIRATION DATE (Provided by HQDA):	

Figure D-11. AE Form 190-13L-R--Continued (Back)

## APPENDIX E WAIVERS AND EXCEPTIONS

### E-1. PURPOSE

This appendix explains how to request waivers to and exceptions of security standards in USAREUR.

### E-2. PROCEDURES

Waivers and exceptions will be requested using AE Form 190-13L-R (Request for Waiver or Exception of Physical Security Requirements).

**a. Part I.** Requesting units or activities will complete part I as follows:

**(1) Address Blocks.** Enter the mailing address of the requesting organization and send to the supporting base support battalion (BSB).

**(2) Block 1.** Select Initial or Extension. Indicate whether the request is for a Waiver (normally good for 1 year) or an Exception (which must be revalidated every 2 years). If the request is either a change to or cancellation of a previous request, mark the appropriate box.

**(3) Block 2.** In one or two sentences, describe the requirement for which the waiver or exception is requested. Also cite the specific regulation and paragraph that establishes that physical-security requirement.

**(4) Block 3.** State the deficiency and, if needed, attach additional documentation to explain the deficiency. Identify the location of facility (for example, arms room, located in an occupied troop billets/unoccupied building; located on a U.S. occupied/unoccupied installation; the outer walls of facility do or do not form a perimeter barrier to the installation).

**(5) Block 4.** State the specific action being taken to correct deficiencies.

**(6) Block 5.** List the compensatory measures being taken until the deficiencies can be corrected. Ensure the security being provided meets or exceeds the requirements of the applicable regulation.

**(7) Block 6.** Indicate expected date deficiencies will be corrected.

**(8) Block 7.** State the project number (work order number) provided by the area support group (ASG) or BSB directorate of engineering and housing (DEH) and the priority assigned to the project.

**(9) Block 8.** Provide an estimate of the cost of the corrective action.

**(10) Blocks 9 through 12.** Self-explanatory.

**b. Part II.** The BSB provost marshal (PM) will review the request and send it to the ASG PM. The BSB PM will recommend approval or disapproval and may provide comments.

**c. Part III.** The ASG PM will review the request and complete part III, which is self-explanatory.

**d. Part IV.** The PM, USAREUR, will review the request, complete part IV, and send the action to HQDA for approval or disapproval.

**NOTE:** The PM, USAREUR, will assign a control number to identify the request in the USAREUR database. Any future correspondence about the waiver or exception request must include the assigned USAREUR control number.

**e. Part V.** HQDA (DAMO-ODL-E) will complete part V.

**APPENDIX F  
INSPECTION CHECKLISTS**

**F-1. PURPOSE**

This appendix provides checklists that may be used to quickly check for compliance with physical-security requirements.

**F-2. GENERAL**

The checklists in this appendix—

- a. Are not intended to be used in place of applicable regulations.
- b. Are only guides and quick references.
- c. May not cover all security requirements for a particular subject area.
- d. Are designed to include the same material as found in the Security Management System (SMS). SMS is a primary

tool of USAREUR physical-security inspectors. Physical-security inspections will be based on SMS, not on the checklists in this regulation.

**NOTE:** The glossary explains abbreviations in the tables.

**F-3. INDEX OF CHECKLISTS**

The following checklists are included in this appendix:

- a. Staff assistance visit (table F-1). This checklist provides for a review of the overall status of a physical-security program.
- b. Unit arms room (table F-2).
- c. Unit motorpool and Government property security (table F-3).
- d. Unit key-and-lock control (K&LC) (table F-4).

<b>Table F-1 Staff Assistance Visit Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
1. Are trained physical-security personnel assigned to the physical-security office (additional skill identifier H3/GS-080-O)?	[ ]	[ ]	[ ]	AR 190-13, para 3-3
2. Have MEVAs, which the physical security office is responsible for inspecting, been identified?	[ ]	[ ]	[ ]	AR 190-13, para 2-4
3. Are inspections being conducted every 18 months for AA&E-related MEVAs and every 24 months for all other MEVAs?	[ ]	[ ]	[ ]	AR 190-13, para 2-11
4. Are AA&E storage facilities re-inspected within 6 months if they fail the initial inspection?	[ ]	[ ]	[ ]	AR 190-11, para 2-6a(4)
5. Is there a physical-security officer who supervises the physical-security program?	[ ]	[ ]	[ ]	AR 190-13, para 1-25
6. Is there a functioning JAWG or physical-security council that meets regularly to discuss physical-security related issues?	[ ]	[ ]	[ ]	AR 190-13, para 1-23c; CINCUSAREUR OPOORD on Force Protection
7. Are physical-security personnel aware of the relationship between physical security and force-protection?	[ ]	[ ]	[ ]	AR 190-13, para 2-5
8. Does the physical-security office have at least the following references on hand:				No reference
AR 190-11	[ ]	[ ]	[ ]	
AR 190-13	[ ]	[ ]	[ ]	
AR 190-16	[ ]	[ ]	[ ]	
AR 190-51	[ ]	[ ]	[ ]	
AR 525-13	[ ]	[ ]	[ ]	
DA Pamphlet 190-51	[ ]	[ ]	[ ]	
FM 19-30	[ ]	[ ]	[ ]	
USAREUR Regulation 190-13	[ ]	[ ]	[ ]	
9. Does the physical-security office have a copy of all active waivers and exceptions for facilities within their area of operation?	[ ]	[ ]	[ ]	AR 190-11, para 2-4i; AR 190-51, para 1-6
10. Does the physical-security office maintain a database of IDS by type, location, and status?	[ ]	[ ]	[ ]	USAREUR Reg 190-13, para 6-13
11. Does the physical-security office maintain a security-guard database consisting of at least: number of manyear requirements for guards, type of guards (for example, CSG, BMM, MP), purpose of guards, location of guards, and number of assigned CSG guards?	[ ]	[ ]	[ ]	USAREUR Reg 190-13, para B-15e
12. Does the physical-security office monitor and track property crime?	[ ]	[ ]	[ ]	AR 190-13, para 2-8
13. Is the physical-security office properly utilizing the SMS Program?	[ ]	[ ]	[ ]	USAREUR Reg 190-13, para B-15h

<b>Table F-2 Unit Arms Room Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
<b>CONSTRUCTION</b>				
1. Does the unit have a DA Form 4604-R that is not more than 5-years old in the arms room indicating the highest category of weapons/ammunition authorized for storage?	[ ]	[ ]	[ ]	AR 190-11, para 2-2d
2. If deficiencies are listed on the DA Form 4604-R, are compensatory measures being taken until the deficiencies are corrected?	[ ]	[ ]	[ ]	AR 190-11, para 2-4
3. Has a request for a waiver or an exception been submitted for uncorrectable deficiencies noted on a physical-security inspection, or is one on file in the arms room?	[ ]	[ ]	[ ]	AR 190-11, para 2-4
4. Is the arms-room door provided with exterior security lighting?	[ ]	[ ]	[ ]	AR 190-11, para 4-2d
5. Are switches for exterior lights installed so that they are not accessible to unauthorized individuals?	[ ]	[ ]	[ ]	AR 190-11, para 4-2d(4)
6. Are exterior security lights covered with mesh screen or vandal-resistant lenses that will prevent their being broken?	[ ]	[ ]	[ ]	AR 190-11, para 4-2d(5)
7. Does the door allowing access to arms rooms containing category I and II arms meet the established criteria?	[ ]	[ ]	[ ]	AR 190-11, app G
8. Are arms-room doors, other than the main entrance, secured from the inside with locking bars, dead bolts, or with approved secondary padlocks (American series 200 or 5200)?	[ ]	[ ]	[ ]	AR 190-11, para 4-2e(1)
9. Are the door hinges the fixed-pin security-hinge type or equivalent? Are exposed hinge pins pinned, spot-welded, or otherwise secured to prevent removal?	[ ]	[ ]	[ ]	AR 190-11, paras 4-2a and G-1d(3)
10. Are the bars or steel mesh that protects windows and openings embedded in the structure of the building or welded to a steel frame that is securely attached to the wall with the fastening inaccessible from the exterior of the arms-storage facility?	[ ]	[ ]	[ ]	AR 190-11, para G-1e
11. Are high-security padlocks (S&G model 831B, NSN 5340-01-188-1560; Hi-Shear model LK 1200, NSN 5340-00-799-8248; or S&G model 833C, NSN 5340-01-217-5068) used with high-security hasps to secure the arms- room door?	[ ]	[ ]	[ ]	AR 190-11, para 4-2e(1)
<b>NOTE:</b> On a double-door system, the high-security lock and hasp will be on the most secure door. The most secure door will normally be the one meeting the specifications in item 9 above. Secondary padlocks with a hardened steel shackle (American series 200 or 5200) may be used to secure the other door.				
12. Are weapons stored in the arms room secured in standard-issue racks or locally-fabricated arms racks or metal containers that are certified by the local engineers (DEH), and is the certificate filed in the arms room?	[ ]	[ ]	[ ]	AR 190-11, para 4-2c(3)
13. Are all weapons racks and containers secured to prevent removal of AA&E, and locked with approved secondary padlocks (American series 200 or 5200)?	[ ]	[ ]	[ ]	AR 190-11, paras 4-2c(2) and (3)
14. Are weapons racks and ammunition containers that weigh less than 500 pounds fastened to the walls or floors, or are they chained together in groups totalling more than 500 pounds? Are the chains secured with approved secondary padlock (American series 200 or 5200), and are the chains heavy duty, hardened steel, galvanized of at least 5/16-inch thickness?	[ ]	[ ]	[ ]	AR 190-11, para 4-2c(2)
15. Are "Restricted Area" signs posted near the entrance on the outer wall of the arms room, at eye level, in English and the HN language?	[ ]	[ ]	[ ]	AR 190-11, para 4-4
16. Are signs posted on the wall near the entrance to the arms storage room, vault, or building in both English and the HN language, announcing the presence of IDS?	[ ]	[ ]	[ ]	AR 190-11, para 4-5; USAREUR Reg 190-13, para 6-34
<b>ARMS-ROOM KEY CONTROL</b>				
1. Are primary and alternate key-and-lock custodians appointed in writing to ensure the proper custody and handling of arms-room keys and locks?	[ ]	[ ]	[ ]	AR 190-11, para 3-8c

<b>Table F-2 Unit Arms Room Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
2. Does the unit have a current roster of personnel authorized to receive arms-room keys, signed by the designated unit official and protected from public view?	[ ]	[ ]	[ ]	AR 190-11, para 3-8a
3. Are inventories of keys and locks conducted twice a year, and are the results documented and retained for 1 year? The inventories may be documented on DA Form 5513-R.	[ ]	[ ]	[ ]	AR 190-11, para 3-8e
4. Does the key-and-lock custodian maintain a record (DA Form 5513-R) identifying all keys and locks and combinations to locks used to secure arms-room racks, containers, security chains, and all replacement or reserve keys and locks?	[ ]	[ ]	[ ]	AR 190-11, para 3-8c
5. Is a DA Form 5513-R used to ensure positive control of keys, and to establish responsibility for the custody of stored AA&E, and is the DA Form 5513-R retained for 90 days when completed?	[ ]	[ ]	[ ]	AR 190-11, para 3-8a
6. Have padlocks and keys that do not have a serial number been given one?	[ ]	[ ]	[ ]	AR 190-11, para 3-8e
7. Are keys providing access to category I or II AA&E that are not in use or are not attended stored in a class 5 GSA security container or equivalent?	[ ]	[ ]	[ ]	AR 190-11, para 3-8b(2); DOD 5100.76-M, chap 3, para H-1b
8. Are keys providing access to category III or IV AA&E that are not in use or are not attended stored in a container of at least 20-gauge steel (or equivalent strength) and equipped with approved secondary padlock (American series 200 or 5200) or a GSA-approved, built-in, 3-position, changeable combination lock?	[ ]	[ ]	[ ]	AR 190-11, para 3-8b(2)
9. In the event of lost, misplaced, or stolen keys, was an investigation initiated immediately? Are replacement or reserve locks, cores, and keys secured immediately to preclude access by unauthorized individuals?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-11, para 3-8b(3)
10. Are padlocks not in use secured to the staple or hasp when the area or container is open to preclude theft, loss, or substitution of the lock?	[ ]	[ ]	[ ]	AR 190-11, para 3-8d
11. Are master-key systems or multiple-key systems used? <b>NOTE:</b> This is prohibited.	[ ]	[ ]	[ ]	AR 190-11, para 3-8b(3)
12. Are keys to arms-room storage buildings, rooms, racks, IDS, or containers removed from the installation?	[ ]	[ ]	[ ]	AR 190-11, para 3-8a
13. When the responsibility for arms-room keys is transferred between two authorized individuals, do both parties conduct a physical count of all arms and ammunition stored in the arms room?	[ ]	[ ]	[ ]	DA Pam 710-2-1, para 9-11a(1)
14. Is the count in 13 above recorded on DA Form 2062 and maintained on file until the next serial-number inventory is conducted?	[ ]	[ ]	[ ]	DA Pam 710-2-1, para 9-11a(2)
<b>IDS</b>				
1. Is the arms room staffed, under constant surveillance (by individuals), or have an active IDS and checked by a security patrol (SDO, SDNCO, or guard) at least once each 8 hours?	[ ]	[ ]	[ ]	AR 190-11, para 4-2a(3)
2. In the event the IDS fails, are armed guards posted 24 hours each day to maintain constant unobstructed observance of the storage structures, prevent unauthorized access to the storage structures, and make known any unauthorized access to the storage structures?	[ ]	[ ]	[ ]	AR 190-11, para 4-2f(1)
3. Is the IDS control-unit door key (maintenance key) kept separate from other operational IDS keys, and is access permitted only to authorized maintenance personnel?	[ ]	[ ]	[ ]	AR 190-11, para 3-8a
4. Do personnel closing the protected area (arms room), ensure that the control unit is changed from "Access" to "Secure" before departing the arms-room area?	[ ]	[ ]	[ ]	USAREUR Reg 190-13, para 6-22
5. Are procedures in effect at the monitoring station to verify the identity of personnel before opening and closing a facility protected by IDS?	[ ]	[ ]	[ ]	USAREUR Reg 190-13, para 6-29
6. Is a response-force identified and capable of responding to an alarm within 15 minutes or less?	[ ]	[ ]	[ ]	AR 190-11, para 3-6a

**USAREUR Reg 190-13**

<b>Table F-2 Unit Arms Room Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
7. Is a DA Form 5513-R maintained for issuing and receiving IDS keys?	[ ]	[ ]	[ ]	AR 190-11, para 3-8
8. Do arms-room personnel have a list of personnel authorized by the DEH and verified by the ASG or BSB security officer to perform maintenance, repair, and testing of IDS?	[ ]	[ ]	[ ]	USAREUR Reg 190-13, para 6-29b
<b>ACCOUNTABILITY OF POF, AMMUNITION, AND OTHER WEAPONS</b>				
1. Are all service members (E-4 and below) POFs stored in the arms room?	[ ]	[ ]	[ ]	USAREUR Reg 190-6, para 12b
2. Are POFs, ammunition, and weapons stored in unit arms rooms tagged with the name, grade, SSN, and DEROS of the owner; make, caliber, and serial number of the weapon; registration number and expiration date of the registration?	[ ]	[ ]	[ ]	USAREUR Reg 190-6, para 14b(1)
<b>NOTE:</b> AE Form 190-6B is required only for POFs. Individual POF owners keep their AE Forms 190-6B; arms-room personnel do not keep the forms for them (USAREUR Reg 190-6, para 14c).				
3. Is USAREUR Regulation 190-6 posted on the unit bulletin board?	[ ]	[ ]	[ ]	AR 190-11, para 4-5a(3)
4. Are POFs, ammunition, and other weapons secured in the arms room stored separate from military AA&E and protected by the same security measures (incl inventory and accountability) that are required for Government arms and ammunition?	[ ]	[ ]	[ ]	AR 190-11, para 4-5a; USAREUR Reg 190-6, para 13
5. Do personnel desiring to use their POF obtain written permission from their commander and sign the weapon out using the same sign-out/sign-in procedures as those required for Government weapons?	[ ]	[ ]	[ ]	USAREUR Reg 190-6, para 14b(1)
6. Are POFs carried on field training exercises by anyone?	[ ]	[ ]	[ ]	USAREUR Reg 190-6, para 15
7. Are prohibited items stored in the arms room?	[ ]	[ ]	[ ]	USAREUR Reg 190-6, glossary, sec II
<b>SECURITY SCREENING PROGRAM</b>				
1. Has the command conducted a security screening program for all personnel who are assigned duties that involve responsibility for control, accountability, or shipment of AA&E?	[ ]	[ ]	[ ]	AR 190-11, para 2-11a
2. Are security screening checks recorded on DA Form 7281-R? Are DA Forms 7281-R kept in unit files until the individual departs or is relieved of his or her AA&E-oriented duties?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-11, para 2-11
3. Have Government employees (civilian or military) who operate a vehicle or provide security to a vehicle transporting category I, category II, or classified AA&E been the subject of a favorable NAC, ENAC, or foreign-national screening?	[ ]	[ ]	[ ]	AR 190-11, para 2-11a(1); USAREUR Reg 604-1
4. Have personnel authorized unaccompanied access to category I and II AA&E been subject to security-screening program? Did security screening include personal interviews by the individual's commander, medical files check, personnel records check, and PM files check?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-11, para 2-11c
5. Are security-screening checks updated every 3 years?	[ ]	[ ]	[ ]	AR 190-11, para 2-11e
<b>USE AND CONTROL OF PROTECTIVE SEALS</b>				
1. Are primary and alternate seal custodians appointed in writing and do they maintain a hardcover logbook that shows seal serial numbers; dates issued; names of recipients; using offices, units, or activities; identification of items to which applied, dates and times applied; locations of items?	[ ]	[ ]	[ ]	AR 190-51, paras D-2 and D-10c
2. Are all seals not issued for actual use secured in a locked metal container with controlled access by the primary and alternate custodians, and is a recorded monthly inventory conducted?	[ ]	[ ]	[ ]	AR 190-51, para D-10b(6)
3. Have procedures been established for checking seals and identifying actions to be taken on finding a broken seal?	[ ]	[ ]	[ ]	AR 190-51, para D-10e
4. Are used seals defaced to prevent unauthorized reuse? Are used seals properly disposed of?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-51, para D-10f
<b>MISCELLANEOUS</b>				
1. Has a written SOP been established for the activity, approved through command channels, and maintained on file?	[ ]	[ ]	[ ]	AR 190-11, para 1-12a

<b>Table F-2 Unit Arms Room Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
2. If the facility is a consolidated arms room, have procedures been established in a written LOA to assign responsibility for access, issue, receipt, and physical accountability for all items? Does the LOA identify the unit that has responsibility for overall security of the facility?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-11, para 4-4
3. If ammunition is stored in the arms room, is it consistent with operational requirements, authorized in writing by the unit commander, and inventoried by lot-number during the monthly serial-number inventories?	[ ]	[ ]	[ ]	AR 190-11, para 5-5c(1)(a); DA Pam 710-2-1, para 9-11b(3)
4. Is the ammunition authorized for storage in the arms room, stored in separate containers from weapons, and secured in banded crates or metal containers equivalent to standard-issue metal wall-lockers?	[ ]	[ ]	[ ]	AR 190-11, para 5-8c(2)
5. Are monthly serial-number weapon inventories being conducted by an NCO, warrant officer, commissioned officer, or DOD civilian appointed by the responsible officer, and not by the same person in consecutive months?	[ ]	[ ]	[ ]	AR 710-2, para 2-12; DA Pam 710-2-1, para 9-11b
6. During monthly arms-room serial-number and sensitive-item inventories, is loose ammunition that is not banded and in sealed containers counted and annotated on the inventory sheet showing total rounds onhand by type? <b>NOTE:</b> Ammunition in banded or sealed containers must be counted by containers and inspected to ensure bands and seals are intact.	[ ]	[ ]	[ ]	DA Pam 710-2-1, para 9-11b(3)
7. Are monthly arms-room inventory records maintained for at least 2 years?	[ ]	[ ]	[ ]	AR 190-11, para 6-2b(2)(b)1
8. Are tools (such as hammers, bolt-cutters, chisels), that could be used to assist unauthorized persons gain access to arms-storage facilities readily accessible to intruders?	[ ]	[ ]	[ ]	AR 190-11, para 4-18a
9. Is the most recent physical-security inspection report maintained on file in the unit?	[ ]	[ ]	[ ]	AR 190-13, para 2-12
10. Have deficiencies (findings) noted on inspection reports been corrected, and has action taken been reported to the PM office by RBI?	[ ]	[ ]	[ ]	AR 190-11, para 2-12
11. Are category-II AA&E storage facilities checked by a security patrol on an irregular basis (not exceeding 8 hours) after duty hours? Are these checks recorded on SF 702, and maintained on file for 90 days?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-11, para 4-2f(2)(a)
12. Has the commander provided written approval for storage of high-value items (such as night vision devices, compasses, field glasses) in the arms room?	[ ]	[ ]	[ ]	AR 190-11, para 4-18
13. Has a "two-person rule" been established for access to category I missile- and rocket-storage facilities?	[ ]	[ ]	[ ]	AR 190-11, para 5-9c
14. Are inert and expended launcher tubes, inert mines, inert rocket-launcher training devices, and practice rockets secured as category-IV AA&E?	[ ]	[ ]	[ ]	AR 190-11, para 5-2c(3)
15. Has the unit armorer signed for all property in the arms room?	[ ]	[ ]	[ ]	AR 710-2, para 2-10

<b>Table F-3 Unit Motorpool and Government Property Security Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
1. Has a risk analysis been conducted on the facility to determine the level of physical-security measures and procedures required?	[ ]	[ ]	[ ]	AR 190-51, chap 2
2. When Army vehicles are not in use, are they parked in a motorpool protected by a perimeter fence or dedicated guards?	[ ]	[ ]	[ ]	AR 190-51, para 3-5d
3. Is the fence around the motorpool constructed according to guidance in FM 19-30; Army Corps of Engineers Drawing No. 40-16-08, type FE-5; or NATO-standard design?	[ ]	[ ]	[ ]	AR 190-51, para 3-1d
4. Is the perimeter fence adequately repaired?	[ ]	[ ]	[ ]	AR 190-51, para 3-1d; FM 19-30, chap 5
5. Is the perimeter-fence clear zone adequately maintained to prevent unobserved detection of intruders?	[ ]	[ ]	[ ]	AR 190-51, para 3-1d; FM 19-30, para 5-12; AR 420-70
6. Is the motorpool checked at least once every 4 hours for tampering, sabotage, loss, or damage?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(1)(a)
7. Do commercial vehicles have activated manufacturer-installed door- and ignition-locking devices?	[ ]	[ ]	[ ]	AR 190-51, para 3-5e(1)(a)
8. Are tactical vehicles and other Army vehicles secured with a chain and padlock that immobilize the steering wheel to prevent the vehicle from being driven? Are hoods, spare tires, and fuel tanks secured if the local environment warrants?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-51, paras 3-5e(1)(b) and (c)
9. Do material-handling equipment (for example, forklifts) have their steering mechanisms immobilized or transmission lever locked in the neutral position?	[ ]	[ ]	[ ]	AR 190-51, para 3-5e(1)(d)
10. Are inoperable, unserviceable vehicles protected from cannibalization?	[ ]	[ ]	[ ]	AR 190-51, para 3-5e(2)(d)
11. Are accessible and easily removable components that are vulnerable to theft because of value or utility removed from vehicles and secured separately? Are components secured in storage structures, locked totally enclosed armed vehicles or truck van, or locked equipment box or similar container secured directly to the vehicle by a locally fabricated method?	[ ] [ ]	[ ] [ ]	[ ] [ ]	AR 190-51, para 3-5e(3)
12. Are primary and alternate key-and-lock custodians appointed in writing to ensure the proper custody and handling of keys and locks?	[ ]	[ ]	[ ]	AR 190-51, para 3-5e(5); this reg, table F-4
13. Are POVs prohibited from motorpools? The installation commander may authorize POV storage in motorpools during unit deployment exercises.	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(1)(c)
14. Are items that can be used to defeat security measures (such as bolt-cutters, hacksaws, axes, steel bars or rods) secured when not in use?	[ ]	[ ]	[ ]	AR 190-51, para 3-5e(6)
15. Do level-II motorpools have both entries and exits controlled? Control may be by guards or by locked gates.	[ ]	[ ]	[ ]	AR 190-51, para 3-5g(2)(a)
16. Are vehicles in level-II or level-III motorpools parked at least 20 feet from the perimeter of the parking area, or as far from the perimeter as possible?	[ ]	[ ]	[ ]	AR 190-51, para 3-5e(7)(c)
17. Are vehicles particularly vulnerable to theft, misappropriation, or damage in level-II motorpools segregated to where guards or unit personnel can readily see them?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(2)(c)
18. Are level-II motorpools checked at least once every 2 hours for tampering, sabotage, loss, or damage?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(2)(d)
19. Are level-III motorpools marked as "Restricted Areas"?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(3)(b)
20. Are level-III motorpools under continuous surveillance by guards, if not protected by IDS?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(3)(e)
21. Are vehicles with missiles or rockets in ready-to-fire configuration provided with constant armed-guard protection?	[ ]	[ ]	[ ]	AR 190-11, para 5-8c(4)

<b>Table F-3 Unit Motorpool and Government Property Security Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
22. Has the unit commander or a designated representative provided written authorization before vehicles in level-III motorpools are dispatched?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(3)(d)
23. Are drivers checked for possession of a valid dispatch and operators permit before they depart a level-III motor pool?	[ ]	[ ]	[ ]	AR 190-51, para 3-5f(3)(d)
24. Do POL tank-trucks that contain fuel and not under surveillance by the operator or guard have locked hatch covers, locked manifold-access doors, and manifold valve, secured with a seal (if manifold-access door cannot be locked)?	[ ]	[ ]	[ ]	AR 190-51, para 3-14a
<b>NOTE:</b> Use specified nonsparking brass locks for safety.				
25. Is packaged POL secured in an adequate storage area?	[ ]	[ ]	[ ]	AR 190-51, para 3-13b(1)(c)
26. Are POL credit cards, identification plates, and aviation fuel plates controlled?	[ ]	[ ]	[ ]	AR 190-51, para 3-13c(1)(c)
27. Are POL pumps not activated by a credit-card-type device locked and electric power turned off when not under constant surveillance?	[ ]	[ ]	[ ]	AR 190-51, para 3-13b(1)(b)
28. Are serviceable used and new repair parts secured in an adequate single-storage area that is accessible only to maintenance or supply personnel?	[ ]	[ ]	[ ]	AR 190-51, paras 3-11f(3) and 3-12
29. Are nonportable repair parts secured inside a building or protected by a perimeter barrier?	[ ]	[ ]	[ ]	AR 190-51, para 3-11c(2)
30. Are toolsets and kits secured with a padlock and with other tools stored in a secure location when not in use?	[ ]	[ ]	[ ]	AR 190-51, paras 3-22b and c

<b>Table F-4 Unit K&amp;LC Checklist</b>				
<b>Requirement</b>	<b>Yes</b>	<b>No</b>	<b>Not Applicable</b>	<b>Reference</b>
1. Are primary and alternate key-and-lock custodians appointed in writing to ensure the proper custody and handling of all keys and locks?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-2a
2. Does the key-and-lock custodian maintain a control register (DA Form 5513-R) to ensure continuous accountability for keys of locks used to secure Government property?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6), D-2c, and D-3
3. Are keys providing access to Government property that are not in use or not attended stored in a container (not containing classified material) or depository made of at least 26-gauge steel, equipped with a tumbler-type locking device, and permanently affixed to a wall or equivalent barrier?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-4a
4. Is there an access roster maintained in the key depository listing those authorized to issue and receive keys?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-3
5. Is the key to the depository secured when not in use?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-5c
6. Are master-key systems or multiple-key systems used? <b>NOTE:</b> This is prohibited except where noted in AR 190-51.	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-5
7. Have padlocks and keys that did not have a serial number been given one?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-6e
8. Are inventories of keys and locks conducted twice a year, and are the results documented and retained until the next inventory is conducted? <b>NOTE:</b> The inventories can be documented on DA Form 5513-R.	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6), D-3, and D-6b
9. In the event of lost, misplaced, or stolen keys, was an inquiry initiated immediately? <b>NOTE:</b> Replacement or reserve locks, cores, and keys will be secured immediately to preclude access by unauthorized individuals.	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-6c
10. Are padlocks and keys not in use secured in a locked container that does not contain classified material, and is access controlled to the container?	[ ]	[ ]	[ ]	AR 190-51, paras 1-4e(6) and D-5c
11. Are keys for arms rooms and basic-load storage areas kept separate from other keys?	[ ]	[ ]	[ ]	AR 190-11, para 3-8a

## APPENDIX G INSPECTOR CREDENTIALS

### G-1. GENERAL

The Office of the Provost Marshal (OPM) (AEAPM-O-PS), HQ USAREUR/7A, will maintain a bulk supply of DA Forms 4261 and 4261-1 (Physical Security Inspector Identification Card) for USAREUR.

a. Custodians from each area support group (ASG) will request bulk issue from OPM. Requests must include a copy of appointment orders for DA Form 4261 and 4261-1 custodians.

b. OPM will send DA Forms 4261 and 4261-1 to the requesting unit using DA Form 410 (Receipt for Accountable Form). Units below the ASG level may not keep stocks of blank DA Forms 4261 or 4261-1.

### G-2. REQUEST

a. Requests for credentials will be made according to AR 190-13 and this regulation. Requests for criminal records checks (CRCs) will include OPM as an information addressee (CINCUSAREUR MANNHEIM GE//AEAPM-O-PS//).

b. Requests for CRCs will be initiated by the ASG commander. ASG commanders may delegate authority to base support battalion (BSB) commanders to initiate CRCs.

c. When the requesting organization receives a favorable CRC, the commander will send a memorandum to the ASG requesting DA Forms 4261 and 4261-1. The memorandum must—

(1) List the complete name, rank, and social security number (SSN) of the inspector.

(2) Verify that the inspector has a favorable CRC and has successfully completed the physical-security course conducted by the United States Army Military Police School or through a DOD-approved course of instruction.

(3) List a point of contact (POC) with a telephone number.

d. ASG provost marshals (PMs) may sign completed DA Forms 4261 for credentials issued in their commands.

e. Once credentials are issued, the ASG will send a written report to OPM (AEAPM-O-PS). In addition to the information required by AR 190-13, paragraph 3-2, the report will show the date the credentials were issued, the date credentials expire, and the unit POC and telephone number.

### G-3. CUSTODIAN RESPONSIBILITIES

ASG PMs will—

a. Keep a log of assigned DA Forms 4261 and 4261-1 showing to whom they are assigned.

b. Inventory both forms twice a year.

c. Prepare a memorandum for record for each inventory, and file it with the log.

### G-4. LOSSES AND WITHDRAWALS

When DA Forms 4261 and 4261-1 are lost or withdrawn, the unit will report, in writing, through the ASG to OPM (AEAPM-O-PS) within 2 workdays after discovery. The report will cite the circumstances of the loss or withdrawal. AR 190-13 lists procedures for withdrawing DA Forms 4261 and 4261-1.

### G-5. ANNUAL REPORT

Credential-control custodians will send a consolidated report for the previous calendar year to the Commander in Chief, USAREUR, ATTN: AEAPM-O-PS, Unit 29931, APO AE 09086, by 15 January, listing each inventory transaction, including the following:

a. The complete name, rank (or general-schedule equivalent), and SSN of the inspector, and the inspector's unit of assignment.

b. The date DA Forms 4261 and 4261-1 were issued and their expiration dates.

c. The date and reason DA Forms 4261 and 4261-1 were lost or withdrawn (for example, permanent change of station, change of duty).

e. Unassigned DA Forms 4261 and 4261-1 by control number.

f. POCs and telephone numbers.

g. Copy of duty-appointment orders for the credential-custodian.

**GLOSSARY**

**SECTION I  
ABBREVIATIONS**

1st PERSCOM	1st Personnel Command	DOD	Department of Defense
AA&E	arms, ammunition, and explosives	DOIM	director(ate) of information management
AAFES-Eur	Army and Air Force Exchange Service, Europe	DOL	director(ate) of logistics
AD	active duty	DS	direct support
ADA	air defense artillery	DPTMS	director(ate) of plans, training, mobilization, and security
ADT	active duty for training	ECS	entry-control system
AMDF	Army Master Data File	ENAC	entrance National Agency Check
AMG	alarm monitor group	ESS	electronic security system
APF	appropriated fund	FM	field manual
AR	Army regulation	FYDP	Future-Year Defense Plan
ASG	area support group	GFE	Government-furnished equipment
AT	annual training	GOV	Government-owned vehicle
ATCOM	United States Army Aviation and Troop Command	GP	German police
ATS	Abrams Tank System	GS	general support
BASOPS	base operations	GSA	General Services Administration
BMM	borrowed military manpower	HN	host nation
BSB	base support battalion	HQDA	Headquarters, Department of the Army
CCTV	closed-circuit television	HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
CID	criminal investigation division	HRP	high-risk personnel
CIDS	commercial intrusion detection system	IC	installation coordinator
CONOPS	United States Army Intelligence Command Continental (United States) Operations	ID	identification
COR	contracting officer's representative	IDS	intrusion detection system
CPSC	civilian personnel service center	IDT	inactive duty training
CPSE	commercial physical-security equipment	IDS MCX	Huntsville Division IDS Technical Center of Expertise
CRC	criminal records check	IG	Inspector General, USAREUR
CSA	USAREUR Civilian Support Agency	IRP	Individual Reliability Program
CSG	Civilian Support Group (Guard)	JA	Judge Advocate, USAREUR
CSUP	Command Security Upgrade Program	JAG	judge advocate general
CTA	common table of allowances	JAWG	joint action working group
DA	Department of the Army	J-SIIDS	joint-services interior intrusion detection system
DCSENGR	Deputy Chief of Staff, Engineer, USAREUR	K&LC	key-and-lock control
DCSIM	Deputy Chief of Staff, Information Management, USAREUR	LN	local national
DCSINT	Deputy Chief of Staff, Intelligence, USAREUR	LOA	letter of agreement
DCSLOG	Deputy Chief of Staff, Logistics, USAREUR	MCA	Military Construction, Army
DCSOPS	Deputy Chief of Staff, Operations, USAREUR	MEVA	mission-essential or vulnerable area
DCSPER	Deputy Chief of Staff, Personnel, USAREUR	MIPR	military interdepartmental purchase request
DCSRM	Deputy Chief of Staff, Resource Management, USAREUR	MOS	military occupational specialty
DEH	director(ate) of engineering and housing	MP	military police
DEROS	date eligible for return from overseas	MSC	major subordinate command
		MTOE	modification table of organization and equipment
		NAC	National Agency Check
		NACI	National Agency Check with written inquiry
		NAF	nonappropriated fund
		NATO	North Atlantic Treaty Organization
		NCOIC	noncommissioned officer in charge
		NSN	national stock number
		ODCSOPS	Office of the Deputy Chief of Staff, Operations, HQ USAREUR/7A

## USAREUR Reg 190-13

ODCSR	Office of the Deputy Chief of Staff, Resource Management, HQ USAREUR/7A
OIC	officer in charge
OMA	Operation and Maintenance, Army
OPA	Other Procurement, Army
OPM	Office of the Provost Marshal, HQ USAREUR/7A
OPORD	operation order
PBO	property book officer
PM	provost marshal
PMCS	preventive maintenance checks and services
POC	point of contact
POF	privately owned firearm
POL	petroleum, oils, and lubricants
POM	program objective management
POMCUS	prepositioned materiel configured to unit sets
POV	privately owned vehicle
PSE	physical-security equipment
PSEMO	physical-security equipment management officer
PWS	performance work statement
RBI	reply-by indorsement
RM	resource management
S&G	Sergeant and Greenleaf
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SDNCO	staff duty noncommissioned officer
SDO	staff duty officer
SJA	staff judge advocate
SMS	Security Management System
SOFA	status of forces agreement
SOP	standing operating procedure
SSN	social security number
TB	technical bulletin
TDA	tables of distribution and allowances
THREATCON	threat condition
TM	technical manual
TTAD	temporary tour of active duty
TÜV	<i>Technischer Überwachungsverein</i>
U.S.	United States
USACCE	United States Army Contracting Command, Europe
USACIDC	United States Army Criminal Investigation Command
USAEDE	United States Army Engineer Division, Europe
USAMC-E	United States Army Materiel Command, Europe
USAREUR	United States Army, Europe

## SECTION II TERMS

### **access**

See DA Physical Security Update.

### **access-control personnel**

Persons whose duties involve screening individuals before entry into a facility. Examples include military police and other types of guard forces, and may also include such people as Army and Air Force Exchange Service employees who check identifications of patrons entering their activities.

### **affiliated civilian**

A DOD civilian employee or family member of a U.S. Forces member who has status under the NATO Status of Force Agreement or supplementary agreements.

### **alarm monitor group (AMG)**

A system consisting of four major components (uninterruptible power supply, converter multiplexer assembly, communication circuit card assembly, and AMG application software). The AMG replaces the monitor cabinets for joint-services interior intrusion detection systems (J-SIIDS). The AMG is designed to receive signals from up to 64 remote areas (zones) and display the location, name, and notes for each zone. The AMG, by means of a computer screen, displays zone status changes by priority, synchronizes automatically with zones, displays intrusion alarms separately from communication alarms, and automatically prints the status report of the various areas.

### **ammunition**

See DA Physical Security Update.

### **area support group (ASG)**

An modification table of organization and equipment organization that exercises command and control over assigned and attached units. The ASG plans and directs provision of selected direct combat service support, general support, supply intermediate general support maintenance, and security within its area of operations. The ASG also plans, budgets, and manages base operations in its area through base support battalions and area support teams.

### **arms**

See DA Physical Security Update.

### **badge**

Identification worn by personnel in a sensitive restricted area. Badges in USAREUR are AE Form 190-13E (Security Badge (Red)), AE Form 190-13F (Security Badge (Green)), and AE

Form 190-13G (Security Badge (Black)). See also DA Physical Security Update.

**base support battalion (BSB)**

An modification table of organization and equipment organization subordinate command of an area support group (ASG). The BSB provides command and control of specific base operations support (such as community family activities, logistics, and engineering, and housing). The BSB has specific areas of responsibility designated by the ASG.

**cable seal lock**

See DA Physical Security Update.

**categories of arms, ammunition, and explosives**

The four security-risk categories (I, II, III, and IV). Minimum security standards are established for each of the categories in AR 190-11, appendix B.

**Civilian Support Group (CSG) guard**

Local national person hired by USAREUR to provide physical security (guard) services. CSG guards are organized into units, called CSGs, which have their own administration and mission. These guards are authorized by tables of distribution and allowances and the CSG to which they are assigned is subordinate to the USAREUR command to which it is assigned.

**constant surveillance**

See DA Physical Security Update.

**controlled area**

See "restricted area" in DA Physical Security Update.

**crime prevention**

The anticipation, recognition, and appraisal of a crime-risk and initiation of some action to remove or reduce it. Crime prevention is a direct crime-control method that applies to before-the-fact efforts to reduce criminal opportunity, protect potential human victims, and prevent property loss. Crime prevention is a commander's program, and is no longer run by the provost marshal.

**crime-prevention survey**

Survey conducted by the United States Army Criminal Investigation Command to detect crime, evaluate the possibilities of easy criminal activity, and identify procedures conducive to criminal activity.

**duress alarm system**

See DA Physical Security Update.

**exception**

A permanent exclusion from specific requirements. Exceptions will be determined individually and involve unique circumstances that make conformance to security standards

impossible or highly impractical. Exceptions in USAREUR will be reviewed every 2 years. Exceptions must go through the Office of the Provost Marshal, HQ USAREUR/7A, and be approved at DA level.

**exclusion area**

See "restricted area" in DA Physical Security Update.

**exclusive use**

See DA Physical Security Update.

**explosives**

See DA Physical Security Update.

**guard post**

A position established as a physical-security measure. A post must have specified orders to cover the responsibilities of the individual staffing the post. Additionally, the hours of the post must be stated and the post must have an identifying designation (such as Post #1). Guardposts must be established for normal operations as well as increased threat condition (THREATCON) levels. When determining manpower requirements for the various threat levels, the sum of individual guardpost requirements provides the total guard requirement.

**high-security padlock**

A key-operated padlock, conforming to military specification MIL-P-43607, designed to resist forced entry and surreptitious entry. High-security padlocks are used with a high-security hasps that meet military specification MIL-H-29181 or MIL-H-24653.

**hot pursuit**

The immediate and continuous pursuit by a law enforcement officer of a person who is fleeing from a recently committed crime.

**independent power source**

A self-contained power source, such as a generator or a battery (normally a battery).

**installation**

A casern, base, station, improved field camp, storage site, training area, firing range, missile or communications site, housing area, shopping area, or separate group of facilities that may be considered by itself and can be designated by appropriate directives.

**intrusion detection system (IDS)**

See DA Physical Security Update.

**joint action working group**

The formation of combatting-terrorism or force-protection committees (AR 525-13); the establishment of physical-security councils (AR 190-16). In USAREUR, these requirements

## **USAREUR Reg 190-13**

are met by the establishment of joint action working groups. The CINCUSAREUR operation order on Force Protection prescribes the composition and duties of a joint action working group. Joint action working groups are required at the area support group and base support battalion levels and will be organized and operated similar to the USAREUR joint action working group.

### **limited area**

See "restricted area" in DA Physical Security Update.

### **major subordinate command**

Command listed in USAREUR Regulation 10-5, appendix A, as a "USAREUR major command" or "USAREUR separate major command."

### **mission-essential or vulnerable area (MEVA)**

Facility or activity within an installation that, because of its functions, is considered by the commander as vital to the successful accomplishment of the installation's mission. MEVAs include areas nonessential to the installation's operational mission, but vulnerable to theft, trespassing, damage, or other criminal activity.

### **nonaffiliated civilian**

A civilian who does not have status under NATO Status of Forces Agreement (SOFA) or supplementary agreement. This includes U.S., German, and other non-U.S. personnel who do not have status under the NATO SOFA or supplementary agreement.

### **physical-security inspection**

A formal, recorded assessment of physical-security measures (procedural and physical) implemented to protect an asset. This inspection is conducted by qualified physical-security specialists according to AR 190-13, paragraph 2-11, and is recorded on DA Form 2806-1-R (Physical Security Inspection Report).

### **physical-security survey**

A formal, recorded assessment of an installation's physical-security program. This survey is conducted by a qualified physical-security specialist (AR 190-13, para 2-10) and recorded on DA Form 2806-R (Physical Security Survey Report). The survey provides the commander an assessment of the overall security posture of the installation, given the threat and mission, and advises the commander on the installation physical-security program's strengths and weaknesses.

### **primary electrical power source**

See DA Physical Security Update.

### **response force**

Personnel designated to respond to alarms. Area support group and base support battalion commanders determine the force's structure, size, and equipment. Forces must be able to arrive on a scene not more than 15 minutes after an alarm is sounded.

### **restricted area**

See DA Physical Security Update.

### **risk analysis**

See DA Physical Security Update.

### **seal**

See DA Physical Security Update.

### **security engineering survey**

The process of identifying, by means of onsite surveys, engineering requirements associated with facility enhancements for physical security and antiterrorism, including intrusion detection system installation. See AR 190-13, paragraph 2-14.

### **Security Management System (SMS)**

An automated information system (part of Military Police Management Information System). The system is used to generate reports of physical-security inspections and surveys, update risk analyses, maintain mission-essential or vulnerable area listings, administer information on waivers and exceptions, and provide for automated management of physical-security administration. Hardware requirements include an IBM-compatible 286 or higher with a minimum of 640 kilobyte random access memory. Software requirements include an MS-DOS operating system, version 3.31 or higher, and SMS program software.

### **storage site**

Static placement (temporary or long-term) of arms, ammunition, and explosives. Storage does not include items in the process of being manufactured, used, researched, developed, tested, or evaluated; nor items being transported to a place of storage or use.

### **temporary restricted area**

See "restricted areas" in DA Physical Security Update.

### **threat condition (THREATCON)**

A level of terrorist threat to U.S. military facilities and personnel. There are four THREATCONs in USAREUR: alpha, bravo, charley, and delta. (See AR 525-13 and the CINCUSAREUR operation order on Force Protection.)

### **waiver**

See DA Physical Security Update.

**INDEX**

This index is organized alphabetically by topics and subtopics. Topics and subtopics are identified by paragraph number.

**Access mode (IDS), 6-22b(2)**

**Access roster (IDS maintenance), 6-29b**

**Alternate installation-access procedures, 4-8**

**Barred (persons) from installations, 4-11**

**Borrowed military manpower (BMM), 7-5d, 7-12c(1)**

**Civilian personnel service center (CPSC), 7-5e, 7-7d, 7-8a(2), 7-12d**

**Civilian Support Agency (CSA), 7-5b**

**Civilian Support Agency guards, 7-5b, 7-8b(3), 7-10b(1), 7-11b(3), 7-12c(2), 7-12e**

**Commercial intrusion detection systems (CIDS), 6-3b**

**Contract guards, 7-5c, 7-8a(1), 7-10b(2), 7-12c(2)**

**Contracting officer's representative (COR), 7-8(4), 7-14b**

**Daily log (IDS), 6-23a**

**Drug screening, 7-9**

**Duress procedures, 6-22d**

**Entry-authorization documents, 4-3**

**Essential warfighting facilities, 3-4**

**Evaluations, 7-14**

**Forecasting of IDS PSE projects, 6-6**

**German police, 4-13**  
     **Entry to restricted areas, 4-13d**

**Guards:**  
     **Arming of Guards, 5-5b**  
     **Authority, 7-4**  
     **Orders, 7-13**  
     **Standards, 7-7**  
     **Training, 7-10**  
     **Uniform and equipment, 7-7f, 7-11, 7-16b(3)**  
     **Use of force, 7-10c(9), 7-13b(2)**

**Huntsville IDS Technical Center (IDS MCX), 6-8b, 6-20d**

**Identification cards, passes, and badges:**

**Accountability, 4-5d**  
     **Confiscating, 4-10**  
     **Disposition Procedures, 4-5d**  
     **Issuing Authority, 4-5**  
     **Requisitioning, 4-4**

**Individual property passes, 4-14**

**Individual Reliability Program, 7-8**

**Intrusion detection system (IDS):**

**Movement of components/systems, 6-32**  
     **Planning guidelines for, 6-3**  
     **System failure when storing AA&E, 5-5b**  
     **Requirements for AA&E, 5-5**  
     **Response force, 5-5c, 6-26d**

**Inventory and accountability of AA&E, 5-4**

**Joint action working group (JAWG), 2-6a**

**Key and lock control (K&LC):**

**For AA&E, 5-6**  
     **For IDS keys, 6-30**  
     **Maintenance keys for high-security padlocks, 5-6c**  
     **Spare keys for AA&E, 5-6b**

**Life-cycle (J-SIIDS), 6-6e**

**Major Construction, Army (MCA), projects, 6-3c**

**Military police, 7-8a**

**Missing and recovered AA&E, 5-7**

**Mission-essential or vulnerable area (MEVA), 2-9**

**National Agency Check (NAC), 6-21a**

**North Atlantic Treaty Organization (NATO) projects, 6-3d**

**Passes:**

**Pass-control procedures, 4-5d**  
     **Pass-issuing authorities, 4-5**  
     **Permanent passes, 4-6**  
     **Restricted-area badges, 4-9**  
     **Temporary passes, 4-7**

**Performance work statement (PWS), 7-7c**

**Periodic operational checks, 6-28**

## **USAREUR Reg 190-13**

**Personnel suitability and reliability checks, 6-21a**

**Physical-security councils (see JAWG), 2-12**

**Physical-security inspection, 2-14**

**Physical-security plan (ASG/BSB) database, 6-13c**

**Physical-security program:**  
    **Objectives, 2-2**  
    **Components, 2-3c; chap 2, sec II**

**Physical-security survey, 2-14**

**Preventive maintenance checks and services (IDS), 6-24c**

**Project request packet (J-IIDS), 6-9**

**Project request packet (commercial EES), 6-10**

**Restricted areas, 2-10**

**Risk analysis, 2-8, para 6-5**

**SCIIFS (IDS requirements), 6-1d**

**Secure mode (IDS), 6-22b(1)**

**Security measures, 2-13**

**Security standards, 3-2a, app C**

**Sensors for IDS, 6-15**

**Signs (bilingual IDS), 6-31**

**Site survey (IDS), 6-8a**

**Specified-country citizens, 4-12**

**Structure standards (AA&E), 5-2**

**Technical review (IDS purchase, lease, or lease renewal), 6-11a**

**Test/reset mode (IDS), 6-22b(3)**

**Transition and sustainment facilities, 3-5**

**Transporting AA&E, 5-8**

**Unit-level maintenance (IDS), 6-24a**

**Unserviceable IDS equipment (nonexpendable), 6-25d**

**Use of force, 7-10c(9), 7-13b(2)**

**Waivers and exceptions (AA&E), 5-3, app E**