

Headquarters
United States Army Europe
Wiesbaden, Germany

Army in Europe
Regulation 190-13*

Headquarters
United States Army Installation Management Command,
Europe Region
Sembach, Germany

4 February 2014

Military Police

USAREUR Physical Security Program

***This regulation supersedes AE Regulation 190-13, 23 October 2003.**

For the Commander:

JAMES B. MINGO
Colonel, GS
Chief of Staff

Official:



DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation—

- Establishes the USAREUR and IMCOM-Europe Physical Security Program. This program is part of the Antiterrorism/Force Protection Program, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, HQ USAREUR.
- Provides supplemental guidance to Department of the Army physical security publications.
- Must be used with AR 190-5, AR 190-11, AR 190-13, AR 190-14, AR 190-16, AR 190-51, DA Pamphlet 190-51, AE Regulation 190-16, and AE Regulation 525-13.

Summary of Change. This revision completely revises the previous edition of the regulation.

Applicability. This regulation applies to USAREUR major subordinate and specialized commands (AE Reg 10-5, app A) (including U.S. Army tenant units in USEUCOM that are subject to local requirements) and IMCOM-Europe.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are on the Army Records Information Management System website at <https://www.arims.army.mil>.

Supplementation. Commanders will not supplement this regulation without approval of the Provost Marshal Division (PMD), G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, HQ USAREUR (AEOP-PDP-SO).

Forms. This regulation prescribes AE Form 190-13H(G), AE Form 190-13H(I), AE Form 190-13I, and AE Form 190-13L. AE and higher level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at <https://aepubs.army.mil/>.

Suggested Improvements. The proponent of this regulation is the PMD, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, HQ USAREUR (AEOP-PDP-SO). Users may suggest improvements to this regulation by sending DA Form 2028 to the PMD (AEOP-PDP-SO), Unit 29351, APO AE 09014-9351.

CONTENTS

CHAPTER 1 INTRODUCTION

- 1-1. Purpose
- 1-2. References
- 1-3. Explanation of Abbreviations
- 1-4. Responsibilities

CHAPTER 2 USAREUR PHYSICAL SECURITY PROGRAM

- 2-1. General
- 2-2. Threat Assessment
- 2-3. Physical Security Planning
- 2-4. Physical Security Plan
- 2-5. Standing Operating Procedures
- 2-6. Mission-Essential Vulnerable Areas
- 2-7. Restricted Areas
- 2-8. Physical Security Surveys
- 2-9. Physical Security Inspections
- 2-10. Reports of Corrective Action
- 2-11. Report Classification
- 2-12. Security Criteria Deviation Process
- 2-13. Security Engineering Surveys
- 2-14. New Construction and Major Renovations
- 2-15. Physical Security Credentials
- 2-16. USAREUR G34 Physical Security Management System

CHAPTER 3 SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

- 3-1. Purpose
- 3-2. General

- 3-3. Access Control Rosters
- 3-4. Key-and-Lock Control of AA&E
- 3-5. Consolidated Arms Rooms
- 3-6. Armed Guard Requirements
- 3-7. Electronic Security System (ESS)
- 3-8. Storage and Supplemental Controls
- 3-9. Control of Weapons
- 3-10. Protection of Missiles, Rockets, Ammunition, and Explosives at Unit Level
- 3-11. Weapons and Ammunition Inventories
- 3-12. Reporting Missing or Recovered AA&E
- 3-13. Privately Owned and Commercial Weapons and Ammunition
- 3-14. Training
- 3-15. In-Transit Security of AA&E

CHAPTER 4

ACCESS CONTROL

- 4-1. Additional Access-Control Point (ACP) Guidance
- 4-2. Investigating and Adjudicating ACP Installation Barrier Incidents

CHAPTER 5

SECURITY OF ARMY PROPERTY AT UNIT AND INSTALLATION LEVEL

- 5-1. General
- 5-2. Communications Security (COMSEC) Material and Controlled Cryptographic Items
- 5-3. Security of U.S. Army Issued Bayonets

CHAPTER 6

PHYSICAL SECURITY EQUIPMENT (PSE)

- 6-1. General
- 6-2. Program Management
- 6-3. Closed-Circuit Television (CCTV)
- 6-4. Electronic Entry/Access Control Systems
- 6-5. ESS Personal Identification Numbers
- 6-6. Maintenance of ESS
- 6-7. Personnel Suitability and Reliability Checks
- 6-8. Movement of ESS Components and Systems
- 6-9. ESS Inspections
- 6-10. Response to Alarms

CHAPTER 7

USAREUR CONTRACT GUARD PROGRAM

CHAPTER 8

USAREUR G34 STAFF ASSESSMENT VISIT (SAV) PROGRAM

- 8-1. Purpose
- 8-2. Security Operations and Assessments Branch

- 8-3. Operational Inspection and SAV Programs
- 8-4. Physical Security Inspection and SAV
- 8-5. USAREUR Contract Guard SAV
- 8-6. Required SAV Actions (Physical Security)
- 8-7. Required SAV Actions (Contract Guard Program)

CHAPTER 9

USAREUR SECURITY EQUIPMENT WORKING GROUP (SEWG)

- 9-1. General
- 9-2. Policy
- 9-3. Definition of Nonstandard Equipment
- 9-4. SEWG Responsibilities
- 9-5. Program Management

Appendixes

- A. References
- B. Guidelines for Developing Installation Barrier Plans
- C. Sample Format for Physical Security Standing Operating Procedure

Figures

- 3-1. Request for Medical Records Check
- 3-2. Request for Personnel Records Check
- 3-3. Request for DES/PM or Security Office Records Check
- 3-4. Sample Arms Room Unaccompanied-Access Roster
- 3-5. Format of Appointment Memorandum for Record for Primary or Alternate AA&E Key Custodian
- 3-6. Bilateral Storage Agreement for Consolidated Arms Room
- 6-1. Format for Requesting Non-Army or Non-USAREUR Standard ESS
- B-1. Sample Matrix
- B-2. Sample Drawing Showing Number and Type of Barriers

Glossary

CHAPTER 1

INTRODUCTION

1-1. PURPOSE

This regulation—

- a. Describes physical security (PS) requirements prescribed by regulatory sources.
- b. Prescribes support documentation and records that each unit must maintain.
- c. Is a tool that commanders may use to manage their PS programs effectively.

1-2. REFERENCES

Appendix A lists references.

1-3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

1-4. RESPONSIBILITIES

Commanders have an inherent PS responsibility for their commands. This responsibility will not be delegated or transferred, except by official orders.

a. Provost Marshal (PM), G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, HQ USAREUR. The USAREUR PM is the proponent for and will exercise staff supervision over the USAREUR PS Program. The USAREUR PM will—

(1) Establish a USAREUR PS Program and monitor policy to ensure the procedures outlined in chapter 6 are followed regarding the issue, purchase, lease, and lease renewal of physical security equipment (PSE).

(2) Provide an advisory member (major, GS-12, or above) to the Army Physical Security Equipment Action Group (APSEAG). A designated representative from IMCOM-Europe may be invited to attend as appropriate.

(3) Maintain proponency for the USAREUR Contract Guard Program throughout USAREUR's forward-deployed locations and provide technical assistance to tactical commanders on all aspects of contract-guard requirements in a deployed area of responsibility (AOR). This includes developing and publishing a standard performance work statement (PWS) for contract guard services in the European theater for tactical environments. IMCOM-Europe will continue to manage the USAREUR Contract Guard Program at all United States Army garrisons (USAGs) and installations.

(4) Conduct inspections of security guard programs in the European theater's deployed AOR to ensure compliance with USAREUR Contract Guard Program requirements and policy according to this regulation and the USAREUR contract guard PWS.

(5) Establish a security staff assessment visit (SAV) program to evaluate and help commanders execute PS programs.

(6) Support the United States Army Criminal Investigation Command (USACIDC) and provide guidance on using the High-Risk Personnel (HRP) Program for USAREUR.

(7) Manage the Installation Access Control System (IACS) for USAREUR.

(8) Appoint a civilian career program manager for PS personnel (CP 19), pay plan GS, occupational code 0080.

b. USAREUR G3/5/7. The USAREUR G3/5/7 will assist and support—

(1) Procurement and maintenance of electronic security systems (ESSs) for contingency operations. Requests for nonstandard force protection/physical security (FP/PS) equipment must be sent through the USAREUR Security Equipment Working Groups (SEWG) for review and to the USAREUR PM for approval.

(2) Obtaining funding for procurement and sustainment costs for ESSs, including all appropriate supporting documents and approvals.

c. USAREUR G6. The USAREUR G6 will use information provided by IMCOM-Europe and USAREUR-assigned units and USAREUR major subordinate and specialized commands to identify the number and locations of ESSs and establish policy and procedures to ensure dedicated communication lines are available to support ESS requirements throughout the European theater.

d. USAREUR G8. The USAREUR G8, in coordination with the ACoS, G8, IMCOM-Europe, will secure funding to support USAREUR and IMCOM-Europe PS program requirements.

e. Director, IMCOM-Europe. The Director, IMCOM-Europe, will—

(1) Use this regulation and all applicable DOD and DA regulations, pamphlets, and directives as the basis for developing the IMCOM-Europe PS Program.

(2) Conduct physical security inspections (PSIs) of tenant units and USAREUR-assigned units and tenant commands to ensure compliance with AR 190-13 and this regulation. The Director, IMCOM-Europe, will report findings to the Security Operations and Assessment Branch (SOAB), Provost Marshal Division (PMD), G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, HQ USAREUR, on the SharePoint portal website at <https://intranet.eur.army.mil/hq/g34/pmd/sitepages/home.aspx> within 14 days of the PSI.

(3) Ensure IMCOM-Europe PS personnel coordinate the design criteria of new construction projects. PS personnel will review all plans and specifications during every step of the planning, design, and construction process. All new plans will be sent to the Director, IMCOM-Europe (IMEU-OPD), for final coordination with the PMD before implementation.

(4) When requested, provide an advisory member (major, GS-12, or above) to the APSEAG.

(5) Review requests for waivers and exceptions to policy, and make recommendations. The Director, IMCOM-Europe, will send requests to the PMD (AEOP-PDP-SO) for final review and before submission to the HQDA approval authority for final decision.

(6) Manage the IMCOM-Europe Contract Guard Program and provide technical expertise to commanders on all aspects of security guard requirements.

(7) Nominate for appointment a contracting officer's representative (COR) to manage the daily execution of contract guard service contracts that are funded and centrally managed by IMCOM-Europe.

(8) In coordination with the PMD, conduct inspections of security guard programs in the European theater to ensure compliance with USAREUR policy according to this regulation and the USAREUR contract guard PWS.

(9) In coordination with the PMD, establish and implement a security staff assistance program to evaluate and help commanders execute PS programs.

(10) In coordination with the PMD, conduct command compliance inspections of PS programs in the IMCOM-Europe theater of operations to ensure these programs comply with regulatory requirements.

(11) Procure and maintain ESSs for USAGs and installations. Requests for nonstandard FP/PS equipment will be sent through the USAREUR SEWG for review and to the USAREUR PM for approval.

(12) Provide funding for procurement and sustainment costs for ESSs, ensuring that requests include all appropriate supporting documents and approvals.

f. ACoS, G4, IMCOM-Europe. The ACoS,G4, IMCOM-Europe, will—

(1) Coordinate the review of all USAREUR and IMCOM-Europe level planning documents and construction plans and specifications at all stages of their development with the PMD.

(2) Ensure installation planning boards include a PS representative from the local directorate of emergency services (DES) or security office as a voting member on all actions. These representatives will ensure that provisions of this regulation and other security-related publications are considered during PS planning.

(3) Develop policy and procedures to ensure that local PS representatives have reviewed every PS and force-protection project request (DA Form 4283) and that PS recommendations are included in the project before final approval or execution.

(4) Provide ESS maintenance services by establishing an IMCOM-Europe level ESS installation, training, and maintenance contract to support ESS program requirements.

(5) Appoint a COR to manage and provide oversight for the installation, training, and maintenance of PS-related contracts.

g. Commanders of USAREUR Major Subordinate and Specialized Commands. Commanders of USAREUR major subordinate and specialized commands will—

(1) Provide appropriate command emphasis to the USAREUR PS Program.

(2) Ensure security programs safeguard personnel, facilities, equipment, operations, and materiel during mobilization and war.

(3) Appoint (in writing) a physical security officer (PSO) for each battalion and higher-level unit. The PSO must—

(a) Attend the USAREUR Physical Security Course within 6 months after being assigned the position.

(b) Log on to the Defense Security Service website at <http://www.cdse.edu/stepp/index.html> within 90 days after being appointed and complete the following training:

1. Introduction to Physical Security (PY011.06).

2. Lock and Key Systems (PY104.16).

3. Physical Security Measures (PY103.16).

(c) Send the certificates of training (b₁ thru 3 above) through the higher headquarters PSO and enter the information in the USAREUR Physical Security Management System (PSMS).

(4) Conduct command PS inspections in accordance with AR 190-13 and identify PS requirements of subordinate command activities.

(5) Ensure subordinate units and activities that receive “not adequate” ratings on PS inspection reports submit reports of corrective actions within 30 calendar days after the inspection. Reports must be submitted to the inspecting agency or activity and uploaded into the Security Management System (SMS) for tracking and recordkeeping.

(6) Ensure a PS representative participates in the Antiterrorism Working Group (ATWG).

(7) Ensure all elements of their command comply with this regulation when executing their PS program, and use the USAREUR standardized checklists (<https://intranet.eur.army.mil/hq/g34/pmd/sitepages/home.aspx>) and references listed in this regulation.

(8) Review subordinate PS plans annually and document them accordingly.

(9) Ensure PS plans provide for proper protection and security for both Government and personal property left behind when units deploy.

(10) Ensure resources required for PS are identified to the servicing USAG, as appropriate.

(11) Coordinate with IMCOM-Europe when design criteria for new construction projects are developed. Commanders of USAREUR subordinate and tenant commands will also ensure that servicing PS personnel review all plans and specifications at every step of the planning, design, and construction process.

(12) Ensure ESS requirement coordination is made with the USAG director of emergency services/provost marshal (DES/PM) for monitoring services before any system is procured to ensure system compatibility with existing monitoring systems.

(13) Conduct a risk analysis according to DA Pamphlet 190-51 for all facilities (planned and existing) that are designated or likely to be designated as mission-essential vulnerable areas (MEVAs).

(14) Ensure that requirements for ESS and monitoring services are coordinated with the local USAG DES/PM and the servicing information management office for communication support.

h. 21st Theater Sustainment Command (21st TSC). The 21st TSC will serve as the USAREUR proponent agency for the development and execution of the transportation of arms, ammunition, and explosives (AA&E), and classified shipments.

i. Commanders of Units Transporting AA&E. Commanders of units transporting AA&E will coordinate the movement with the Provost Marshal Office, 21st TSC (AETS-OPM), and ensure that the movement is in compliance with the security requirements outlined in the following references:

(1) DOD Manual 5100.76, enclosure 9, paragraphs 7 and 8, and enclosure 10.

(2) DTR 4500.9-R, part II, chapter 205, paragraph M.

(3) ATTP 3-39-32, chapter 10.

(4) AR 190-11, chapter 7, paragraphs 7 to 10.

(5) USAREUR TASKORD 12-0260.

(6) USAREUR GENADMIN Message No. 1205094, Security, Storage, and Transportation of Category I and II Ammunition.

(7) AE Regulation 55-4, section IV, paragraphs 29 to 36.

j. Commanders of Non-USAREUR Tenant Commands and Activities. Commanders of non-USAREUR tenant commands and activities will—

(1) Ensure PS interests are represented in the ATWG process and other planning processes.

(2) Ensure elements of their command, unit, or activity comply with and use this regulation when executing their PS program.

(3) Appoint a PS representative in writing who will develop and oversee the overall PS program.

(4) Develop and publish a unit or organization PS plan.

(5) Coordinate PS plans once each year with the supporting USAG DES/PM office to ensure their security procedures are consistent with current requirements and directives.

(6) Ensure resources required for PS are identified to the servicing DES/PM office.

(7) Coordinate with the servicing USAG directorate of public works (DPW) and PS personnel from the servicing DES/PM office when design criteria for new construction projects are formulated. Commanders of non-USAREUR tenant commands and activities are responsible for ensuring that servicing PS personnel review all plans and specifications during every step of the planning, design, and construction process.

(8) Coordinate with the servicing DES/PM office for ESS and monitoring services, and coordinate with the servicing director of information management before any system is procured to ensure that the system is compatible with existing monitoring systems.

(9) Send requests identifying PS-support requirements for Government-owned, contractor-operated facilities unable to support these requirements to the next higher headquarters or the supporting USAG, as appropriate.

k. USAG Commanders. USAG commanders are responsible for the PS programs of their communities as directed by IMCOM-Europe. USAG commanders will—

(1) Ensure unit commanders identify and approve MEVAs in writing and revalidate the consolidated MEVA list each year.

- (2) Appoint a PSO in accordance with AR 190-13, chapter 3, paragraph 3-1.
- (3) Ensure a member of the DES/PM PS section is an active participant in the ATWG process.
- (4) Ensure all elements of their command comply with and use this regulation when executing their PS program.
- (5) Ensure command inspections and PS SAVs are conducted to evaluate supported command activities, installations, and facilities.
- (6) Review supported command PS plans each year.
- (7) Standardize and synchronize PS requirements, plans, training, and operations in their AOR.
- (8) Ensure rear-detachment PS plans include provisions for continuing PS protection of unit and personal assets left behind when tenant units deploy in accordance with AR 190-11, AR 190-13, AR 190-51, and all other applicable regulations and directives.
- (9) Ensure supported units and activities that receive “not adequate” ratings on PS inspection reports submit reports of corrective actions within 30 calendar days after the inspection. Reports must be submitted to the inspecting agency or activity and uploaded into SMS for tracking and recordkeeping.
- (10) Coordinate with the servicing USAG DES/PM and servicing signal battalion for ESS monitoring services and support before systems are procured to ensure that systems are compatible with existing monitoring systems and regulatory requirements.

I. USAG DES/PM. The USAG DES/PM will—

- (1) Assess installation PS needs by conducting PS surveys and inspections in accordance with AR 190-13, chapter 1, paragraph 1-26, and chapter 2, paragraphs 2-14 and 2-15.
- (2) Ensure supported units and activities that receive “not adequate” ratings on PS inspection reports submit reports of corrective actions within 30 calendar days after the inspection. Reports must be submitted to the inspecting agency or activity and uploaded into SMS for tracking and recordkeeping.
- (3) Provide weekly updates to the PMD and the IMCOM-Europe DES on PS issues that are of interest to the USAREUR Command Group.
- (4) Keep copies of and monitor all waivers and exceptions to PS requirements for units and activities in their AOR.
- (5) Help prepare and review requests for exceptions and waivers to current HQDA and USAREUR PS policy and procedures.
- (6) Ensure the standard PS inspection checklists posted on the SOAB SharePoint portal website at <https://intranet.eur.army.mil/hq/g34/pmd/sitepages/home.aspx> are used to conduct PS inspections.

(7) Serve as the proponent and subject-matter expert to commanders on all aspects of the Command Security Guard Force Program. The USAG DES/PM will also develop, implement, and manage local security guard programs as directed by higher authorities.

(8) Designate qualified quality assurance evaluator personnel in writing to help site contracting officer's representatives (SCORs) implement the Contract Guard Quality Assurance Program. The USAG DES/PM should consider using military police (MP) supervisory personnel to routinely check contract guard posts to ensure all required guard posts are properly manned and operated.

m. Company- and Detachment-Level Commanders of Units and Activities. Commanders of units and activities will—

(1) Ensure all elements of their unit or activity comply with this regulation when executing their PS programs.

(2) Apply all requirements according to AR 190-11, AR 190-13, and AR 190-51.

(3) Coordinate PS requirements with their higher headquarters.

(4) Coordinate PS requirements once each year with the supporting USAG DES/PM office to ensure their security procedures are consistent with current requirements and directives.

(5) Maintain a copy of the servicing USAG's PS plan. Commanders will direct subordinate units to maintain a copy of the host organization's PS plan if the units are tenants of a different command.

(6) Designate and approve restricted areas in writing and provide this information to the higher headquarters PSO and USAG DES/PM.

(7) Ensure serious incident reports (SIRs) are submitted in a timely manner according to AE Regulation 190-45 and all USAREUR and USEUCOM directives concerning SIR reporting.

(8) Ensure that key custodians have written appointment orders specifying their responsibility to issue and receive keys and maintain accountability for office, unit, or activity keys in accordance with AR 190-51. Commanders of units and activities are also responsible for developing and maintaining a unit key-and-lock control standing operating procedure (SOP).

(9) Review inspection and survey reports received from inspecting agencies and ensure that corrective actions are taken for reported deficiencies within the timeframes outlined in this regulation.

(10) Ensure that personnel meet training and certification requirements before they are armed to perform armed guard duties.

(11) Ensure that deploying personnel are briefed on in-transit security requirements.

n. Commander, 5th Military Police Battalion (CID). The Commander, 5th Military Police Battalion (CID), will—

(1) Provide appropriate, threat-related criminal information to the local DES/PM and the PMD.

(2) Plan and coordinate personal protective services for DOD and DA officials as directed by HQDA.

(3) Ensure personal security vulnerability assessments (PSVAs) are completed for all personnel designated as HRP level 1 and 2.5 or as directed by DOD.

(4) Establish procedures to ensure appropriate liaison between the USACIDC, the United States Army Intelligence and Security Command (USAINSCOM), USAG DES/PMs, and USAREUR G34 FP/PS officers operating in support of the USAREUR PS Program.

(5) Immediately notify the affected USAG DES/PMs, the servicing FP/PS officer, and the CG, USAREUR, on receipt of time-sensitive threat information.

(6) Provide a copy of USACIDC initial and final reports on terrorist acts to the USAREUR G2, USAREUR G3/5/7, PMD, and the Director, IMCOM-Europe.

(7) Immediately provide terrorist-related criminal information to local military intelligence detachments, USAREUR G2, PMD, and the Director, IMCOM-Europe.

o. Commander, 66th Military Intelligence Brigade. The Commander, 66th Military Intelligence Brigade, will—

(1) Provide appropriate threat-related information to local or affected USAG DES/PMs and the PMD.

(2) Ensure PSVAs are completed for all personnel designated as HRP level 1 and 2.5 or as directed by DOD.

(3) Establish procedures to ensure appropriate liaison among the USACIDC, USAINSCOM, USAG DES/PM, and USAREUR G34 antiterrorism/force protection (AT/FP)/PS officers operating to support the USAREUR PS Program.

(4) Immediately notify the affected USAG DES/PM, the servicing FP/PS officer, and the CG, USAREUR, on receipt of time-sensitive threat information.

p. PSOs at USAGs and Tenant Units and Activities. PSOs at USAGs and tenant units and activities will—

(1) Implement their unit PS program in accordance with this regulation and other applicable directives, as appropriate.

(2) Write and implement their unit PS plan and security SOPs for the inspecting activity or agency.

(3) Validate compliance with all PS regulations, policy, and programs.

(4) Keep the commander informed of PS issues.

(5) Coordinate PS training for the command.

- (6) Help prepare the USAG PS plan.
- (7) Provide input to the USAG PS and antiterrorism-funding processes.
- (8) Manage and provide oversight to the unit's key-and-lock control program.

CHAPTER 2

USAREUR PHYSICAL SECURITY PROGRAM

2-1. GENERAL

PS is a critical part of the USAREUR Force Protection Program. PS measures are designed to detect, deter, delay, and defend against threats to the U.S. Forces. PS measures are a combination of active and passive systems, devices, and security personnel. Measures may be physical (for example, barriers, fences, lights, walls), electronic (for example, alarms, cameras, electronic entry/access control systems (EECSs)), and procedural (for example, inspections and surveys, property inventory and accountability procedures, security checks, security training and awareness programs). A successful PS program cannot be achieved without appropriate command emphasis and the cooperation of every element of a commander's staff. PS personnel must be fully engaged in and remain active participants in the USAREUR PS Program. This chapter—

- a. Implements the U.S. Army regulatory requirements for commanders and directors to establish a PS program.
- b. Prescribes policy and procedures and assigns responsibility for developing a practical and effective PS program in support of USAREUR OPORD 0040-13.

2-2. THREAT ASSESSMENT

PS programs must be tailored to meet local needs. A key element of this process is assessing the local threat. Installations and their equivalents will develop a local threat statement. This statement will identify local threats and make full use of investigative resources available in the geographic area to anticipate criminal and intelligence activities that threaten the security of U.S. Forces property and personnel. The PS threat assessment will be taken from the overall force protection (FP) threat statement. The local threat statement must be included in the installation PS plan.

2-3. PHYSICAL SECURITY PLANNING

a. Commanders at all levels must plan for the security of assets under their control. PS plans will combine security measures and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. Plans must include realistic, reasonable, and affordable protective measures. Requirements at different force protection conditions (FPCONs) must be identified. More guidance is provided in AR 190-13, paragraph 2-12, and AR 190-13, appendix B.

b. PS planning includes—

- (1) Coordinating with installation PS, FP, engineer, and information management personnel to ensure that all requirements are identified and responsibilities are assigned.
- (2) Ensuring that vulnerability assessments and site security surveys are conducted.

(3) Prioritizing the resources critical to performing the command's mission.

(4) Identifying and establishing minimum PS standards for protecting MEVAs.

(5) Designing ESSs to reduce vulnerability to potential or credible threats, and to reduce vulnerabilities and reliance on fixed security forces.

(6) Training security forces at facilities or sites to defend against and respond to threats to the U.S. Forces.

(7) Identifying requirements that cannot be met due to a lack of resources or manpower.

(8) Coordinating and maintaining liaison with the host nation (HN) and other nonorganic or assigned security forces.

(9) Ensuring planned reactive measures are established and guidance is provided in writing for the following:

(a) Bomb threats.

(b) Civil disturbances.

(c) Consequence management.

(d) Increased FPCONs.

(e) Intrusion or mass-notification alarms.

(f) Natural disasters.

(g) Other contingencies that would seriously affect the ability of personnel to perform their mission.

(10) Maintaining barriers that control access to installations or other areas.

(11) Predesignation and prepositioning personnel, equipment, and other resources used to enforce restricted access and respond to incidents.

(12) Exercising contingency plans to validate their effectiveness.

2-4. PHYSICAL SECURITY PLAN

a. Commanders will develop and maintain an installation PS plan and include it as an annex to their AT/FP plan. The PS plan will be developed according to AR 190-13, paragraph 2-12, and follow the format and include the content outlined in AR 190-13, appendix B. PS plans must incorporate elements of a comprehensive PS program (for example, access control, barriers, guard forces, key-and-lock control, lighting). PS plans will include tenant activities, DOD elements, and personnel over which the commander has AT/FP responsibility.

b. The USAG commander is responsible for coordinating PS plans for units and activities in the AOR. PS plans will—

- (1) Assign responsibilities and establish procedures.
- (2) Address contingency procedures for when a unit that is assigned a specific task is deployed.
- (3) Address changes in requirements at higher FPCONs.
- (4) Ensure subordinate and tenant activity plans integrate with and complement the installation plan.
- (5) Be reviewed annually to evaluate the plan's effectiveness and validity.

c. Appendix B provides guidance on barriers and developing installation barrier plans.

2-5. STANDING OPERATING PROCEDURES

SOPs will address unique security requirements and procedures. Unit commanders and heads of activities must approve SOPs before they can be implemented. Appendix C provides a sample format for unit PS SOPs.

2-6. MISSION-ESSENTIAL VULNERABLE AREAS

MEVAs consist of equipment, property, and facilities that have been recommended by the DES/PM and approved by the garrison commander as requiring additional protection through the application of increased PS measures, procedures, and equipment. A list of mandatory sites that are required to be designated as MEVAs is in AR 190-13, chapter 2-7.

a. MEVAs are not the same as high-risk targets (HRTs) (for example, high-density targets (HDTs)) or high-value targets (HVTs), but an HRT, HDT, or HVT may be designated as an MEVA.

b. The USAG DES/PM will rank MEVAs based on the results of the risk analysis, existing security measures, and threat analysis.

c. Garrison commanders will review the MEVA list annually and approve all MEVAs applicable to their installations and areas of operation.

d. The USAG DES/PM will consolidate approved MEVA lists and send them to the Director, IMCOM-Europe, with an information copy to the PMD by 1 September each fiscal year.

2-7. RESTRICTED AREAS

A restricted area is an area or facility that is either required by regulation or identified by the commander as requiring additional security and access controls to restrict access to classified information and other DOD assets.

a. **Categories of Restricted Areas.** AR 190-13, glossary, section II, provides a complete list of the types of restricted areas and their definitions.

b. Designation of Restricted Areas.

(1) When conditions warrant, commanders and heads of organizations will designate restricted areas in writing to protect classified information and safeguard property or material for which they are responsible.

(2) Installation tenant units and activities will provide a list of designated restricted areas to the installation commander for planning purposes.

(3) When required, physical safeguards will be installed to deter unauthorized persons or deny them access to restricted areas.

(4) Commanders designating restricted areas for the protection of classified information will coordinate with the USAREUR G2 (AEIN-SAP).

c. Posting Restricted Areas. Restricted area warning signs will be posted in accordance with AR 190-13, chapter 6.

2-8. PHYSICAL SECURITY SURVEYS

PS surveys will be conducted in accordance with guidance in AR 190-13, chapter 2, paragraph 2-14, and this regulation.

2-9. PHYSICAL SECURITY INSPECTIONS

a. PS inspections will be conducted in accordance with AR 190-13, paragraph 2-15, and this regulation. The SMS will be used to document and analyze inspection results. If the SMS is not available, DA Form 2806-1 will be used to record the inspection. Units that do not have SMS capability will notify their servicing information assurance (IA) or information management officer and request assistance in resolving any compatibility issues involved. If required, further assistance should be requested from IMCOM-Europe (IMEU-OPD).

b. PSIs will be conducted every 2 years for highly sensitive, sensitive, or nonsensitive information system (IS) service center activities or facilities servicing multiple customers. Inspections of all other IS activities or facilities not classified as critically sensitive will be incorporated into scheduled PS inspections of the individual activity or facility.

c. Courtesy inspections will not be conducted in place of inspections required by regulation.

d. To discourage last-minute cancellations and schedule changes due to lack of preparation, requests to change the date of a scheduled inspection must be approved by the organization's next higher commander.

e. PS inspectors will give units and activities a verbal outbriefing after the inspection if deficiencies were found during the inspection.

f. Deficiencies noted during the inspection that are corrected on the spot will be identified on the inspection report as an observation only. Recurring findings will be reported on future PS inspections until the deficiency is corrected.

g. When a deficiency is identified, the unit or activity commander will correct it immediately or use adequate compensatory measures until the deficiency can be corrected. Compensatory measures must provide an equal or greater degree of security than the standard requirement.

h. Paper or electronic copies of PSI reports will be uploaded to the USAREUR PSMS in accordance with paragraph 2-16.

i. The USAG DES/PM will send completed inspection reports by e-mail to the inspected unit within 5 workdays after the inspection and send a paper copy within 15 workdays after the inspection. If a unit or activity receives two “not adequate” ratings in a row, the inspecting agency will send a copy of the report to IMCOM-Europe (IMEU-OPD) and an information copy to the PMD.

2-10. REPORTS OF CORRECTIVE ACTION

Reports of corrective action will be provided to recipients identified in AR 190-13, chapter 2, paragraph 2-15 e(1) through (3).

2-11. REPORT CLASSIFICATION

The results of a survey, inspection, or assessment often identify critical deficiencies or vulnerabilities in an installation or facility PS program. Therefore, the reports will be classified according to AR 190-13, paragraph 2-17. Reports of completed inspections or surveys will be classified and safeguarded according to DOD 5200.1-R and AR 380-5, as appropriate.

2-12. SECURITY CRITERIA DEVIATION PROCESS

Requests for waivers and exceptions to PS requirements will be—

a. Coordinated through the servicing USAG DES/PM office and with the USAG DPW when requesting a waiver or exception to structural deficiencies.

b. Forwarded by the servicing USAG DES/PM office through the PMD to IMCOM-Europe (IMEU-OPD-PS).

c. Submitted in standard memorandum format with AE Form 190-13L. AE Form 190-13L must include a complete justification and the compensatory measures that are in effect.

2-13. SECURITY ENGINEERING SURVEYS

a. AR 190-13, paragraph 2-18, provides information on security engineering surveys.

b. Requests for security engineering surveys beyond local capabilities must be sent to IMCOM-Europe (IMEU-OPD-PS) for coordination with an information copy sent to the PMD.

c. Technical assistance regarding site surveys, contracts, and the design, installation, and maintenance of ESSs may also be obtained from the Huntsville Center of Expertise (COE) for Intrusion Detection Systems, United States Army Corps of Engineers (USACE), Huntsville, Alabama, or from the Product Manager-Force Protection Systems (PM-FPS), Fort Belvoir, Virginia. Requests for assistance from the COE or the PM-FPS must be routed through IMCOM-Europe (IMEU-OPD-PS) and the PMD.

2-14. NEW CONSTRUCTION AND MAJOR RENOVATIONS

Commanders must ensure that every aspect of PS structural design is incorporated into the initial planning or renovation of facilities. PSOs are required to review and authenticate all copies of DD Form 1391 certifying that PS considerations have been thoroughly reviewed and are integrated into the proposed construction as applicable to the USAG. The PSO will maintain close liaison with installation engineers for early coordination of proposed new construction projects. The PSO should be an active voting member on the installation planning board.

2-15. PHYSICAL SECURITY CREDENTIALS

a. The PMD is the approval and issuing authority for PS inspector credentials for USAREUR subordinate units and will establish policy to control the issue and accountability of PS credentials in accordance with AR 190-13 and this regulation. All credentials will be inventoried and accounted for quarterly by the credential custodian.

b. USAREUR-assigned units and tenant commands will request PS credentials by sending a memorandum request to the PMD (AEOP-PD-SO). The request will include the name, rank, unit, two passport-size photographs, and a copy of the individual's Additional Skill Identifier H3 (Physical Security Operations) qualification record. All requests for PS inspector credentials must be signed by the individual's commander or designated representative and forwarded through his or her chain of command to the PMD for approval. PSOs will be issued credentials only if they conduct PSIs and PS surveys.

c. All commands that control and issue PS credentials will establish a PS credential program that meets the requirements of AR 190-13 and this regulation. The PMD (AEOP-PD-SO) can provide further assistance or guidance.

2-16. USAREUR PHYSICAL SECURITY MANAGEMENT SYSTEM

The PMD developed a web-based PSMS to facilitate oversight of the USAREUR PS Program and to reduce paperwork. The USAREUR PSMS is located on the PMD website at <https://intranet.eur.army.mil/hq/g34/pmd/sitepages/home.aspx>. Commanders of units and activities will provide a copy of all PS inspections and surveys to their higher headquarters PSO. The higher headquarters PSO is responsible for uploading required inspections, assessments, surveys, appointment orders, MEVA lists, and deviations into PSMS. Disposition of web-based files must be completed in accordance with AR 25-400-2.

CHAPTER 3 SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

3-1. PURPOSE

This chapter—

a. Is intended to help unit and activity armorers meet regulatory requirements for AA&E security and accountability.

b. Is not intended to be a substitute for AR 190-11, AR 385-10, AR 385-64, DA Pamphlet 385-64, and garrison arms room policy.

3-2. GENERAL

a. The term “armed guard” used throughout this chapter is defined as guard personnel having a weapon with a magazine loaded with ammunition, regardless of whether or not a round is chambered.

b. This chapter provides the minimum security requirements for categories of AA&E. Commanders will refer to both Army and USAREUR safety regulations for guidance on how to obtain an ammunition and explosives storage license for their storage structures and to determine the maximum permissible amount of ammunition and explosives that may be stored.

c. The garrison safety director is the licensing authority for all garrison arms rooms and AA&E storage facilities.

3-3. ACCESS CONTROL ROSTERS

a. Commanders will ensure that access to AA&E is controlled at all times in accordance with AR 190-11 and AR 190-13. Commanders will complete DA Form 7281 on all personnel identified to work with AA&E. Figures 3-1 through 3-3 show examples of how to request information needed for completing DA Form 7281.

b. The names and duty positions of authorized personnel must be posted on an unaccompanied access roster (fig 3-4) inside the arms room and covered from view.

c. Commanders will establish and use the two-person rule for all category I AA&E storage facilities and require that two authorized persons be present during any operation that requires access to these facilities. Commanders will also establish appropriate key-and-lock control procedures to prevent anyone from circumventing the two-person rule.

d. The use of the two-person rule for other categories of AA&E is at the discretion of the commander.

e. Commanders will minimize the number of individuals authorized unaccompanied access. Personnel must be selected based on a genuine need for unaccompanied access to the room. Everyone selected must undergo required background checks and security screenings to ensure suitability before being granted unaccompanied access in accordance with AR 190-11, chapter 2, paragraph 2-11.

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

OFFICE SYMBOL

Date

MEMORANDUM FOR (*address of the organization that maintains copies of the individual's military medical records*)

SUBJECT: Request for Military Medical Records Check, (*individual's name, rank or grade*)

1. (*Individual's rank or grade, name, unit*) is being considered for a position requiring unaccompanied access to our unit arms room. AR 190-11, paragraph 2-11, requires a medical records check on each individual being considered for such a position.

2. Please review the medical records of (*individual's rank or grade and name*) and identify any information that may or should be considered when determining (*his/her*) suitability for this position. Once you have completed the review, please complete DA Form 7281, section III, and send it to the POC in paragraph 3.

3. The POC is (*rank or grade and name of security officer*), military (*telephone number*).

Unit/Activity Commander
Signature Block

Figure 3-1. Request for Medical Records Check

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

OFFICE SYMBOL

Date

MEMORANDUM FOR (*address of the organization that maintains copies of the individual's personnel records*)

SUBJECT: Request for Personnel Records Check, (*individual's name, rank or grade*)

1. (*Individual's rank or grade, name, unit*) is being considered for a position requiring unaccompanied access to our unit arms room. AR 190-11, paragraph 2-11, requires a personnel records check on each individual being considered for such a position.

2. Please review the personnel records of (*individual's rank or grade and name*) and identify any information that may or should be considered when determining (*his/her*) suitability for this position. Once you have completed the review, please complete DA Form 7281, section II, and send it to the POC in paragraph 3.

3. The POC is (*rank or grade and name of security officer*), military (*telephone number*).

Unit/Activity Commander
Signature Block

Figure 3-2. Request for Personnel Records Check

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

OFFICE SYMBOL

Date

MEMORANDUM FOR (*address of the DES/PM or security office that maintains copies of the individual's security records*)

SUBJECT: Request for Security Records Check, (*individual's name, rank or grade*)

1. (*Individual's rank or grade, name, unit*) is being considered for a position requiring unaccompanied access to our unit arms room. AR 190-11, paragraph 2-11, requires a security records check on each individual being considered for such a position.

2. Please review your security and military police records of (*individual's rank or grade and name*) and identify any information that may or should be considered when determining (*his/her*) suitability for this position. Once you have completed the review, please complete DA Form 7281, sections IV and V, and send it to the POC in paragraph 3.

3. The POC is (*rank or grade and name of security officer*), military (*telephone number*).

Unit/Activity Commander
Signature Block

Figure 3-3. Request for DES/PM or Security Office Records Check

3-4. KEY-AND-LOCK CONTROL OF AA&E

a. AR 190-11, chapter 3, and AR 190-51, appendix D, provide guidance on key-and-lock control.

b. A sample unaccompanied-access roster is shown in figure 3-4. Commanders will appoint a key custodian in writing (fig 3-5). Only the commander and the key custodian (or alternate, if appointed) may issue keys to, and receive keys from, individuals on the key access roster.

c. Key custodians will—

(1) Store the alternate or spare set of AA&E keys in a separate security container that is approved by the General Services Administration and does not contain and is not used to store classified documents or material. The container storing these keys must be located in a different room from the primary set of keys. Keys may be stored locally with another unit or organization when the next higher command is not in the same community or geographic location. If stored outside the unit or organization, a memorandum of understanding with the unit or organization maintaining the keys must be established. Personnel authorized to sign for the keys will be annotated on DA Form 5513.

(2) Ensure that keys to locks securing key containers are given double-barrier physical protection. Key custodians will also ensure that replacement and reserve locks, cores, and keys are inventoried and secured to prevent access by unauthorized individuals.

(3) Investigate immediately when keys are misplaced or lost and conduct a 100-percent serial number inventory to determine if any AA&E is missing. Key custodians will immediately replace compromised locks or cores.

(4) Ensure keys that are not placed in a sealed container are inventoried by serial number or by other identifying information on the key (for example, a stamped number on the key). The inventory and change of custody will be recorded on DA Form 5513.

(5) Ensure controls are established so that envelopes containing combinations to locks or containers are not made available to unauthorized personnel.

3-5. CONSOLIDATED ARMS ROOMS

Procedures for operating a consolidated arms room are outlined in AR 190-11, chapter 4, paragraph 4-4. Procedures will also be outlined and included in the memorandum of understanding between both commanders (fig 3-6).

3-6. ARMED GUARD REQUIREMENTS

a. If the ESS fails, an armed guard will immediately be posted by the unit responsible for the AA&E facility until the ESS returns to normal operation. Local commanders will provide guidance and orders to the armed guard force.

b. Armed guards will accompany all shipments of AA&E when transported off an installation as described in paragraph 1-4i of this regulation.

3-7. ELECTRONIC SECURITY SYSTEM (ESS)

ESSs must meet the requirements of AR 190-11, chapter 3, and AR 190-13, chapter 9. ESS purchase and installation must first be approved by the PMD. Because an ESS is nonstandard PS equipment, commanders are not authorized to purchase or install an ESS without prior coordination and approval by the PMD.

3-8. STORAGE AND SUPPLEMENTAL CONTROLS

AR 190-11, chapter 4, section 2, provides additional requirements for all categories of AA&E storage and supplemental controls.

3-9. CONTROL OF WEAPONS

AR 190-11, chapter 4, provides guidance on the control of weapons.

3-10. PROTECTION OF MISSILES, ROCKETS, AMMUNITION, AND EXPLOSIVES AT UNIT LEVEL

AR 190-11, chapter 5, provides guidance on the protection of missiles, rockets, ammunition, and explosives at unit level.

3-11. WEAPONS AND AMMUNITION INVENTORIES

AR 190-11, chapter 6; AR 710-2-1, chapter 2; and DA Pamphlet 710-2-1, chapter 9, provide guidance for commanders, hand-receipt holders, and unit armorers on AA&E inventory procedures.

3-12. REPORTING MISSING OR RECOVERED AA&E

When AA&E is lost, missing, stolen, or recovered, the USAG DES/PM or designated representatives will immediately complete a SIR and DA Form 3056 and send copies to the PMD (AEOP-PDP-LE) and the 5th MP Battalion (CID).

3-13. PRIVATELY OWNED AND COMMERCIAL WEAPONS AND AMMUNITION

All personnel subject to the NATO Status of Forces Agreement will comply with the policy outlined in AR 190-11, ALARACT 063/2013, AE Regulation 190-6, and HN laws as applicable.

3-14. TRAINING

Commanders and managers responsible for AA&E will establish a training program for personnel responsible for the security and accountability of these items. Annual refresher training will also be conducted to ensure that all personnel are aware of their responsibilities for controlling and safeguarding AA&E.

3-15. IN-TRANSIT SECURITY OF AA&E

Commanders will ensure that any unit movement of AA&E is done in accordance with the security requirements outlined in paragraph 1-4i of this regulation.

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

AEFG

1 February 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Arms Room Unaccompanied-Access Roster

1. The following individuals are authorized unaccompanied access to this arms room:

NAME	RANK/ GRADE	UNIT	POSITION
Johnson, Samuel G.	1LT	289th ENGR CO	Unit Supply Officer
Jones, Pamela M.	SGT	289th ENGR CO	Unit Armorer
McKinney, John K.	SFC	343d PSB	Unit Supply NCOIC
Ball, Pamela	SGT	343d PSB	Unit Armorer

2. Inspecting officers and other visitors will not be allowed unaccompanied access to this arms room.

3. The POC is Sergeant Jones, military 123-4567 or e-mail: earl.jones.mil@mail.mil.

JOHN DOE
Lieutenant Colonel, AR
Commanding

DISTRIBUTION:
Tenant Unit/Activity Commander
Individuals Concerned
Posted Inside Arms Room
Unit Physical Security Officer/NCO

Figure 3-4. Sample Arms Room Unaccompanied-Access Roster

OFFICE SYMBOL

Date

MEMORANDUM FOR RECORD

SUBJECT: Duty Appointment for (*Primary or Alternate*) Arms, Ammunition, and Explosives Key Custodian

1. EFFECTIVE: (*date, rank or grade, name*) is appointed as the (*primary or alternate*) Arms, Ammunition, and Explosives Key Custodian for the (*unit or activity*) arms room and electronic security system keys.
2. AUTHORITY: AR 190-11, paragraph 3-8.
3. PURPOSE: Assure proper control, accountability, and handling of keys and locks for the arms room.
4. PERIOD: Until officially relieved or released from this appointment.
5. SPECIAL INSTRUCTIONS: Become familiar with the key-control provisions of AR 190-11 and AR 190-51, appendix D.
6. POC: The POC is (*rank or grade and name of security officer*), military (*telephone number*).

Unit/Activity Commander
Signature Block

DISTRIBUTION:
Unit/Activity Commander
Individual Concerned
Unit Physical Security Officer/NCO
Physical Security Files

**Figure 3-5. Format of Appointment Memorandum for Record
for Primary or Alternate AA&E Key Custodian**

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

OFFICE SYMBOL

Date

MEMORANDUM FOR All Unit Commanders Storing Weapons in (*Unit or Facility*) Arms Room

SUBJECT: Bilateral Storage Agreement for Consolidated Arms Room

1. As the host commander with overall responsibility for the (*unit or facility*) arms room, I am establishing this agreement and have overall responsibility for this storage facility. All undersigned tenant commanders and their arms-room personnel who share the use of this facility will strictly adhere to the following bilateral storage agreement.
2. Quantities of arms, ammunition, and explosives (AA&E) to be stored will not exceed those authorized by the unit table of distribution and allowances or table of organization and equipment, contingent on adequate space being available and garrison safety office approval. Ammunition may not be stored in this facility except in limited quantities to support armed-guard requirements or for authorized training. Written authorization must be obtained from the undersigned host commander.
3. Each unit will install supply caging to separate one unit's weapons from another unit's (*where available*). All cage bolts must be spot-welded or peened, and the caging must be joined to prevent unauthorized access. Each unit's caging must be equipped with its own General Services Administration approved keys and locks in accordance with AR 190-11. The appointed AA&E key custodian will control the keys and locks. If supply caging is not used to separate one unit's weapons from another, space separation will be maintained and approved racks and containers will be used to secure each unit's weapons.
4. Individual units are responsible for conducting their own inventories in accordance with AR 190-11, AR 190-13, and AR 190-51. (*This applies only to arms rooms where unit weapons are adequately separated and accessible only to unit personnel. In cases where all weapons are accessible to anyone entering the arms room, a physical count of all weapons must be conducted on entry and exit of the arms room. If a discrepancy is discovered during a physical count, a serial-number inventory of all the weapons must be conducted immediately. Monthly serial-numbered inventories are an individual unit responsibility.*) Units will provide results of monthly inventories to the commander responsible for overall security of the arms room.

Figure 3-6. Bilateral Storage Agreement for Consolidated Arms Room

OFFICE SYMBOL

SUBJECT: Bilateral Storage Agreement for Consolidated Arms Room

5. Reporting losses for investigation. *(The guidance in this paragraph will be developed locally by the commanders whose units store weapons in the facility.)*
6. Key control. *(The primary key-and-lock custodian will control the arms room, AA&E, and intrusion-detection system (IDS), and will maintain current unaccompanied-access rosters from each unit in the arms room. This section should emphasize the need for each unit to control and account for its own AA&E keys and locks. Unit commanders will maintain current access rosters identifying who can sign for keys and gain unaccompanied access to the arms room by each unit. Copies of rosters must be provided to the unit that has overall responsibility for the arms room. The number of individuals on each access roster should be limited to only those essential for mission accomplishment. In all cases, appropriate accountability and control procedures in AR 190-11 must be followed.)*
7. IDS Failure Procedures. *(This section should establish procedures for guarding the arms in the event of electronic security system failure in accordance with AR 190-11, AR 190-13, and AR 190-51.)*
8. Units not complying with this Bilateral Storage Agreement for Consolidated Arms Room will be denied access.
9. The POC is *(rank or grade and name of security officer)*, military *(telephone number)*.

*Host Unit/Activity Commander
Signature Block*

*Tenant Commander
Signature Block*

*Tenant Commander
Signature Block*

DISTRIBUTION:
Unit/Activity Commanders
Individuals Concerned
Unit Physical Security Officer/NCO
Physical Security Files

Figure 3-6. Bilateral Storage Agreement for Consolidated Arms Room—Continued

CHAPTER 4

ACCESS CONTROL

AE Regulation 190-16 describes procedures for controlling access to and from U.S. Army installations in the European theater. AE Regulation 525-13 prescribes policy and procedures for physically searching individuals and vehicles. This regulation (AE Reg 190-13) addresses PS issues, but does not apply to restricted areas governed by other regulations.

4-1. ADDITIONAL ACCESS-CONTROL POINT (ACP) GUIDANCE

TC 19-210 provides additional guidance and procedures. Commanders should refer to the DOD Technical Support Working Group Vehicle Inspection Checklist as a guide for developing and conducting training on search techniques.

- a. ACP guards will use AE Form 190-13H(G) (English/German) or AE Form 190-13H(I) (English/Italian), as applicable, at every ACP to manually log in visitors and their vehicles. ACP guards will record visitor information electronically once the ACP is equipped with an IACS computer terminal.
- b. Commanders will ensure that all contract and military guards perform cursory visual inspections of the interior of vehicles as they conduct identification checks of vehicle occupants. When something or someone appears suspicious, the vehicle will be diverted for a more thorough search.
- c. Communication between ACP guards and search teams must be established to alert the search teams of suspicious vehicles.
- d. Guards will conduct threat-focused searches of vehicles and large containers. Emphasis will be placed on searching vehicles such as commercial vans and trucks, delivery and cargo-type vehicles, and vehicles that do not have U.S. Forces license plates. Emphasis will also be placed on searching containers and the personal baggage of workcrews that must be signed onto the installation.
- e. During periods of greater threat such as holidays, special events, and military or governmentally recognized anniversaries, commanders must increase the frequency and locations of searches of vehicles entering their installations.
- f. Commanders will ensure that all guards (civilian and military) receive proper and continuous training on effective vehicle search techniques. Search personnel must be proficient in detecting not only the obvious, but also in noticing modifications that may indicate the presence of hidden compartments or explosives.
- g. Guards should also be trained to note operator and passenger behavior through means such as casual questions while checking identification to help verify their purpose for entering the installation.
- h. Commanders will continuously check to ensure guards thoroughly understand the commander's intent and comply with policy on access control, arming, rules of engagement, and use of force.
- i. Installation Access Control Point (IACP), restricted area, and traffic control signs will be posted in accordance with AR 190-13, chapter 6; AR 420-1; TM 5-807-10; USACE Army Installation Design Standards; USACE Army Access Control Point Standard and Design/Criteria; United States Department of Transportation, Federal Highway Administration, Manual on Uniform Traffic Control Devices; and HN laws and regulations.

4-2. INVESTIGATING AND ADJUDICATING ACP INSTALLATION BARRIER INCIDENTS

a. IMCOM-Europe uses vehicle barriers at IACPs as a traffic control and security measure. Standard security drop-bar barriers are generally used to signal drivers to stop and wait until required identification checks are completed before proceeding through the gate. Heavy-duty barriers and other FP devices are used to stop high-speed penetration of the gate by unauthorized personnel. Access-control personnel posted at the gate are responsible for operating vehicle barrier systems. Procedures addressed in this regulation apply when barrier incidents occur and injuries to personnel or damage to property has occurred regardless of the type of access-control personnel employed (for example, contractor, U.S. or HN military) in the USAREUR AOR.

b. To ensure fair and equitable adjudications of barrier incidents, installation commanders and agencies that are responsible for installation access control will—

(1) Conduct an initial safety survey of each ACP using vehicle barriers to identify safety concerns that need to be resolved. Points of interest should include, but are not limited to, the adequacy of stand-off distance, the line of sight between the barrier operator and the barrier, the location of activation switches, and warning signals. After the initial safety survey, a follow-up survey will be conducted at least every 2 years or when ACP requirements change, whichever occurs first. Coordination will be made for a representative from the garrison safety office to participate in the initial and periodic safety surveys to identify safety hazards at each installation ACP.

(2) Ensure new gate designs are reviewed by the USAG DPW, DES/PM, USAG safety office, and USAG antiterrorism office to identify safety and operational concerns before plans are approved and construction begins.

(3) Ensure that special orders for gate guards include adequate instructions on barrier operations, activations, and reporting procedures. As a minimum, when a barrier incident causes damage to property or injury to personnel, access-control personnel will carry out the following procedures:

(a) Secure the accident site and render first aid, as appropriate.

(b) Notify military police, the guard supervisor, the USAG SCOR, and, if required, emergency services.

(4) Appoint or designate an individual to investigate barrier incidents that caused damage to property or injury to personnel. The investigating officer must be an officer or noncommissioned officer (sergeant first class or higher) or a DOD civilian (GS-09 or higher). These individuals should be appointed from the USAG SCOR, DES/PM, USAG safety office, and USAG antiterrorism office. The USAG safety office will be notified of all ACP accidents as soon as possible.

(a) The responding member of the MP will conduct a traffic investigation in accordance with AR 190-5 and AR 190-45, and provide a copy of the final MP report to the investigating officer.

(b) If a contract guard is involved, the contractor will conduct a separate investigation in accordance with the contractor's own policy. The contractor's report must be as thorough as possible and indicate the date the barrier operator completed required training on barrier operations and activation procedures. A copy of the special orders for the barrier operator must be attached to the

contractor's report. The contractor will provide a copy of the contractor's final report to the investigating officer within 2 weeks after the incident.

(c) The investigating officer will coordinate with the USAG legal, safety, and antiterrorism offices and provide a copy of the final investigation report to the servicing legal office within 4 weeks after the date of the accident or incident.

(d) The United States Army Claims Service, Europe, will provide guidance to the USAG DES/PM, DPW, USAG safety office, and USAG antiterrorism office on unusual or complicated barrier accidents and incidents and serve as the sole POC for communicating with HN military and contract security guard administrative personnel in barrier accidents and incidents when the evidence does not indicate negligence of U.S. Government employees.

CHAPTER 5 SECURITY OF ARMY PROPERTY AT UNIT AND INSTALLATION LEVEL

5-1. GENERAL

AR 190-51 provides guidance for the security of army property at the unit and installation level.

5-2. COMMUNICATIONS SECURITY (COMSEC) MATERIAL AND CONTROLLED CRYPTOGRAPHIC ITEMS

AE Regulation 380-40 provides policy and procedures for safeguarding, controlling, and disposing of COMSEC material, controlled cryptographic items, and other secure communications equipment.

5-3. SECURITY OF U.S. ARMY ISSUED BAYONETS

a. When not in use, U.S. Army-issued bayonets must be stored in a locked and sealed footlocker or container inside the unit arms room or other secure storage structure as prescribed by AR 190-51, appendix B. A copy of the bayonet inventory must be placed inside the container before sealing it, and the original must be kept in inventory records and be available for inspections and inventories. A memorandum will be placed on the outside of the container describing the contents and include the date, seal number used to seal the container, and the two signatures of the individuals who conducted the inventory.

b. Bayonets will be inventoried each month in conjunction with the inventory of weapons. During inventories, the containers storing the bayonets need not be opened as long as the seal is intact and there are no signs of tampering. If signs of tampering are present, the container must be opened and a 100-percent inventory must be conducted to ensure no bayonets are missing.

c. When the primary hand-receipt holder transfers custody of the hand-receipt to someone else, a 100-percent inventory should be conducted.

CHAPTER 6 PHYSICAL SECURITY EQUIPMENT (PSE)

6-1. GENERAL

In accordance with AR 190-13, chapter 4, and this regulation, PS resources will be used to protect Army assets and capabilities including national security information and materiel. Nonstandard PSE may be used if DOD or DA standardized equipment is not available or does not meet a technical requirement.

An operational needs statement will be sent to the United States Army Training and Doctrine Command user representative when DOD- or DA-standardized equipment needs to be developed. Once a component or system is developed or adopted from commercial sources, it is considered standardized and may be adopted by all DOD components to meet joint operational requirements. ESSs are not routine requirements for Army facilities or areas, but rather for assets when specifically prescribed by policy.

6-2. PROGRAM MANAGEMENT

USAG DES/PMs will help commanders and tenant activities identify and develop PSE and ESS projects to meet requirements, establish standards, and ensure compatibility with existing systems. In coordination with the USAG DPW, the USAG DES/PM will track and maintain data on intrusion-detection systems and other ESSs in his or her AOR.

a. IMCOM-Europe will procure and maintain ESSs for USAG installations. Requests for nonstandard FP/PS equipment must be coordinated and approved through the SEWG.

b. IMCOM-Europe will schedule and provide funding for procurement and sustainment costs for ESSs, to include all appropriate supporting documentation and approvals.

c. Priorities for PSE and ESSs are determined by the security or risk level of the installation or facility and the degree of protection required by regulation. Other determining factors are identified vulnerabilities and threats.

d. In accordance with AR 190-51, supported tenants will conduct a risk analysis on all MEVAs, facilities, and installations being considered for PSE and ESS enhancements or upgrades. A copy of the risk analysis will be provided to the USAG DES/PM. The results of the risk analysis will be used during security planning to identify, assess, and validate PS requirements, including the need for PSE and ESS.

e. Commanders at all levels will properly forecast and coordinate PSE requirements, develop cost estimates, and establish a maintenance plan before any acquisition.

f. Commanders will prioritize forecasted PSE requirements and coordinate with the servicing USAG DES/PM office, DPW, director of resource management, and servicing signal battalion. Commanders will review, consolidate, and prioritize forecasted requirements before submitting them to IMCOM-Europe (IMEU-OPD-PS). Forecasted submissions alone do not constitute approval for PSE.

g. All requests to upgrade, purchase, issue, lease, and renew the lease of nonstandard ESSs require approval by the PMD. Requests must be sent through the USAG DES/PM and IMCOM-Europe (IMEU-OPD-PS) to the PMD.

h. When required, ESS engineering site surveys must be conducted and submitted through IMCOM-Europe (IMEU-OPD-PS) to the PMD for review and approval. Site surveys are required for nonstandard ESSs before final approval and funding.

i. Extensive or complex ESS projects require the expertise and participation of qualified electronic security engineers to properly complete the survey and design. Requests for this assistance must be sent through the DES/PM and through IMCOM-Europe (IMEU-OPD-PS) to the PMD.

j. Figure 6-1 shows the format for requesting non-Army or non-USAREUR-standard installation of an ESS.

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

OFFICE SYMBOL

Date

MEMORANDUM THRU United States Army Garrison Directorate of Emergency Services (IMXX-XXX), Unit 12345, APO AE 09014-2345

FOR Office of the Provost Marshal (AEOP-PDP-SO), HQ USAREUR, Unit 29351, APO AE 09014-29351

SUBJECT: Request Approval for Non-USAREUR Standard Electronic Security System

1. The purpose of this memorandum is to request approval to install an electronic security system (ESS) for the (*unit, facility type, or room*) located in building (*building number, installation, garrison, city, country*). The risk level of this facility is risk level (*level of risk*).
2. *Enter the justification for the ESS (for example, to meet regulatory requirements, reduce vulnerability identified during a risk analysis or security survey, to reduce manpower requirements).*
3. *Provide an independent Government cost estimate of the ESS that includes details on manpower, cost savings, or both.*
4. *Provide an operational concept plan that describes how the system will be deployed, operated, and integrated into the existing garrison ESS (for example, who will monitor it and where will it be located). This paragraph should also describe how the ESS operates.*
5. *Provide a maintenance and sustainment plan that describes how the ESS will be maintained, how the ESS has been included or programmed into the unit's or garrison's Schedule 75, and when these funds are expected to be available.*
6. In accordance with the U.S. Army Corps of Engineers Site Survey Procedures Guide for Electronic Security Systems, the United States Army Garrison (USAG) Physical Security Office has conducted a site survey in coordination with the USAG Physical Security Inspector, USAG Director of Public Works, and information assurance personnel as indicated on the engineering survey.
7. The projected FY for the installation is FY (*year*), subject to available funding.

Figure 6-1. Format for Requesting a Non-Army or Non-USAREUR-Standard ESS

OFFICE SYMBOL

SUBJECT: Request Approval for Non-USAREUR Standard Electronic Security System

8. The USAG Directorate of Emergency Services POC is (*rank or grade and name of security officer*), military (*telephone number*).

Encls

Unit/Activity Commander

1. Engineering Site Survey

Signature Block

(*TM 5-853-4*)

2. Technical Specifications of Proposed Components

3. Equipment List and Cost Estimate

4. Digital Photos for Visual Support (*recommended but not required*)

5. Other Supporting Documentation

Figure 6-1. Format for Requesting a Non-Army or Non-USAREUR-Standard ESS—Continued

6-3. CLOSED-CIRCUIT TELEVISION (CCTV)

a. CCTV provides a technological substitute for continuous surveillance for certain assets. CCTV is not a routine requirement for Army facilities or areas, but used as an aid to PS or when specifically prescribed by policy.

b. CCTV—

(1) May be installed when interfacing with existing or planned ESSs as an alarm-assessment tool.

(2) Generally may not be installed for surveillance purposes. CCTV may be used at ACPs to record personnel and vehicles entering the installation for investigative purposes.

(3) Must be connected to a digital recording device and recording at all times when used.

c. Commanders are prohibited from using CCTV and other electronic EECSs for time-and-attendance purposes.

6-4. ELECTRONIC ENTRY/ACCESS CONTROL SYSTEMS

Specifications for constructing EECSs are outlined in the Corps of Engineers Guide Specification 13720. The requirement for using EECSs to control access to classified information is described in AR 380-5, chapter 7. AR 600-8-14 also provides guidance on EECSs. All—

a. Newly acquired EECSs in the USAREUR AOR must use contactless proximity technology.

b. Newly acquired or upgraded EECSSs will, as a minimum, be equipped with a 12-hour battery backup.

c. Systems must be approved by USAG fire and safety officials before and after installation. Fire and safety officials will ensure that the system has life and safety features built in.

6-5. ESS PERSONAL IDENTIFICATION NUMBERS

Personal identification numbers (PINs)—

a. May be used to activate or deactivate an alarm panel or used to gain access to restricted areas.

b. Will not be shared or written down in locations where others have access.

c. Will never be used twice by the same organization.

d. Will be changed at least once a year. PINs must also be changed when the individual assigned the PIN no longer requires access or if there is reason to suspect that the PIN was compromised.

6-6. MAINTENANCE OF ESS

a. Commanders will ensure that only trained and qualified personnel maintain ESSs as outlined in AR 380-67. Requirements for personnel suitability checks and clearances for PSE installation and maintenance must be clearly stated in contracts.

b. The USAG DPW is responsible for maintaining ESS drawings, providing copies of drawings to the using activity, and updating drawings when changes occur.

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

d. ESSs will be maintained in accordance with AR 190-11, paragraph 3-6, and as specified in maintenance contracts. Maintenance requirements specified in AR 190-11, paragraph 3-6, will be included in the maintenance contract statement of work or PWS.

6-7. PERSONNEL SUITABILITY AND RELIABILITY CHECKS

a. In accordance with AR 190-11, paragraph 3-6, personnel who design, operate, monitor, or maintain ESSs must meet the personnel screening requirements listed.

b. Authorized command-oriented background checks include AE Form 190-45D and the Local National Screening Program (LNSP). AE Form 190-45D will be processed by the USAG PM/DES office. The USAREUR G2 (AEIN-SAP) is the proponent for the LNSP.

c. When the duties of local national employees or contract personnel involve designing, operating, monitoring, or maintaining ESSs, these personnel must be processed through the LNSP in accordance with AE Regulation 604-1 and must not have any derogatory information on file. At no time will an uncleared, non-U.S. citizen perform any type of maintenance on systems providing protection of facilities that house sensitive compartmented information.

6-8. MOVEMENT OF ESS COMPONENTS AND SYSTEMS

ESSs will not be activated, deactivated, or moved without written prior notification and approval from the IMCOM-Europe PSO (IMEU-OPD-PS).

6-9. ESS INSPECTIONS

The checklist located in the SOAB Automated Physical Security Management Portal must be used for ESS inspections.

6-10. RESPONSE TO ALARMS

a. Commanders will establish alarm response policy and procedures in accordance with applicable Army regulations (for example, AR 190-11, AR 190-51, AR 380-5) and the USAG DES/PM. Policy implemented through USAG AT/FP and crisis management plans must designate the type, size, and armament of the response force.

b. The USAG DES/PM will establish procedures on the use of force in accordance with AR 190-14.

CHAPTER 7

USAREUR CONTRACT GUARD PROGRAM

Questions and concerns regarding the USAREUR Contract Guard Program may be sent to the Contract Guard Program Manager, COR, Emergency Services Branch, IMCOM-Europe (IMEU-OPD-S).

CHAPTER 8

USAREUR G34 STAFF ASSESSMENT VISIT (SAV) PROGRAM

8-1. PURPOSE

This chapter prescribes policy and assigns responsibility for developing and maintaining practical, economical, and effective SAV programs. SAV programs will be used to identify, document, and report installations or activities that require special PS or contract guard considerations because of their mission-essential, critical status and vulnerability to—

- a. Criminal acts.
- b. Dissidence.
- c. Hostile intelligence activities.
- d. Terrorist acts.
- e. Other disruptive influences.

8-2. SECURITY OPERATIONS AND ASSESSMENTS BRANCH

The SOAB is responsible for overall PS policy and programs in the European theater based on an analysis of the mission and known or anticipated requirements and threats. This responsibility extends to contingency operations and missions throughout the European theater.

8-3. OPERATIONAL INSPECTION AND SAV PROGRAMS

IMCOM-Europe will establish and execute a command organizational inspection program (OIP) and an SAV program to monitor the adequacy of PS program implementation and requirements at USAGs.

Each USAG will be inspected at least once every 24 months or more frequently as determined by the Director, IMCOM-Europe. Inspections may be more frequent as a result of findings noted during other PS and command inspections and surveys or because of a change in operational requirements or the threat condition. Inspection schedules should be established and coordinated with the garrison to be inspected at least 6 months before the inspection.

8-4. PHYSICAL SECURITY INSPECTION AND SAV

The SOAB is responsible for conducting SAVs and participating in command OIPs that specifically address the USAREUR PS Program. This is in addition to PS inspections required by AR 190-11, AR 190-13, and AR 190-16. Only personnel who have received training from the H3 Physical Security School will conduct SAVs. An outbriefing will be given to the commander of the unit after the SAV. Findings will be posted by PSOs and PSIs on the USAREUR G34 SharePoint portal website at <https://intranet.eur.army.mil/hq/g34/pmd/sitepages/home.aspx>.

8-5. USAREUR CONTRACT GUARD SAV

The SOAB is responsible for conducting SAVs specifically addressing the USAREUR Contract Guard Program. The intent of the contract guard SAV is to identify program discrepancies within contract guard programs. The SOAB staff conducting SAVs will also identify contractual discrepancies and report all findings to the IMCOM-Europe Contract Guard COR and the Chief, SOAB.

8-6. REQUIRED SAV ACTIONS (PHYSICAL SECURITY)

During SAVs, the SOAB representative will check the PS plan by referring to AR 190-13, appendix B, and its appendixes. In addition, PS plans must address the following appendixes listed in AR 190-13:

- a. Appendix K, Physical Security Credential Accountability.
- b. Appendix L, Host Nation Coordination.
- c. Appendix M, Barrier Plan(s).

8-7. REQUIRED SAV ACTIONS (CONTRACT GUARD PROGRAM)

During SAVs, the SOAB representative will check overall compliance with the current contract describing the USAREUR Contract Guard Program.

CHAPTER 9

USAREUR SECURITY EQUIPMENT WORKING GROUP (SEWG)

9-1. GENERAL

This chapter outlines responsibilities and provides guidance for the procurement of nonstandard, commercial FP/PS equipment. In addition, it provides policy guidance and procedures for the SEWG.

9-2. POLICY

- a. Technological advances and limited resources require commanders to be prudent in assessment and selection practices. Because of numerous technological advances, a wide variety of commercial FP/PS equipment is available to enhance security throughout the European theater.

b. The SEWG provides commanders with sound recommendations on the types of security equipment available to reduce identified vulnerabilities. The SEWG also provides recommendations for specific manufacturers and model numbers when commanders want to procure specific security hardware.

c. The SEWG program addresses nonstandard, commercial FP/PS equipment only (para 9-3). Commanders may continue to procure standard FP/PS equipment without contacting the SEWG. Commanders are also authorized to procure standard FP/PS equipment to supplement or maintain existing approved systems if they coordinate with the USAG DES/PM.

d. The intent of this regulation is not to limit commanders, but to avoid the need for each commander to conduct independent market analyses, operational evaluations, or other resource-intensive actions to select the best system for the mission. Additionally, equipment and technology throughout the USAREUR AOR can be standardized, which facilitates economic initial procurement; operator training; maintenance, procurement, stockage, and distribution of repair parts and expendable supplies; and contractor-logistics support. To be effective, the SEWG review must include a review of the detailed plan for the use of the proposed nonstandard equipment. The SEWG can provide assistance by reviewing the commander's detailed implementation plan.

9-3. DEFINITION OF NONSTANDARD EQUIPMENT

Nonstandard security equipment is any equipment not procured or available through the U.S. Army supply system. AR 190-13 prohibits commanders below those who command Army commands, Army service component commands (for example, USAREUR), and direct reporting units from approving requests to purchase, issue, replace, lease, or renew leases for nonstandard PSE such as mass notifications systems, vehicle inspection equipment, and vehicle tracking systems and devices.

9-4. SEWG RESPONSIBILITIES

a. The USAREUR PM or designated representative will chair the SEWG. The membership of the SEWG will consist of selected command representatives.

b. The SEWG chairperson may establish subordinate working or advisory groups to address specific functional areas. These groups will be established by charter and disestablished when the group's function is no longer required.

c. Specific functions of the SEWG are to—

(1) Conduct research and collect data concerning performance specifications and published test results for nonstandard, commercial FP/PS equipment systems. The SEWG is also responsible for validating (or refuting) manufacturer's performance claims found in advertising and marketing literature.

(2) Provide a resource database to users of DOD-approved systems and systems considered viable by the SEWG.

(3) Provide a mechanism to consolidate, standardize, and approve requests for FP/PS equipment throughout the USAREUR AOR. The SEWG is also responsible for conducting formal operational evaluations of FP/PS hardware to document performance capabilities and limitations.

9-5. PROGRAM MANAGEMENT

a. The SEWG will—

(1) Serve as the single POC for validating FP/PS equipment in coordination with the Office of the Science Advisor, HQ USAREUR, and the Force Protection Division, Office of the Chief of Staff, G3/5/7, HQ USAREUR.

(2) Coordinate with the following HQ USAREUR staff offices, as required: G1, G2, G4, G6, Engineer, G8, Judge Advocate. The SEWG may also coordinate with the Office of the ACoS, G4, IMCOM-Europe.

(3) Coordinate with other staff offices as needed to ensure maximum cooperation and compliance with policy.

(4) Coordinate issues concerning communication systems, vehicle-tracking systems, and microwave technologies with the Office of the Deputy Chief of Staff, G6, HQ USAREUR.

(5) Ensure that only effective FP/PS equipment is recommended for procurement and use in the USAREUR AOR. SEWGs are also responsible for continually reviewing emerging technology with DOD and DA security equipment organizations.

b. Commanders will—

(1) Ensure that all requests for procurement of commercial, nonstandard FP/PS equipment (para 9-3) are coordinated with the USAREUR PM. A detailed plan of how the proposed equipment is to be used must accompany the request. The plan must include schematics and detailed information about how the technology will be used and what threat it is intended to defeat, to include the regulatory requirement.

(2) Actively participate in the operational evaluation process for FP/PS equipment to ensure a complete and accurate analysis is conducted.

(3) Notify the SEWG of any equipment they wish to have evaluated, and provide the system type, the source of information, and the desired use of the equipment.

c. The United States Army Contracting Command, Europe, and other contracting activities supporting units in the European theater will ensure that requests for procurement of nonstandard commercial FP/PS equipment include written approval from the SEWG before the procurement action is processed.

APPENDIX A REFERENCES

SECTION I PUBLICATIONS

Defense Transportation Regulations 4500.9-R, Part II, Cargo Movement

United States Department of Transportation, Federal Highway Administration, May 12, subject: Manual on Uniform Traffic Control Devices

DOD 5200.1-R, Information Security Program

DOD Manual 5100.76, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)

DOD Vulnerability Assessment Benchmarks, 1 January 2013

DOD Technical Support Working Group Vehicle Inspection Checklist, 23 October 2000

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 190-5, Motor Vehicle Traffic Supervision

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 190-45, Law Enforcement Reporting

AR 190-51, Security of Unclassified Army Property (Sensitive and Nonsensitive)

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

AR 380-67, Personnel Security Program

AR 385-10, The Army Safety Program

AR 420-1, Army Facilities Management

AR 600-8-14, Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel

AR 710-2, Supply Policy Below the National Level

DA Pamphlet 190-51, Risk Analysis for Army Property

DA Pamphlet 385-64, Ammunition and Explosives Safety Standards

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

ALARACT Message 063/2013, March 2013, subject: Control and Reporting of Privately Owned Weapons

USEUCOM OPORD 11-05, HQ EUCOM Antiterrorism Operations Order

United States Army Corps of Engineers, May 2004, subject: Army Installation Design Standards

United States Army Corps of Engineers, January 2009, subject: Army Access Control Point Standard and Design/Criteria

Corps of Engineers Guide Specification 13720, Electronic Security System

Technical Manual 5-807-10, Signage

Technical Manual 5-853-4, Security Engineering Electronic Security Systems

Training Circular 19-210, Access Control Handbook

AE Regulation 10-5, Headquarters, United States Army Europe

AE Regulation 55-4, Safe Movement of Hazardous Goods by Surface Modes

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

AE Regulation 190-16, Installation Access Control

AE Regulation 380-40, Safeguarding and Controlling Communications Security Material

AE Regulation 525-13, Antiterrorism

AE Regulation 604-1, Local National Screening Program in Germany

USAREUR OPORD 0040-13, General Officer for Force Protection (GOFP) Designations

USAREUR TASKORD 12-0260, Transportation Security Measures for Arms, Ammunition, and Explosives

USAREUR GENADMIN Message No. 1205094, Security, Storage, and Transportation of Category I and II Ammunition

SECTION II FORMS

DD Form 1391, FY___ Military Construction Project Data

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 2806-1, Physical Security Inspection Report

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

DA Form 4283, Facilities Engineering Work Request

DA Form 5513, Key Control Register and Inventory

DA Form 7281, Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Record

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

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

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

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

AE Form 190-45D, Military Police Record Check

AE Form 525-13A, Army in Europe Bomb Threat Telephone Guide

APPENDIX B

GUIDELINES FOR DEVELOPING INSTALLATION BARRIER PLANS

B-1. GENERAL

Barrier plans are part of the overall antiterrorism plan evaluated during joint services integrated vulnerability assessments (JSIVAs) by the Defense Threat Reduction Agency (DTRA). Barrier plans consider the threat from stationary (parked) and moving vehicles. Barriers may be used to restrict parking, redirect traffic, or both. These guidelines will help installations develop and execute effective barrier plans for various threat conditions.

B-2. OBJECTIVE

The objective of a barrier plan is to provide orderly and timely security to U.S. Forces, their tenants, and all U.S. property. A clear, detailed, and rehearsed plan should reduce the manpower and time needed to execute force-protection requirements while maintaining a safe environment as the force protection condition (FPCON) increases.

B-3. REFERENCES

- a. DOD Vulnerability Assessment Benchmarks.
- b. USEUCOM OPORD 11-05.
- c. AE Regulation 525-13.
- d. Local policy (if any).

B-4. BARRIER PLAN ELEMENTS

A clear and detailed barrier plan identifies the needs, resources, and associated actions, for securing the perimeters of installations and any other local U.S. military facilities under the operational control of the installation commander. Until necessary construction projects are completed, the barrier plan should provide for temporary barrier placement. The barrier plan should meet the intent and standards described in the DOD Vulnerability Assessment Benchmarks, direct various units and activities to take specific actions, and include the following subjects:

a. Responsibilities. The local commander will develop barrier plans supported by class 4 supplies from the director of public works (DPW) and the director of logistics (DOL). The DPW and DOL are responsible for barrier emplacement. Directorate of emergency services (DES) personnel are responsible for quality control.

b. Design Threat Basis (DTB). The DTB of vehicle size, weight, speed, and pounds or kilograms of equivalent trinitrotoluene (TNT) will be determined based on the USEUCOM threat standard and local force protection teams.

c. Plan Components. The following components must be addressed in writing or illustrated in drawings for each FPCON:

(1) Types and Count. Barrier plans must identify in writing (table format) and on maps the types of barriers (for example, concrete, plastic, jersey barrier, bollard, drop-down bar) and the number of each barrier type required at each emplacement location. Maps in the plans must also identify the location, type, and number of all barriers currently in use.

(2) Storage Location. Locations where barriers are stored (not in use) must be listed.

(3) Purpose. The purpose of barriers at each location must be indicated (for example, using a serpentine route to reduce speed, using plastic barriers to channel traffic for visual inspections, using drop-bars to stop vehicles).

(4) Movement Plan. Resources needed must be identified (forklifts, trucks) to move barriers from one location to another.

(5) Privately Owned Vehicle (POV) Centralized Parking. If applicable, a central location for POV parking and a mass-transportation schedule should be identified both in writing and on drawings.

(6) Traffic Patterns. Any vehicle or pedestrian rerouting due to barrier emplacement must be identified.

d. Subordinate Unit Tasks. The tasks for which each unit is responsible when preparing and executing the barrier plan must be specified. For example:

(1) DPW will provide—

- (a) Supplies according to barrier plans (develop a matrix).
- (b) Representatives during the execution phase.
- (c) An onsite maintenance team for workorder and emergency workorder support.
- (d) Assistance to the DOL with emplacement equipment.

(2) DOL will provide—

- (a) Support and equipment to place barriers, including operators.
- (b) A representative during the execution phase.
- (c) A maintenance team for generator maintenance.

(3) The director of emergency services/provost marshal (DES/PM) will provide—

- (a) Overall development of the barrier plan.
- (b) Representatives to oversee execution and quality control.

(4) Local tenant units will be designated to provide manpower to—

(a) Help with barrier emplacement.

(b) Fill barriers as required (for example, with sand or water).

B-5. RECOMMENDATIONS

a. A barrier plan matrix by FPCON (fig B-1) and by location that specifies the who, what, where, when, and how can be a significant part of a barrier plan, especially when a timeline is included.

b. Barrier-emplacement considerations must include priorities since it is unlikely that enough resources will be available to emplace all barriers simultaneously.

c. While centralized barrier storage appears practical, onsite prepositioning makes more sense. At low FPCONs, if practical, barriers may be doubled up or emplaced double-high or double-wide according to the higher FPCON. It is easier to reconfigure than to draw, haul, and reconfigure.

d. To conserve traffic-control barriers, readily available obstacles should be used effectively (such as boulders and large tree trunks backed by anchored barriers for denial barriers). Plastic water-filled barriers are a greater deterrent when also filled with sand.

e. Denial barriers at choke points are a good measure for lesser-used routes at higher FPCONs.

f. Barriers should be placed on the ground and not on bricks or blocks. Anchoring barriers works better on hard surfaces, while cabling together works better on soft, unprepared surfaces.

g. Barrier plans should be in writing and shown on maps if possible.

h. Alternate support units should be identified in the event that a designated support unit's mission changes or the unit is deployed.

FPCONs Alpha and Bravo				
Timeline: event + hours				
Event	Timeline	Barriers	Resources	Responsible Activities
Barricade two-way traffic into separated lanes at delivery gate.	E+3	8 Jersey concrete barriers	Barriers, forklifts, trucks	DES, DOL, DPW
Restrict access of main entrance to one lane.	E+3	20 Jersey concrete barriers (serpentine)	Barriers, forklifts, trucks	DES, DOL, DPW
Restrict parking areas adjacent to buildings 1, 131, and 345.	E+2	3 temporary drop-down bars	Signs, drop-down bars, trucks	DES, DOL

FPCON Charlie (in addition to FPCON Alpha and Bravo)				
Timeline: event + hours				
Event	Timeline	Barriers	Resources	Responsible Activities
Close both gates 2 and 4.	E+1	Lock gate, raise bollards		DES
Restrict access of main entrance to enter only.	E+3	1 drop-down bar, 4 Jersey concrete barriers, 2 tetrahedrons	Barriers, forklifts, trucks	DES, DOL, DPW
Close parking areas adjacent to buildings 1, 131, and 345.	E+3	18 Jersey plastic barriers	Barriers, trucks	DES, DOL, DPW, Unit X

FPCON Delta (in addition to FPCON Charlie)				
Timeline: event + hours unless otherwise noted				
Event	Timeline	Barriers	Resources	Responsible Activities
Convert traffic loop to one-way traffic.	E+3	10 Jersey plastic barriers	Signs, barriers, trucks	DES, DOL, DPW, Unit X
Enclave military Family housing.	E+6	Wire standoff at 15 meters, 24 Jersey plastic barriers	Wire, posts, barriers, trucks	DES, DOL, DPW, Unit X

Figure B-1. Sample Matrix

i. As appropriate, United States Army garrison public affairs offices will establish notification procedures for any significant parking or traffic-pattern changes within the community.

j. The DTRA concept for barrier plans includes several supporting actions at higher FPCONs such as enclaving, centralized parking, and a curtailment plan.

(1) Enclaving should be used for key on-post (critical or high-occupancy) facilities during higher FPCONs or for grouped buildings that require additional standoff due to physical-security requirements or structural vulnerability.

(2) Centralized parking is a denial measure that limits vehicle access on the installation by creating vehicle-exclusion areas. This may require significant guard and transportation efforts to successfully implement.

(3) A curtailment plan is the planned cessation of nonmission-essential operations. If the conduct of a unit's primary mission is temporarily changed to installation guard or other force-protection measure, a written curtailment plan is in order. If civilian operations, schools, and Family and morale, welfare, and recreation facilities will cease operations and close, this should be included in the curtailment plan.

B-6. USACE ACCESS-CONTROL POINT BARRIERS

The use of vehicle barriers can greatly enhance a commander's force protection posture. Careful consideration must be given to the planning and installation of barriers. Figure B-2 is a sample drawing showing the use of different types of barriers. The DOD Anti-Ram Vehicle Barriers List provides more information (<https://pdc.usace.army.mil/library/BarrierCertification>).



Figure B-2. Sample Drawing Showing Number and Type of Barriers

APPENDIX C

SAMPLE FORMAT FOR PHYSICAL SECURITY STANDING OPERATING PROCEDURE

This appendix provides a sample format that commanders may follow when creating their physical security (PS) standing operating procedure (SOP). The SOP will apply only to those personnel under the supervision of the person signing the SOP.

DEPARTMENT OF THE ARMY
ORGANIZATIONAL NAME/TITLE
STANDARDIZED STREET ADDRESS CITY
STATE 12345-1234

OFFICE SYMBOL

Date

PHYSICAL SECURITY STANDING OPERATING PROCEDURE (SOP)

Applicability. This SOP applies to all personnel in the (*unit*).

Table of Contents (*optional*)

(*Suggested paragraph headings; modify as needed.*)

1. Purpose.
2. References.
3. Responsibilities.
4. Policy.
5. Procedures.

Unit/Activity Commander
Signature Block

1. PURPOSE

This SOP establishes responsibilities and procedures for safeguarding arms, ammunition, and explosives (AA&E); supplies; equipment; and personnel of *unit or activity name*.

2. REFERENCES

- a. AR 190-11.

- b. AR 190-13.
- c. AR 190-51.
- d. AR 710-2.
- e. DA Pamphlet 190-51.
- f. DA Pamphlet 710-2-1.
- g. AE Regulation 190-13.

3. APPLICABILITY

The provisions of this SOP apply to all personnel and units assigned or attached to *unit or activity name* or residing on *installation name*.

4. RESPONSIBILITIES *(suggested position titles, modify as needed)*

a. Unit Commander. The unit commander has overall responsibility for security and accountability of all weapons, ammunition, explosives, supplies, and equipment *assigned/issued* to the *unit/activity*.

b. Physical Security Officer (PSO) and Garrison PSO. *List the duties and responsibilities assigned as listed in paragraph 1-4 of this regulation.*

c. First Sergeant. *List the duties and responsibilities assigned to the first sergeant by the commander based only on PS considerations, if applicable.*

d. Unit Supply Sergeant. *List the duties and responsibilities assigned to the unit supply sergeant by the commander and first sergeant based only on PS considerations, if applicable.*

e. Unit Armorer. *List the duties and responsibilities assigned to the armorer by the commander, first sergeant, and supply sergeant based on PS considerations, if applicable.*

f. Civilian Personnel. *Designate which, if any, civilian personnel have PS duties and specify the duties and responsibilities for each. Use the guidance in this regulation to develop the duties for each individual, such as the primary and alternate key custodian.*

5. ANNEXES. Procedures and responsibilities for each function are indicated as follows:

- a. Annex A.** AA&E.
- b. Annex B.** Security of Property and Equipment.
- c. Annex C.** Key-and-Lock Control.
- d. Annex D.** Emergency Evacuation of Arms and Ammunition.
- e. Annex E.** Electronic Security System (ESS).
- f. Annex F.** Bomb Threat.
- g. Annex G.** In-Transit Security of AA&E, Property, and Equipment.
- h. Annex H.** Security of Arms, Ammunition, Property, and Equipment in a Field Environment.

ANNEX A AA&E

- 1. References.** *List applicable references, such as regulations, field manuals, and other documents relating to the security of AA&E.*
 - 2. Purpose.** This annex establishes the responsibilities, standards, and procedures for securing AA&E in the *unit or activity name*.
 - 3. Applicability.** This annex applies to all personnel assigned or attached to the *unit or activity name*.
 - 4. Responsibilities.** *Specify the duties and responsibilities of the PSO or representative, first sergeant, supply sergeant, armorer, and other personnel relating to the security, issue, and turn-in of AA&E, as applicable.*
 - 5. Procedures.** *Specify the manner in which weapons and ammunition will be stored in racks, containers, or cabinets in the arms room. Indicate key-and-lock control procedures for arms-room keys and all inventory procedures required by regulation. Briefly describe access-control procedures and the requirements for background checks for all personnel authorized unaccompanied access to the arms room by the commander. Briefly address ammunition management procedures or refer those personnel to DA Pamphlet 710-2-1, chapter 11.*
 - 6. Issue and Turn-In Procedures.** *Specify the procedures used by the unit or activity to issue and turn in all weapons (AE Form 190-13I), both individual and crew-served.*
 - 7. Inspections and Inventories.** *Specify which inspections of arms security will be conducted, the frequency and type of inventories that must be completed, and the procedures to follow for recording the results of the inspection and inventories.*
 - 8. Formats and Forms.** *Attach locally formatted samples of the forms required to accomplish all tasks or refer to those in this regulation.*
-

ANNEX B SECURITY OF PROPERTY AND EQUIPMENT

- 1. References.** *List applicable references such as AR 190-51, AR 710-2, DA Pamphlet 710-2-1, and AE Regulation 190-13.*
- 2. Purpose.** This annex establishes the responsibilities, standards, and procedures for safeguarding property and equipment in the *unit or activity name*.
- 3. Applicability.** This annex applies to all personnel assigned or attached to the *unit or activity name*.
- 4. Responsibilities.** *Designate the duties and responsibilities of the PSO or representative, unit supply sergeant, and other personnel with respect to the security of property and equipment to ensure duties and procedures outlined are specifically identified, if applicable.*
- 5. Procedures.** *Follow the risk-analysis procedures in DA Pamphlet 190-51 with assistance from the servicing United States Army garrison (USAG) PSO or applicable agency to determine the level of risk assigned to a facility. Make use of the USAG's services to help fulfill this requirement. When the level of risk is known, adhere to the protective and procedural measures in AR 190-51. The SOP need only refer to AR 190-51, chapter 3, for personnel to determine the protective and procedural standards associated with each category of property and equipment.*

ANNEX C KEY-AND-LOCK CONTROL

1. References. *List applicable references, such as AR 190-11, AR 190-51, and AE Regulation 190-13.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for identification and control of all locks, keys, and combinations used in the security of AA&E, property, and equipment. *Use chapters 3 and 5 of this regulation to develop this annex.*

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the responsibilities of the PSO and key/lock primary and alternate custodians, and ensure that the specific functions described in chapters 3 and 5 of this regulation are addressed.*

5. Procedures. *Describe how the PSO or representative and key custodian will be appointed and how storage facilities and containers will be identified for controlled locking devices. Describe how the locking devices will be identified for inclusion in the control system and how individual Soldiers will be authorized issue of keys, locks, and combinations. Include information on the temporary issue of keys, those used for personal retention by limited individuals, and the type of containers where the key custodian will secure the locks, keys, or combinations in their custody.*

ANNEX D EMERGENCY EVACUATION OF ARMS AND AMMUNITION

1. References. *List applicable references, such as AR 190-11 and AE Regulation 190-13.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for the emergency evacuation of arms and ammunition to a secure location in the event of a threat to the security of the arms and ammunition.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the duties of the PSO or representative, civilian personnel, and unit personnel responsible for the emergency evacuation of weapons and ammunition.*

5. Procedures. *Identify the conditions for the emergency removal of arms and ammunition, the manner of removal, the security precautions to be used during the transportation of the arms and ammunition, the location to which the arms and ammunition will be taken, the routes to be used, and which inventory and inspection procedures to initiate to ensure that all arms and ammunition are properly accounted for during and after the evacuation.*

6. Test. *The personnel responsible for implementation must test these procedures and record the results. Testing personnel will help correct weaknesses or forward a list of weaknesses, if necessary, to higher command levels for help with resolving them. Normally, tests are conducted without moving the arms or ammunition.*

ANNEX E ELECTRONIC SECURITY SYSTEM (ESS)

- 1. References.** *List applicable references such as AR 190-11, AR 190-13, and AE Regulation 190-13.*
 - 2. Purpose.** This annex establishes the responsibilities, standards, and procedures for the operation of the ESS in the *unit or activity name* arms room.
 - 3. Applicability.** This annex applies to all personnel assigned or attached to the *unit or activity name*.
 - 4. Responsibilities.** *Specify the responsibilities of the PSO or representative, supply sergeant, key custodian, and civilian personnel with respect to the control and operation of the ESS.*
 - 5. Procedures.** *Specify the procedures to be used by unit personnel for the placement of warning signs, operation of the ESS, control of ESS keys, inspections, checks, and tests of the ESS, and the documentation of such inspections, checks, and tests, both by unit personnel and the agency monitoring the system. Also identify what the unit personnel must do if the ESS alarm fails (armed-guard requirements, relocation of weapons).*
 - 6. Forms and Formats.** *See chapters 2, 3, and 5 for samples of support documentation.*
-

ANNEX F BOMB THREAT

- 1. References.** *List applicable references such as AR 190-13 and AE Regulation 190-13.*
- 2. Purpose.** This annex establishes the responsibilities, standards, and procedures to be used in the event of a bomb threat against the *unit or activity name*.
- 3. Applicability.** This annex applies to all personnel attached or assigned to the *unit or activity name*.
- 4. Responsibilities.** *Specify the duties and responsibilities of the PSO or representative, civilian personnel, and unit personnel regarding bomb threats.*
- 5. Procedures.** *Specify the internal notification, external notification, and evacuation procedures to be followed in the event of a bomb threat at the unit or facility.*
- 6. Forms and Formats.** *Use AE Form 525-13A for telephonic threats. These cards may be ordered through normal publication channels.*
- 7. Serious Incident Reports (SIRs).** *Meet the SIR requirements in AR 190-45 and in local command procedures.*

ANNEX G IN-TRANSIT SECURITY OF AA&E, PROPERTY, AND EQUIPMENT

1. References. *List applicable references such as AR 190-11, DA Pamphlet 710-2-1, AE Regulation 55-4, and AE Regulation 190-13.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures to be used to secure AA&E, property, and equipment during transportation.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the duties and responsibilities of the PSO or representative, unit supply sergeant, armorer, civilian personnel, and convoy commander with respect to the security of AA&E, property, and equipment while in transit.*

5. Procedures. *Specify the vehicles in which AA&E, property, and equipment may be transported, the specific type of equipment, arms, or ammunition requiring security during transit, the requirement for armed guards (if applicable), the types and number of locks required to secure the equipment, the number of personnel and their grade needed to accomplish the mission, and inventory and accountability procedures to be used from start to completion of the mission.*

ANNEX H SECURITY OF ARMS, AMMUNITION, PROPERTY, AND EQUIPMENT IN A FIELD ENVIRONMENT

1. References. *List applicable regulations such as AR 190-11, DA Pamphlet 710-2-1, and AE Regulation 190-13.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for securing arms, ammunition, property, and equipment in a field environment.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the duties and responsibilities of the unit PSO or representative, first sergeant, armorer, key custodian, civilian personnel, and individual Soldiers for securing arms, ammunition, property, and equipment in a field environment.*

5. Procedures. *Specify the procedures to be used for securing arms, ammunition, property, and equipment while in a controlled, consolidated location when issued to the individual Soldier. Make specific reference to the manner by which the individual Soldier is expected to secure his or her weapon and ammunition. Develop separate inventory and key-and-lock procedures for the field environment.*

GLOSSARY

21st TSC	21st Theater Sustainment Command
AA&E	arms, ammunition, and explosives
ACoS	assistant chief of staff
ACP	access-control point
AE	Army in Europe
AEPUBS	Army in Europe Library & Publishing System
ALARACT	all Army activities
AOR	area of responsibility
APSEAG	Army Physical Security Equipment Action Group
AR	Army regulation
AT/FP	antiterrorism/force protection
ATWG	antiterrorism working group
CCTV	closed-circuit television
CG, USAREUR	Commanding General, United States Army Europe
COE	Center of Expertise
COMSEC	communications security
COR	contracting officer's representative
DA	Department of the Army
DES	director(ate) of emergency services
DES/PM	director of emergency services/provost marshal
DOD	Department of Defense
DOL	director of logistics
DPW	director(ate) of public works
DTB	design threat basis
DTRA	Defense Threat Reduction Agency
EECS	electronic entry/access control system
ESS	electronic security system
FP	force protection
FPCON	force protection condition
FP/PS	force protection/physical security
G1	Office of the G1, Headquarters, United States Army Europe
G2	Deputy Chief of Staff, G2, United States Army Europe
G3/5/7	Deputy Chief of Staff, G3/5/7, United States Army Europe
G6	Deputy Chief of Staff, G6, United States Army Europe
G8	Deputy Chief of Staff, G8, United States Army Europe
GENADMIN	general administration
HDT	high-density target
HN	host nation
HQDA	Headquarters, Department of the Army
HQ USAREUR	Headquarters, United States Army Europe
HRP	high-risk personnel
HRT	high-risk target
HVT	high-value target
IACP	installation access control point
IACS	Installation Access Control System
IDS	intrusion-detection system
IMCOM-Europe	United States Army Installation Management Command, Europe Region

IS	information system
MEVA	mission-essential vulnerable area
MP	military police
NCO	noncommissioned officer
OIP	organizational inspection program
OPORD	operation order
PIN	personal identification number
PM	Provost Marshal, United States Army Europe
PMD	Provost Marshal Division, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, Headquarters, United States Army Europe
PM-FPS	Product Manager-Force Protection Systems
POC	point of contact
PS	physical security
PSE	physical security equipment
PSI	physical security inspection
PSMS	Physical Security Management System
PSO	physical security officer
PSVA	personal security vulnerability assessment
PWS	performance work statement
SAV	staff assessment visit
SCOR	site contracting officer's representative
SEWG	United States Army Europe Security Equipment Working Group
SIR	serious incident report
SMS	Security Management System
SOAB	Security Operations and Assessments Branch, Provost Marshal Division, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, Headquarters, United States Army Europe
SOP	standing operating procedure
TASKORD	tasking order
TNT	trinitrotoluene
U.S.	United States
USACE	United States Army Corps of Engineers
USACIDC	United States Army Criminal Investigation Command
USAG	United States Army garrison
USAINSCOM	United States Army Intelligence and Security Command
USAREUR	United States Army Europe
USAREUR G34	G34 Protect Directorate, Office of the Deputy Chief of Staff, G3/5/7, Headquarters, United States Army Europe
USEUCOM	United States European Command