Army Regulation 190–13

Military Police

The Army Physical Security Program

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

Headquarters
Department of the Army
Washington, DC
27 June 2019

FOR OFFICIAL USE ONLY

SUMMARY of CHANGE

AR 190–13
The Army Physical Security Program

This major revision, dated 27 June 2019—

- Updates responsibilities (chap 1).
- Implements the U.S. Military Police Security Management System (Counter Measures) and mandates use to document physical security inspections (para 1–10*h*).
- Extends the time period from 60 to 90 days for deficiencies that are correctable before a waiver to policy must be submitted (para 2–3*b*(1)(*a*)).
- Adds a requirement that Army commands, Army service component commands, direct reporting units, and the Army National Guard have a physical security plan, and provides a format (para 2–8*a* and app B).
- Revises the list of facilities that can be designated as mission essential vulnerable areas (para 2–11*d*).
- Changes the inspection period from 24 to 18 months for conventional arms, ammunition, and explosives bulk storage, nuclear reactors, special nuclear materials, chemical agents, and biological select agents and toxins (paras 2–15*c*(1) through (3)).
- Establishes a personnel reliability screening and evaluation program (para 2–21).
- Moves policy on physical security protection requirements for high-risk personnel from AR 190–51 to this regulation (para 2–22).
- Provides instruction and guidance for the Department of Defense Security Professional Education Development certification program (para 3–8).
- Removes the warning sign for site perimeters, and extends the use of the warning sign at figure 6–1 to include use at site perimeters (para 6–7).
- Revises policies on the survivor access card and incorporates AD 2014–05, which provides fitness adjudication standards and procedures for installation access control (paras 8–4 and 8–5).
- Provides guidance on how to manage and use small, unmanned aircraft systems on, or near, installations (chap 11).
- Revises the format for physical security plans for installations, stand-alone facilities, and units (app C).
- Provides a format for the barracks physical security plan (app D).
- Provides instructions to complete a DA Form 7708 (app E).
- Provides manning factors for installation access control points (app F).
- Provides requirements to maintain and test systems and equipment at installation access control points (app G).
- Provides procedures for the monthly operational test of an intrusion detection system (app H).

Headquarters
Department of the Army
Washington, DC
27 June 2019

*Army Regulation 190–13

Effective 27 July 2019

Military Police

The Army Physical Security Program

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation implements Department of Defense Instruction 5200.08, Department of Defense Instruction 3224.03, and Army Directive 2014-05. It prescribes policies and procedures to plan and implement the Department of the Army Physical Security Program. It provides policies on how to use physical security equipment; appoint physical security officers and inspectors; conduct physical security inspections and surveys; manage physical security credentials; manage and use identification cards and badges; manage restricted areas; conduct access control for installations and stand-alone facilities; and manage security forces.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to Government-owned and Government-operated activities.

Proponent and exception authority. The proponent of this regulation is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. This approval authority is delegated to the Chief, Office of the Provost Marshal General, Operations Division. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander, director, or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to paragraph 2–3 of this regulation for specific guidance.

Army internal control process. This regulation contains internal controls and identifies key internal controls that must be evaluated (app J).

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

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Provost Marshal General (DAPM–MPO–PS), 2800 Army Pentagon, Washington, DC 20310–2800 or usarmy.pentagon.hqda-pmg.list.ps@mail.mil.

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

Contents (Listed by paragraph and page number)

* This regulation supersedes AR 190–13, dated 25 February 2011.

Table List

Figure List

Glossary

Chapter 1
Introduction

Section I

General

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

1–2. Reference and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Responsibilities
See section II of this chapter.

1–5. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in the Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

Section II

Responsibilities

1–6. Assistant Secretary of the Army (Acquisition, Logistics and Technology)
The ASA (ALT) will—

a. Coordinate early in the research, development, and acquisition process concerning physical security requirements for Army materiel.

b. Establish an integrated logistics support program for centrally managed, physical security equipment (PSE) per AR 700–127.

c. Provide one nonvoting advisor (in the rank of major, lieutenant colonel, or civilian equivalent (CE)) to the Army Physical Security Equipment Action Group (APSEAG) per paragraph 7–2.

1–7. Assistant Secretary of the Army (Civil Works)
The ASA(CW) will ensure physical security requirements are included in U.S. Army Corps of Engineers (USACE) civil works and like projects.

1–8. Assistant Secretary of the Army (Installations, Energy and Environment)
The ASA(IE&E) will—

a. Program physical security requirements in military construction projects through a formal process.

b. Coordinate PSE requirements funded by Other Procurement, Army with the Provost Marshal General and the Commanding General (CG), U.S. Army Corps of Engineers.

c. Incorporate physical security standards as part of facility designs.

d. In connection with the Office of the Provost Marshal General (OPMG) revise the Army Access Control Point Standard as required.

1–9. Assistant Secretary of the Army (Manpower and Reserve Affairs)
The ASA(M&RA) will—

a. Oversee OPMG operations per DAGO 2017-01.

b. Coordinate and document Army implementation of Homeland Security Presidential Directive 12 (HSPD-12) requirements per AD 2011-08.

1–10. Provost Marshal General

The PMG is the Army Staff principal officer responsible for the Army physical security program and is the functional chief of the Career Program (CP) 19 (CP19). Under the PMG, the Chief, Operations (DAPM–MPO) will—

a. Develop policies, goals, and objectives for the program.

b. Coordinate physical security policy to ensure integration and synchronization with other programs.

c. Coordinate with the Army Staff and other Army elements when establishing physical security policies, procedures, and standards.

d. Approve waivers and exceptions to this regulation when determined to be appropriate.

e. Validate, prioritize, and program the Army's physical security resource requirements.

f. Coordinate the process of a business case analysis to determine the feasibility of multi-site maintenance for contracts and multi-site monitoring of intrusion detection systems (IDS).

g. Centrally plan and direct certain PSE efforts.

h. Implement the web-based Security Management System (CounterMeasures) (SMS(CM)).

i. Provide one voting member and one alternate voting member to represent the Army in the DOD Physical Security Enterprise and Analysis Group.

j. Provide one voting member to the APSEAG, per paragraph 7–2.

k. Provide one voting member to the DOD Physical Security Requirements Group, who will also chair it as the responsibility rotates among the Military Departments, per DOD Instruction 3224.3.

l. Provide a physical security subject matter expert (SME) to support the Army Protection Program Assessments of physical security programs for Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs).

m. Provide SME oversight for the management of Army physical security IT systems.

n. Provide a non-voting physical security SME to attend the DOD Security Enterprise Assessment Group meetings.

o. In support of the Army Insider Threat Program, develop a capability to initially vet visitors and continuously vet all personnel for access to Army facilities against authoritative U.S. Government databases to identify potential criminals, terrorists, or other security and insider threats.

p. Oversee and advocate for the continued professionalization of the CP19 work force in accordance with Executive Order 13434, AR 350-1, and AR 690-950.

1–11. Deputy Chief of Staff, G–1

The DCS, G–1 will provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

1–12. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Provide intelligence and counterintelligence functions in support of physical security programs and planning, related to protecting Army personnel, materiel, facilities, and operations from espionage, sabotage, criminal activity, subversion, terrorism, and sedition.

b. Identify threats that may increase physical security requirements.

c. Coordinate with the CG, USACE to ensure the threat definition is uniform and sufficiently specified to serve as a basis for physical security requirements in construction design.

d. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

e. As the Army representative to the DOD Security Enterprise Assessment Group, consider the OPMG physical security SME's input.

1–13. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG per paragraph 7–2.

1–14. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Provide copies of surveys, inventory adjustments, and reports that indicate actual or possible criminal activities to HQDA (DAPM–MPO–PS) and CG, U.S. Army Criminal Investigation Command upon request by the PMG.

b. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

c. Coordinate supply accountability and Command Supply Discipline Program policies with PMG.

1–15. Chief Information Officer/G–6

The CIO/G–6 will—

a. Support and help the PMG gain authorization to operate information technology (IT) based PSE and electronic security systems (ESS), under the Department of Defense Risk Management Framework (DOD RMF).

b. Coordinate with the PMG for other IT-supporting physical security, to include—

(1) Interoperability of common access card (CAC) attributes in computerized card or badge systems.

(2) Validity of CAC attributes against established DOD and Army information databases.

(3) Authenticity of CAC and CAC holder, using match-on-card and anti-counterfeit protection measures embedded in the CAC.

c. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

1–16. Assistant Chief of Staff for Installation Management

The ACSIM will—

a. Program physical security requirements in military construction through a formal process.

b. Establish a formal process to coordinate with the CG, USACE to plan, evaluate, apply, design, install, and construct facility enhancements for all aspects of physical security and antiterrorism-protective construction, through the mandatory centers of expertise, per paragraph 1–20.

c. Coordinate with the PMG on construction policies and design standards that may impact physical security.

d. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

1–17. The Inspector General

The Inspector General will provide follow up inspections to ensure compliance with Secretary of the Army direction to senior commanders (SC) to vet visitors, control access to installations, and secure installations to detect criminals, terrorists, and insider threats.

1–18. The Surgeon General

The Surgeon General will—

a. Provide technical assistance to the PMG concerning physical security policy for medical resources and facilities.

b. Establish a formal oversight process for the U.S. Army Health Facilities Planning Agency, to ensure physical security requirements are incorporated when building Army medical facilities.

c. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

1–19. Chief of Engineers

The COE will—

a. Establish a formal process to ensure physical security design criteria are considered for proposed construction projects in compliance with Army military construction policy.

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

c. Provide administrative and technical advice and assistance, and make recommendations on physical security construction matters to the ASA (IE&E), the PMG, and other principal Army Staff officers.

1–20. Commanding General, U.S. Army Corps of Engineers

The CG, USACE will—

a. Coordinate with the ACSIM to properly plan, evaluate, apply, design, install, and build facility enhancements for all aspects of physical security and antiterrorism-protective construction, through the mandatory centers of expertise in paragraph 1–20*h*.

b. Provide criteria and guidance for the proper design, installation, and acceptance testing of commercial IDS and other ESS installed in construction projects, where required. This requirement does not apply to DOD and DA standardized systems.

c. Develop and maintain guidance and criteria documents, and provide training on how to plan, evaluate, apply, design, install, and build projects requiring physical security-related, protective construction and equipment. Designs will incorporate protective construction criteria, ESS, IDS, and other PSE, as required.

d. Develop requirements and execute programs for research and development efforts supporting physical security-related, protective construction and PSE applications for protective construction.

e. Identify problem areas that might impact the design and installation of IDS and other PSE.

f. Coordinate security engineering surveys with the local provost marshal (PM), director of emergency services (DES), or senior physical security officer (PSO) for surveys conducted for the U.S. Army Recruiting Command and U.S. Army Cadet Command.

g. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

h. Maintain the Protective Design Center (PDC) and the Electronic Security Center (ESC) as mandatory centers of expertise for protective design and electronic security system (ESS) technical expertise to Army organizations.

(1) The Protective Design Center will help the OPMG review, analyze, and apply facilities standards and criteria to meet physical security, antiterrorism, and other protection policies and objectives.

(2) The Electronic Security Center will help OPMG review, analyze, and apply of facilities standards and criteria to comply with policies and meet objectives for IDS and ESS. The review will include a process to identify and cost IDS/ESS requirements for military construction, coordinating as needed with USACE offices, master planners, and other stakeholders to ensure construction plans are correct, equipment installation procurement costs are accurate, and equipment does not exceed policy requirements.

i. The Protective Design Center and Electronic Security Center each will provide one nonvoting advisor (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG per paragraph 7–2.

j. Ensure commanders and directors of divisions and districts, responsible for civil works and like projects, comply with requirements in paragraph 1–24.

1–21. Chief, Army Reserve

The CAR will—

a. Establish standards, criteria, and metrics for ESS and other PSE that meet the capabilities required for Army Reserve off-installation and standalone facilities (SAFs).

b. Plan, program, budget, and execute physical security and ESS requirements consistent with this regulation and in accordance with Army Reserve standards, criteria, and metrics.

c. Ensure ESS technology implementation complies with Risk Management Framework (RMF) requirements.

d. Program physical security and PSE requirements, including IDS, access control systems (ACS), and other electronic security systems (ESS) in all military construction, Army Reserve (MCAR) projects to ensure physical security requirements are incorporated when building Army Reserve facilities.

e. Provide one voting member (O-5 or CE) to the APSEAG, per paragraph 7–2.

1–22. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC is the user's representative to develop Army concepts and supports Joint concept development through proponents. As such, the CG, TRADOC will—

a. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

b. Through the Commander, Maneuver Support Center of Excellence—

(1) Formulate concepts, doctrine, organizational structure, materiel objectives, and requirements to employ U.S. Army forces in a theater of operation, in control of civil disturbances, to secure garrisons, and to combat terrorism.

(2) Develop physical security concepts and determine the actions necessary to implement them as they impact Army doctrine, organization, training, materiel, leadership and education, personnel, and facilities.

(3) Conduct Army physical security experimentation, user evaluations, and military utility assessments of IDS and other PSE.

(4) Provide training and doctrine support in developing physical security procedures and measures.

(5) Comply with AR 71–9 to ensure that materiel, training, personnel, logistics, doctrine, tactics, and essential system requirements for a PSE item are identified, integrated early, tested, and refined throughout the materiel acquisition process.

(6) Ensure the requirements above are included in requirements documents, development contracts, tests, evaluations, and other key actions in the acquisition of materiel systems.

(7) Ensure physical security requirements and related subsystems, measures, and procedures are identified in the developmental process for new materiel systems in coordination with the product manager, Force Protection Systems, and as an integral part of the combat development process.

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

(9) In conjunction with the user representative for specified physical security requirements, develop operational concepts and plans to improve the physical security posture of the Army; and, when appropriate, to implement physical security policy as established by HQDA (DAPM–MPO–PS).

(10) Determine PSE research, development, test, and evaluation requirements designed to correct for deficiencies. Implement approved physical security operational concepts and plans.

(11) Coordinate with other Army elements to identify PSE requirements and coordinate the preparation and staffing of capability needs statements.

(12) Resource the conventional physical security/crime prevention course (7H–31D/830–ASIH3) at a level required to satisfy training requirements for Service members and Government civilians.

(13) Provide one nonvoting advisor (in the rank of major, lieutenant colonel, or civilian equivalent) to the Army voting member for the DOD Joint Requirements Working Group.

(14) Provide one nonvoting advisor (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

c. Through the Army Capabilities Integration Center director, determine future Army PSE requirements.

1–23. Directors and supervisors of Army staff agencies and commanders or directors of Army organizations not on military garrisons

These commanders and directors are responsible for physical security within their activities per applicable Army policy. Coordination for support with the nearest Army physical security office is recommended.

1–24. Senior commanders, directors, and managers appointed per AR 600–20

The senior commanders, directors, and managers will—

a. Establish a command physical security program to coordinate physical security matters across the command to ensure practical, effective, and common sense measures are used.

b. Establish a written command physical security plan per appendix B to operationalize Army physical security policies.

c. Issue formal written orders appointing a command PSO per paragraph 3–1 to be the single point of contact for all command physical security matters.

d. Establish a formal command management assessment program to ensure compliance with requirements, and meet oversight and audit responsibilities per AR 525-2.

e. Ensure compliance with applicable physical security regulations by assessing subordinate organizations.

f. Coordinate with the land-managing command for results of physical security inspections.

g. Will use SMS(CM) per paragraph 2–13.

h. Coordinate threat information across the command and with other senior commanders, directors, and managers, as applicable.

i. Provide command guidance to subordinate organizations to ensure program compliance per paragraph 2–12.

j. Prioritize physical security resource requirements identified by the supporting garrison commander or director.

k. Control access to installations to include vetting visitor personnel and adjudicating the denial and waiver process in accordance with chapter 8 of this regulation. This responsibility may be delegated in writing to the garrison commander or director.

l. Review all waivers and exceptions as required by paragraph 2–3 of this regulation and revise as required. A brief statement affirming currency of all command waivers and exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM-MPO-PS) 2800 Army Pentagon, Washington, DC 20310-2800.

m. Establish a local policy, program, base orders or procedures to inform military, dependent, and civilian employees who are sUAS hobbyists of the established local policy, program, installation order or procedure in regards to sUAS.

1–25. Commanders and directors of Army commands, Army service component commands, direct reporting units, U.S. Army Corps of Engineers, and the Chief, National Guard Bureau

These commanders and directors will—

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

b. Establish a formal physical security program consistent with this regulation by means of a written physical security plan per appendix B. The command physical security plan will be used to operationalize Army physical security policies for the command.

c. Establish a barracks physical security plan per appendix D appropriate for the command (for example, an environment of permanent party or trainees or other unique factors), and implement consistent use across the command. Leaders will actively monitor barracks security to afford Soldiers a secure housing environment.

d. Issue formal written orders appointing a command PSO per paragraph 3–1 to be the single point of contact for all command physical security matters.

e. Establish a formal command management assessment program to ensure compliance with requirements and meet oversight and audit responsibilities per AR 525-2.

f. Review, approve, and maintain a copy of the physical security plans of supported organizations, installations, and SAFs.

g. Validate and prioritize physical security resource requirements identified by subordinate organizations.

h. Implement approved physical security operational concepts and plans.

i. Coordinate with TRADOC as the user's representative and with the product manager, Force Protection Systems as the Army physical security materiel developer when an operational need is identified for PSE performance requirements.

j. Will use SMS(CM) per paragraph 2–13.

k. Review threat statements prepared for installations activities and SAFs for content and accuracy.

l. Ensure engineers, physical security personnel, and antiterrorism personnel coordinate design criteria for new construction projects and document the coordination on DD 1391 (Military Construction Project Data) for military funded construction projects.

m. Ensure physical security personnel track construction projects at every milestone of the planning, design, and construction process and document the tracking process.

n. Implement procedures for the issue, control, accountability, and destruction of physical security inspector credentials.

o. Ensure designated personnel qualified per paragraph 3–2 are issued inspector credentials for the duration of their deployment tour or civilian employment. Ensure issued credentials are recovered and accounted for per paragraph 3–5 after deployment or civilian employment.

p. Establish a formal process to record, track, and resolve deficiencies found during physical security inspections and surveys.

q. Provide one voting member (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG per paragraph 7–2.

r. Approve the purchase, issue, lease, or lease renewal of non-standard PSE. Establish internal procedures for the request and approval process. This authority will not be further delegated.

s. USACE commanders and directors will apply these requirements to USACE laboratories, field operating activities (FOAs), centers, divisions, districts, and USACE civil works and like projects.

t. State adjutants general will establish a physical security program per this paragraph, and coordinate requirements with C, NGB or the chief's designee to ensure program synchronization and efficiency.

u. Review and revise all waivers and exceptions as required by paragraph 2–3 of this regulation. A brief statement affirming currency of all command waivers and exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM-MPO-PS) 2800 Army Pentagon, Washington, DC 20310-2800.

v. Establish a local policy, program, base orders or procedures to inform military, dependent, and civilian employees who are sUAS hobbyists of the established local policy, program, installation order or procedure in regards to sUAS.

w. Mission Area Domain portfolio managers make it easier to use the Army Portfolio Management System (APMS) for IT-based ESS.

1–26. Product manager, force protection systems

The product manager, force protection systems (PdM-FPS) will—

a. Practice centralized research, development, and acquisition management of PSE for Army use, and for PSE developed by the Army for Joint Service applications per DODI 3224.03.

b. Manage PSE projects as assigned per the management standards of AR 70–1 and AR 700–127.

c. Apply AR 700–127 requirements to projects resourced by OPMG when a business case analysis indicates a financial benefit.

d. Implement and sustain post-award competition.

e. Ensure site surveys conducted for installation of the Integrated Commercial Intrusion Detection System (ICIDS) identify resources having regulatory requirements for IDS. If additional local requirements are identified beyond those established by policy, segregate them in planning documents for evaluation.

f. Develop and implement standard design templates for common type new facilities to the extent feasible. Information on standard Army standards and standard designs can be found at https://mrsi.erdc.dren.mil/cos/.

g. Maintain a catalog of design templates to ease installation of ICIDS in future Army facilities.

h. Serve as the Army representative to the Joint Service Security Equipment Integration Working Group.

i. Serve as a technical advisor to the Army representative at the DOD Physical Security Enterprise & Analysis Group and the Joint Requirements Working Group.

j. Assist OPMG to acquire, procure, deploy and install certain PSE items, provide quarterly performance briefings concerning execution of the plan and coordinate business processes.

k. Provide one voting advisor (in the rank of major, lieutenant colonel, or civilian equivalent) to the APSEAG, per paragraph 7–2.

1–27. Commanders and directors with mission command responsibility for Army-managed Armed Forces Reserve Centers, Army Reserve Centers, Army National Guard Armories, and similar Army stand-alone facilities subject to DA jurisdiction or administration, or in DA custody

These commanders and directors will—

a. Direct physical security policy and publish a physical security plan per appendix C.

b. Protect personnel and property in their commands and on their facilities against trespass, terrorism, sabotage, theft, arson, and other illegal acts, and secure personnel, places, and property under their command per this regulation and Title 50 USC 797. An adequate security posture will be determined by considering—

(1) The types of activity areas or resources and their criticality to the mission.

(2) Current threats to the installation or activity area, including trespassing, terrorism, sabotage, theft, arson, and other illegal acts.

(3) The vulnerability of the installation or activity including construction and physical layout of the area, geographical location, and social and political environment.

c. In writing, designate restricted areas per chapter 6.

d. In writing, designate mission essential vulnerable areas (MEVA) under their control as identified by the senior law enforcement officer or PSO.

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

f. Direct the establishment of a local physical security council (PSC) for Reserve Component (RC) SAFs, per paragraph 7–1. The heads of the RCs may authorize the establishment of the PSC at a higher level of command or organization as an exception due to unique circumstances.

g. Direct the organization responsible for threat assessments to—

(1) Develop an installation or activity threat statement in coordination with the PSO, local intelligence and law enforcement support elements, based on support elements, based on higher HQ threat statements. or combatant command threat statements.

(2) Handle threat information in accordance with AR 380–13 and AR 381–10.

(3) Pass threat information to all military activities on and off the installation as well as to all SAF tenant units and activities and other military activities in proximity to the SAF.

h. Ensure the written appointment of a SAF PSO by the local responsible commander at each SAF. The heads of the RCs may authorize the appointment of a SAF PSO at a higher level of the command or organization as an exception due to unique circumstances.

i. Will use SMS(CM) per paragraph 2–13.

j. Include physical security as an annex to all orders and plans as required.

k. Provide information about the organization and its activities to the supporting military intelligence element as needed for the force protection mission.

l. Provide physical security support when requested by tenant activities.

m. Ensure physical security programs provide for safeguarding Army resources—personnel, information, equipment, facilities, activities, and operations at all times (pre-mobilization, mobilization, and deployment).

n. Ensure personnel meeting the qualification requirements in paragraph 3–2 conduct physical security surveys per paragraph 2–14 and/or physical security inspections per paragraph 2–15 covering Army resources in SAFs.

o. Perform risk analysis per DA Pam 190–51 for new and existing facilities.

p. Control access to installations to include vetting visitor personnel and adjudicating the waiver denial and waiver process in accordance with chapter 8 of this regulation. SAFs without NCIC-III access will escort non CAC-holding visitors at all times.

q. Review all waivers and exceptions as required by para 2–3 of this regulation and revise as required. A brief statement affirming currency of all command waivers and exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM-MPO-PS) 2800 Army Pentagon, Washington, DC 20310–2800.

r. Establish a local policy, program, base orders or procedures to inform military, dependent, and civilian employees whom are sUAS hobbyists of the established local policy, program, Installation order or procedure in regards to sUAS.

s. RC commanders and directors of Army organizations not on military garrisons will coordinate physical security per RC policies and mission command relationships.

1–28. Commanders and directors of installation garrisons and Army-led Joint bases, and commanders of tenant units on Army installations and Army-led Joint bases

a. Garrison commanders, directors, and equivalent civilian leaders will—

(1) Direct physical security policy and publish a physical security plan per appendix C.

(2) Issue formal written orders appointing a command PSO per paragraph 3–1 to be the single point of contact for all physical security matters.

(3) Direct the execution of installation access control operations in accordance with chapter 8.

(4) Designate restricted areas in writing per chapter 6.

(5) Designate MEVAs under their control as identified by the senior law enforcement officer or PSO in writing.

(6) Designate and prioritize MEVAs in writing.

(7) Provide law enforcement or guard patrols as required to protect personnel and government resources.

(8) Install, operate, and maintain IDS and other PSE as required per AR 37–49 for reimbursable costs.

(9) Respond to IDS alarms.

(10) Will use SMS(CM) per paragraph 2–13.

(11) Conduct physical security surveys and inspections per paragraph 2–14 and 2–15.

(12) Provide a copy of the inspection report to the commander, director, and, when applicable, the Installation Management Command (IMCOM) PSO.

(13) Coordinate physical security resource requirements with the senior commander or director.

(14) Convene the physical Security Council per paragraph 7–1.

(15) Coordinate barracks physical security measures with tenant commanders or directors.

(16) Control access to installations to include vetting visitor personnel and adjudicating the waiver denial and waiver process in accordance with chapter 8 of this regulation.

(17) Test and maintain equipment at installation access control points (IACPs), per appendix G.

(18) Review all waivers and exceptions as required by paragraph 2–3 of this regulation and revise as required. A brief statement affirming currency of all command waivers and exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM–MPO–PS) 2800 Army Pentagon, Washington, DC 20310–2800.

b. Tenant commanders, directors, and equivalent civilian leaders will—

(1) Exercise their inherent responsibility to secure organization resources.

(2) Provide entry control to their facilities.

(3) Provide Soldiers or other personnel to supplement the security forces for the garrison common defense plan where required by policy.

(4) Publish a physical security plan or standard operating procedure per appendix C.

(5) Ensure PSOs are appointed in writing commands battalion and above, unit, and activity level.

(6) Request physical security support beyond their means from the garrison commander/director consistent with common levels of support.

(7) Inform the garrison commander or director of all physical security measures in effect.

(8) Designate MEVAs in writing and forward the list to the garrison commander or director for inclusion in the installation physical security plan.

(9) Coordinate unit physical security plans with the garrison commander or director.

(10) Forward a copy of physical security plans to the garrison commander or director for inclusion as an annex in the installation physical security plan.

(11) Develop a barracks physical security plan using the format at appendix D and coordinate the plan with the garrison commander or director.

1–29. Installation and activity provost marshals, directors of emergency services, or physical security officers

The PMs, DES, or PSOs—

a. Assess installation physical security needs by conducting physical security surveys, per paragraph 2–14, and physical security inspections, per paragraph 2–15.

b. Will use SMS(CM) per paragraph 2–13.

c. Recommend physical security and antiterrorism design considerations in the preparation of installation engineer construction projects for new construction, renovation, modification, or lease acquisition.

d. Serve as the installation or activity single PSE point of contact for units under control of and within the area of responsibility of the installation, garrison, or command activity. Ensure coordination of equipment requirements with users, engineers, logistics, and communications personnel.

e. Provide technical support to the organization responsible for threat assessments.

f. Monitor resource management of the installation or USACE civil works and like projects physical security program. Plan and program necessary resources for physical security projects in the program budget cycle in coordination with the comptroller or USACE civil works and like projects business line managers.

g. Submit physical security resource requirements to comply with Army physical security policy direction.

h. Coordinate physical security with operations security and antiterrorism officers.

i. Coordinate with engineers during the planning, design, and construction of all projects to identify physical security requirements, including supporting communications, and to ensure the requirements are incorporated into the projects at the inception of the project planning. Ensure that all access control point projects are designed in accordance with the Army access control points (ACP) standard and reviewed by the Center of Standardization (COS) for Access Control Points and USACE Protective Design Center.

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

k. Provide an advisor to engineer planning and design charrettes.

l. Review all waivers and exceptions as required by paragraph 2–3 of this regulation and revise as required. A brief statement affirming currency of all command waivers and exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM-MPO-PS) 2800 Army Pentagon, Washington, DC 20310-2800.

m. Execute and oversee installation and SAFs access control to include vetting visitor personnel and carrying out denial and waiver process decisions in accordance with chapter 8 of this regulation.

n. Oversee the training and execution of access control operations by security forces.

1–30. Installation, garrison and activity engineers and master planners

Engineers and planners will—

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

b. Coordinate the review of all planning documents and construction plans and specifications at all stages of their development with the PM, DES, or PSO.

c. Program PSE for military construction in tab E of the DD Form 1391, and program the cost to install PSE in tab A of the DD Form 1391 (Military Construction Project Data).

1–31. Career Program 19 (Physical Security and Law Enforcement) functional chief representative and career program manager

The CP19 functional chief representative and career program manager (CPM) will—

a. Provide Career Program management of the DA Civilian security professionals in the occupational series 0080, 0086, 0085, and 0301, as applicable.

(1) Maintain the Army Civilian Training Education Development System (ACTEDS) Plan.

(2) Develop and maintain career ladders, paths, and career maps.

(3) Manage developmental assignments and the CP19 Intern Program.

(4) Coordinate funding and policy with DCS, G-3/5/7 Civilian Training and Leader Development Division and ASA (M&RA)/AG1-CP.

(5) Budget and fund competitive professional development opportunities to support critical skills and competencies.

b. Conduct strategic human capital planning for CP19 security professionals, as the component functional community manager.

(1) Assess workforce skills and competencies; identify and mitigate competency gaps.

(2) Provide mandatory competency reports on mission-critical occupations to DOD and Congress.

(3) Forecast manpower requirements by analyzing mission requirements, attrition, retirement trends, and workload forecasts.

Chapter 2
Department of the Army Physical Security Program

2–1. General

a. The Army Physical Security Program is an integrated approach to physical security designed to provide risk-based protection to Army installations, SAFs, USACE public works and other locations from threats to readiness to generate, project, and sustain Army forces carrying out operations Worldwide and in securing the Homeland. This regulation implements DOD physical security policies and minimum standards for physically protecting Army personnel, information, equipment, facilities, activities, and operations (see references). Nothing in this regulation abrogates the authority or responsibility of commanders to apply more stringent security standards, as necessitated by increased threat or required by other Army issuances during emergencies, increased threat level or high risk determinations, or as the commander or director deems necessary. Commanders and directors at every level are responsible for the physical security of the Army resources under their care.

b. Physical security programs and plans will include multiple security components that complement each other to produce a comprehensive approach to security matters, including physical security plans; physical security inspections and surveys; participation in antiterrorism committees and fusion cells; validated task critical assets; and a continuing assessment of the installation's or command's physical security posture. The program prescribes policies for the protection of critical resources: arms, ammunition, explosives, biological select agents and toxins, unclassified Army property, nuclear reactors and special nuclear materials, and chemical agents. The program prescribes policies for protecting Army sites in terms of controlling access to installations, SAFs, and restricted areas. The program also prescribes policies for Army civilian police and security guards. However, detailed security standards and policy for AA&E, nuclear, chemical, biological, and unclassified Army property is provided in other AR 190 series physical security regulations.

c. The intent of the program is to counter threats against the Army mission, resources, and capabilities in all aspects of operations by means of policies that set minimum physical protective measures and security procedures. The program counters threats by addressing the full spectrum of aggressors, and their tactics and tools, based on historical and current use.

d. Physical security plans, processes, and procedures will synchronize with other protection programs such as antiterrorism, information security, personnel security, and with related efforts such as continuity of operations, information assurance, emergency management, and resource management.

e. Physical security includes protective measures such as equipment and devices, personnel, and procedures. These measures include, but are not limited to—

(1) Armed qualified personnel.
(2) Military working dogs.
(3) Physical barriers and systems.
(4) Badging systems.
(5) Security containers.
(6) Locking devices and systems.
(7) IDS.
(8) Security lighting.
(9) Security barriers equipment and barrier systems, to include fencing.
(10) Assessment and surveillance systems.
(11) Installation access control devices and systems.
(12) Installation visitor control systems.
(13) Facility entry control devices and systems.
(14) Facility hardening and other real property protective enhancements.

(15) Standards compliance assessments.

2–2. Privacy and freedom of information

Requirements in AR 25-22 and AR 25–55 will be rigorously applied to all aspects of physical security planning and operations.

2–3. Security criteria deviation process

a. Deviation programs. These programs provide a management tool for commanders and directors to review, monitor, plan, and program for corrections to deviations from physical security standards, impacting Army resources, or resources over which they have controlling authority and responsibility. The deviation programs:

(1) Ensure prescribed security requirements are properly observed and implemented.

(2) Provide a management tool to monitor corrective actions.

(3) Ensure deviations from established physical security requirements are systematically and uniformly identified, concurred to by the chain of command, and adjudicated by OPMG.

(4) Ensure that waivers and limited or permanent exceptions are deviations from specific security requirements.

(5) Ensure that waivers and limited or permanent exceptions are not used to reduce or eliminate minimum security requirements.

(6) Evaluate each waiver or limited or permanent exceptions on a case-by-case basis.

b. Categories of deviations. To ensure alignment with DOD-approving authorities will categorize deviations from this regulation as waivers, limited exceptions, or permanent exceptions.

(1) Waivers.

(a) Installation commanders and directors, or facility directors must request a waiver when they cannot meet a prescribed minimum standard, the deficiency cannot be corrected within 90 days, but it can be corrected within 1 year.

(b) The approving authority must formally review waivers every 9 months and document progress made to correct the waivered deficiency. A brief statement affirming currency of all command waivers and exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM-MPO- PS) 2800 Army Pentagon, Washington, DC 20310-2800.

(c) If security standards or the situation affecting the security of the resources changes, another deviation request must be submitted.

(d) Submitted and approved waiver requests must be retained on file, to include periodic reviews of waivers.

(2) Limited exceptions.

(a) Installation commanders and directors, or facility directors, must request a limited exception when they cannot meet a prescribed minimum standard and the deficiency is exceptions-correctable within 3 years.

(b) Limited exceptions are granted when:

1. Corrective action of a security deficiency is beyond the capability of the organization.

2. The deficiency can be corrected within 3 years.

(c) The approving authority will formally review limited exceptions every 12 months and document progress made to correct the deviation.

(d) If security standards or the situation affecting the security of the Army resources changes, another deviation request must be submitted.

(e) Submitted and approved limited exceptions requests must be retained on file, to include annual reviews of limited exceptions.

(f) A brief statement affirming currency of all command limited exceptions will be certified current by (principal official) (date) and a copy sent to HQDA (DAPM-MPO-PS) 2800 Army Pentagon, Washington, DC 20310-2800.

(3) Permanent exceptions.

(a) Installation commanders and directors, or facility directors, must request a permanent exception when they cannot meet a prescribed minimum standard and this is not correctable in 3 or more years. Justification must clearly explain why the standard cannot be met and why correcting the deviation is adjudged not to be feasible or cost-effective, after a most careful and critical evaluation of the facts.

(b) Deviations approved as permanent exceptions require compensatory measures.

(c) Permanent exceptions, once formally approved, will be incorporated into security plans. If a security standard or situation affecting the security of resources changes, another deviation request must be submitted.

(d) Submitted and approved permanent-exceptions requests must be retained on file, to include a command review annually of permanent exceptions.

(4) Exception reviews. All exceptions will be reviewed during physical security inspections or when a major change in site configuration or mission offers the opportunity for corrective action to terminate the exception. The commander or director to whom the exception was granted will conduct the review. All reviews will be forwarded through command channels to the approving authority.

c. Compensatory measures.

(1) Compensatory measures will be in place for each deficiency.

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

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

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

(5) Compensatory measures that consist primarily of instructions to the security force to increase their alertness are not sufficient.

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

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

d. Approval procedures. Requests for a waiver, or a limited or permanent exception, are initiated by the commander or director and forwarded through appropriate command channels to HQDA (DAPM-MPO-PS) 2800 Army Pentagon, Washington, DC 20310-2800 or usarmy.pentagon.hqda-pmg.list.ps@mail.mil.

e. Request coordination. Requests for a waiver, or a limited or permanent exception, concerning facility design will be coordinated with OACSIM. All waiver or exception requests will include the following information—

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

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

(3) Reasons for noncompliance. Explain why the organization cannot comply with this regulation. For waiver or exceptions, show what actions have been taken, planned, or scheduled to correct the deficiencies. Waivers and exceptions should not be used to reduce or eliminate minimum security standards.

(4) Detailed information. Provide detailed information on current compensatory measures.

(5) List of all waivers or exceptions currently in effect. Explain why these deviations, collectively, do not create an overall site vulnerability greater than the stated compensatory measures can mitigate.

(6) Coordination. Show coordinated efforts with the affected staff agencies such as the PM, DES, PSO, PSO, supporting judge advocate of the installation, supporting engineer, or activity.

(7) Commander or director's evaluation of the requests.

f. Endorsements. Commanders or directors in the chain of command will review and endorse each waiver or exception request.

(1) Commanders and directors of ACOMs, ASCCs, and DRUs, the ARNG, and IMCOM region directors may delegate this authority to a colonel or civilian equivalent division chief, or deputy division chief responsible for physical security matters.

(2) Each chain of command endorsement will include comments assessing the adequacy of compensatory measures, taking into consideration the required criteria for waiver or exception.

g. Classification. Requests for waivers or exception may require appropriate security classification per AR 380–86, AR 380-5, or appropriate security classification guide.

h. Physical security requirements. The requirements intelligence activities and communication facilities are prescribed in other policies and are exempt from this policy, unless otherwise specified in those policies.

2–4. Crime prevention

a. Crime prevention is the commander's or director's responsibility. A successful program needs continuing command emphasis to prevent criminal activity from hindering mission accomplishment.

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

c. A crime prevention program reduces crime by—

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

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

(3) Discouraging potential offenders from committing criminal acts.

d. The U.S. Army Criminal Investigation Command provides support for crime prevention surveys.

2–5. Program assessment

The following factors, at a minimum, will be considered to determine the type and extent of the commitment of resources toward physical security—

a. A risk analysis that identifies critical resources, threats and hazards, vulnerabilities, and risk mitigation.

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

(1) Nature and arrangement of the activity.

(2) Number of personnel involved.

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

(4) Storage of classified information and equipment.

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

c. Whether the area is protected as a MEVA, in accordance with paragraph 2–11.

2–6. Planning factors

a. Integrate physical security requirements into plans for mobilization, war, and current and contingency operations.

b. Evaluate planning to permit adjustments in physical security as the threat changes. Physical security planning will be tied to force protection conditions per AR 525–13 and unified facilities criteria (UFC).

c. Develop contingency plans for each installation or activity, to include support installations and key facilities per appendix C.

d. Test physical security procedures during unit training and during operations that require security precautions to protect against criminals, hostile intelligence, paramilitary forces, terrorists, or saboteurs, protest groups and disaffected persons.

e. Installations and organizations that expand upon mobilization must identify buildings and facilities to be assigned to expanded activities such as hospital wards, U.S. Army Reserve (USAR) schools and logistics warehouses. Buildings and facilities should be evaluated for physical security requirements once the mobilization assignment has been made. Reasonable efforts should be made to correct identified physical security deficiencies within the means of the organization.

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

g. Include restricting movement within specific areas of the installation using barrier plans, as required.

h. Establish evacuation route plans.

i. Units and activities located in SAFs face unique challenges when planning physical security matters. Additional factors for SAF include—

(1) Consideration of a relatively small footprint when compared with standard installations, limited number of personnel and/or lack of a full-time staff, local ordinances, and complete reliance on local law enforcement response capabilities.

(2) Establish a plan to control access to any public road entering or exiting the outer property boundaries of the SAF. Coordinate entry and exit closures and restriction plans with local and State law enforcement agencies.

(3) For RC units and activities, commanders should test their physical security plans and procedures during weekend training assemblies or during opportune times when personnel are available.

(4) For RC units and activities developing contingency plans for critical structures, containers, buildings, and work areas, take into account additional variables. These include having more SAF occupants for training assembly weekends, or that different tenant unit commanders may be overall responsible for SAF protection depending on when their units attend training assemblies.

(5) Threat and vulnerability assessments must consider a much broader spectrum of factors that are unique to every local community and that differ from region to region.

2–7. Planning coordination

a. Coordination through close liaison while developing a security plan should happen between the commander or director and—

(1) Adjacent installations or units.

(2) Federal agencies.

(3) State and local agencies.
(4) Similar host country agencies.
(5) Tribal nations for USACE, as applicable.

b. As permissible, such interaction should allow for an exchange of intelligence, security measures being employed, contingency plans, and any other information to strengthen local security.

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

(1) Maximum quantities of equipment items to be stored or extent of capabilities, as determined by the commander or director.
(2) Physical safeguards to be employed.
(3) Who is responsible, and how often, for conducting physical inventories or reconciliations.
(4) Reporting losses for investigation.
(5) Lock and key control.
(6) Identifying the organization with overall responsibility.
(7) Procedures to authorize and identify individuals to receipt for, and physically take custody of, Army property.

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

2–8. Physical security plans

a. The ACOM, ASCC, DRU, ARNG, and U.S. Army Reserve command (USARC) level.

(1) The physical security plan at this command level will be used to standardize how the command implements or operationalizes Army physical security policies. The plan will contain sufficiently detailed organizational processes and procedures to ensure that practical, effective, and common sense measures are employed in a risk-based method across the command.

(2) The plan will be specific enough that subordinate organizations can clearly determine their roles, responsibilities, timelines, and other related requirements. The physical security plan is a stand-alone document or an annex to a protection plan or operational order.

(3) The plan will be reviewed annually and revise as required. A brief statement affirming currency will be placed on the front page in this format: Certified current by the commander/director (principal official) (date).

(4) Care will be taken to mark pertinent portions for classification per applicable policy.

(5) See appendix B for minimum plan requirements.

(6) Physical security plans will be added to the Integrated Protection Plan in accordance with AR 525-2, The Army Protection Program, as an appendix.

b. Installations, SAFs, unit, and activity levels.

(1) The physical security plan at these command levels will be specific to a location or organization. Local requirements may require inclusion of additional material.

(2) Individual annexes will be exercised annually, except for every 36-months at USACE MEVA designated civil works and like projects and every 60-months at USACE non-MEVA designated civil works and like projects. The exercise will be conducted in coordination with other protection plans to the greatest extent practical for synchronization and cost effectiveness.

(3) The physical security plan may be a stand-alone document or an annex to a protection plan or operational order.

(4) The plan will be reviewed annually and revise as required. A brief statement affirming currency will be placed on the front page in this format: Certified current by (principal official) (date).

(5) Plan annexes may be separated from the basic plan for operational efficiency. The publication containing the separated annexes will be cited in the physical security plan as a cross reference.

(6) Care will be taken to mark pertinent portions for classification per applicable policy.

(7) See appendix C for minimum plan requirements.

2–9. Contingency plans

a. It might be necessary to increase security for arms, ammunition, and explosives (AA&E) and other sensitive resources during periods of natural disasters, natural emergencies, or periods of increased threat from terrorist or criminal elements. Contingency plans should include provisions for increasing physical protective measures and security procedural

measures based on the local commander/director's assessment of the situation. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.

b. Contingency plans will be coordinated across the staff offices, and with external supporting agencies. AA&E and other designated sensitive items will have an alternate storage location in the event the primary location becomes untenable. This location will be identified in a memorandum of agreement. The feasibility of the alternate storage location will be validated during a physical security exercise, a continuity of operations exercise, or similar exercise.

c. An alternate storage site might not be practical for bulk storage sites having a large volume of stored AA&E or sensitive items. For these sites, a contingency plan for in-place operations will be issued and practiced.

2–10. Barracks plans

a. Commanders and directors will develop physical security plans for barracks to the extent possible.

b. Plans will address at a minimum the requirements in appendix D.

c. The plan will be reviewed annually and revised, as needed, to remain current. A brief statement affirming currency will be placed on the front page in this format: Certified current by (commander, director, or designated representative) (date).

d. The plan is an inspectable item. The plan will be included in command operations inspections, installation inspections, and similar inspections and assessments.

e. The plan does not have to be a separate document. It can be an annex to a barracks management plan, a protection plan or similar encompassing plan, but will address each planning element identified in appendix D.

2–11. Mission essential vulnerable areas

a. MEVAs are facilities or activities or resources on or off the installation or SAF that, by virtue of their function, are evaluated by the commander or director as vital to the successful accomplishment of the installation's, State National Guard, major USAR command, or USACE mission. The intent of the MEVA designation is to help the commander or director focus attention and resources. This includes areas nonessential to the installation's or facility's operational mission but which, by the nature of the activity, are considered vulnerable to theft, trespass, damage, terrorism, or other criminal activity.

b. Tenant commanders will provide their list(s) of MEVA(s) to the senior commander for inclusion in the host MEVA master list and verified annually. The MEVA list will be prioritized to aid the decision-making process for the allocation of resources and deployment of forces in the event of an increased security posture.

c. Risk analysis will be conducted in accordance with AR 190-51 and process aids are available in DA Pam 190-51 and SMS(CM). The following criteria will be included in the process—

(1) Criticality to the national defense, to the Army mission, and to the organization's mission.

(2) Local criminal, terrorist insider and acts of nature threat assessments.

(3) Nature and arrangement of the activity.

(4) Number of personnel involved.

(5) Strategic, tactical, or monetary value of resources.

(6) Classification level.

(7) Other factors such as natural or human-made hazards.

d. At a minimum, the following will be designated as a MEVA—

(1) Airfields and aircraft parking and maintenance areas for tactical aircraft.

(2) On-post public and privatized primary and alternate electric power supply transmission and generation facilities; utility distribution systems to include tank farms, supply points, and distribution hubs; and water sources and treatment facilities.

(3) All arms, ammunition, and explosive storage areas, nuclear reactors, special nuclear materials, chemical agents, and biological select agents and toxins.

(4) Critical communications facility that is essential to the continuity of operation of the National Command Authorities during the initial phases of national emergencies, and other nodal points of element designed as crucial to mission accomplishment.

(5) Motor pools and maintenance activities which are assessed at Risk Level III in accordance with AR 190-51.

(6) Medical treatment facilities with controlled drug vaults or storage areas and radioactive materials storage areas identified in AR 190-51.

(7) USACE civil works and like projects or resources that are assessed at a Risk Level III.

(8) Classified information storage and transmission sites in accordance with AR 380-5.

(9) Petroleum, oils, and lubricants (POL) at bulk storage facilities which are assessed at Risk Level III in accordance with AR 190-51.

e. Commanders or directors may add MEVAs they feel are critical or vulnerable to the above minimum requirements, however, may have to justify the MEVA to the senior commander.

2–12. Threat assessment

a. A local threat assessment will be developed for installations and SAFs. The assessment will include the aggressors and tactics listed in DA Pam 190–51. The assessment will identify local threats and make full use of the investigative resources available in the geographic area to anticipate criminal and intelligence activities that pose a threat to Army resources. The assessment will be coordinated with the following agencies, where applicable—

(1) Local Federal Bureau of Investigation (FBI) field office.

(2) Local law enforcement agencies.

(3) Intelligence and investigative agencies of the uniformed services.

(4) Local Bureau of Alcohol, Tobacco, Firearms, and Explosives field office.

(5) Host country agencies, where applicable.

b. Threat assessments will be disseminated to subordinate and tenant activities, and will be included as an annex in the physical security plan.

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

d. Local threat assessments will be reviewed, updated as necessary, and certified annually or when a significant change in threat occurs.

2–13. U.S. Army Security Management System (CounterMeasures)

a. PSOs and inspectors will use SMS(CM) to standardize procedures to conduct physical security inspections, surveys, and for planning and programming.

b. SMS(CM) is a—

(1) Web-enabled, enterprise software solution that optimizes the process of collecting information by automating routine tasks.

(2) Decision-support tool that presents a coherent view of the physical security posture for a defined area of responsibility.

(3) Optimizer of planning procedures by providing objective, risk-based prioritization of action.

(4) Standardized set of risk analysis measurements based on risk management techniques published by the National Institute of Standards and Technology.

c. SMS(CM) will be used to—

(1) Schedule, conduct, and record physical security inspections and surveys.

(2) Submit timely information to higher headquarters.

(3) Justify program requirements.

(4) Create risk mitigation action plans based on trend analysis, cost-benefit analysis, and loss-expectancy analysis as means to determine the best use of resources.

(5) To conduct a risk analysis and complete the DA Form 7278 (Risk Level Worksheet).

(6) To conduct analysis of inspections and survey results and provide a detailed report to commands on physical security needs.

(7) Access to SMS(CM) is located at http://smshelp.countermeasures.com/.

2–14. Physical security surveys

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

b. Formal, recorded surveys will be conducted by personnel qualified per paragraph 3–2.

c. Surveys are not required for SAFs if a physical security inspection provides the commander or director with sufficient information to determine the physical security posture of the facility, not just the tenant units. For example, an Armed Forces Reserve Center managed by the USAR might not require a survey if the center is assessed by conducting one

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

d. Surveys will be recorded and results analyzed in SMS(CM). DA Form 2806 (Physical Security Survey Report) may be used if SMS(CM) is not immediately available. The report will be transferred to SMS(CM) on the next available business day, or when the system is available. Survey reports will show findings of policy deficiencies and observations concerning potential means to improve site security. Procedures and measures to evaluate will include—

(1) Threat assessment procedures.

(2) Security forces types, availability, training, equipment, and guard orders.

(3) Implementation of access control procedures per chapter 8.

(4) Control of visitors and packages.

(5) Use of PSE.

(6) Security lighting.

(7) Control, issuance, and accountability of keys used at the installation perimeter such as for limited access gates and for industrial spaces.

(8) Identification of critical areas or facilities.

(9) Process used to track physical security work orders and vulnerability mitigation efforts.

(10) Outstanding waivers and exceptions to policy.

e. Surveys will be conducted every 36 months except—

(1) When an installation is activated.

(2) When no record exists of a previous physical security survey.

(3) When the commander/director determines a greater frequency is required.

f. Physical security surveys will include—

(1) An executive summary for the senior commander, director, or manager.

(2) A detailed assessment of the security posture of the installation.

(3) Recommended prioritized application of resources for reducing vulnerabilities.

(4) Exhibits, such as photographs, sketches, graphs, and charts to clarify findings and recommendations, and an assessment of criticality and vulnerability.

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

(1) The commander or director of the garrison or the stand-alone facility.

(2) The ACOM, DRU, or ARNG command chain.

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

i. All survey reports will be signed and completed by the PSI within 30 days of the scheduled survey date.

j. Surveys will be kept on file for 5 years.

2–15. Physical security inspections

a. A physical security inspection is a formal recorded assessment of the physical protective measures and security procedural measures implemented to protect resources. SMS(CM) will be used with required naming convention within SMS(CM) to gather and record inspection information. DA Form 2806–1 (Physical Security Inspection Report) may be used if SMS(CM) is not immediately available. The report will be transferred to SMS(CM) on the next available business day, or when the system is available. Formal inspections will be conducted by personnel qualified per paragraph 3–2.

b. All Army resources identified in this paragraph will be inspected. The responsible ACOM, ASCC, DRU, or the ARNG will determine how to consistently account for derivative or subordinate command organizations such as detached platoons or other SAFs.

(1) It is prohibited to conduct illegal or dangerous acts intended to demonstrate security weaknesses.

(2) Inspections will be coordinated with the command to ensure all personnel who are required to be available are notified. Inspections may be unannounced; however, the inspector should be flexible to understand all personnel required for the inspection may not be readily available. The inspector will review unit schedules to minimize adverse impact with training, mobilization, demobilization, or similar requirements.

(3) Resources identified in paragraph 2–11 will be inspected for compliance with minimum physical protective and security procedural measures. Physical security plans and the management of locks and keys will also be inspected.

(4) Inspections of classified facilities identified in paragraph 2-11 will be inspected in accordance with AR 380-28.

(5) One report will be produced for each inspected organization, regardless of the number of inspectable resources in the organization.

c. Physical security inspections will be conducted—

(1) On an 18-month basis for conventional AA&E, regardless of bulk or non-bulk storage.

(2) On an 18-month basis for the nuclear reactor and special nuclear materials.

(3) On an 18-month basis for chemical agents and biological select agents and toxins, alternating between inspections by facility-level and higher headquarters-level personnel.

(4) On a 24-month basis for other resources when designated as a MEVA, when—

(a) A unit or activity is activated.

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

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

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

(e) The commander or director determines a greater frequency is required.

(5) On a 36-month basis for—

(a) USACE MEVA designated SAF resource, facility, or activity.

(b) USACE MEVA designated civil works and like project resources, facility, or activity.

(6) On a 60-month basis for—

(a) USACE non-MEVA designated SAF resource, facility, or activity.

(b) USACE non-MEVA designated civil works and like project resources, facility, or activity.

(7) On a more frequent basis than defined above when the responsible commander or director determines a greater frequency is required.

d. Reserve Officer Training Corps regional physical security personnel will conduct a physical security inspection during the overarching annual formal inspection. For the purpose of this specific situation—

(1) The inspector is not required to be formally trained at the U.S. Army Military Police School's Conventional Physical Security/Crime Prevention Course.

(2) The inspector is not required to possess the combined DA Form 4261.

(3) The inspection is not required to be recorded on the DA Form 2806–1.

(4) The inspection will, however, adhere as close as possible to the standards of a formal inspection.

e. The PS inspector will be granted access to facilities, resources, records, and other information on a need-to-know basis, consistent with the inspector's security clearance for access to classified information and provisions of applicable regulations.

f. A copy of the physical security inspection report, with exhibits if beneficial, will be provided to the—

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

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

(3) Supporting installation PS Office.

(4) USACE commander or director, for their review and their "approval." The commander or director will sign the inspection report within 30 days of the scheduled inspection, which reflects concurrence with the report content that will be provided to the next higher headquarters.

(5) All inspection reports will be signed and completed by the PSI within 30 days of the scheduled inspection date.

g. All deficiencies will be corrected or mitigated regardless of an inspection rating of adequate or not adequate. Deficiencies beyond the capability of the inspected command to correct will be reported to the next higher command to program resource requirements.

h. The submission of a work order work package, or operation and maintenance work request does not resolve a deficiency. Compensatory measures will be employed within available resources until funding is received and construction is complete, thus mitigating the deficiency.

i. Recurring deficiencies will be tracked during future physical security inspections until corrected. Recurring deficiencies in future reports will be identified with the date it was first identified, and will be designated as "Recurring since DD MM YYYY".

j. A complete follow-up inspection consisting of all applicable countermeasure in SMS(CM) will be conducted no later than 6 months later, if the initial inspection resulted in a not-adequate rating and subsequent failures, until an adequate inspection is recorded.

k. Inspections will be kept on file for 5 years.

2–16. Report of action taken or planned for physical security surveys and inspections

a. A commander's or director's report of corrective action taken or planned will be submitted and filed with report in response to—

(1) Physical security survey findings.

(2) Physical security inspection findings when the inspection result is rated as not adequate as determined by the PS inspector.

(3) In addition, the ACOM, ASCC, DRU, and ARNG will determine if—

(a) Inspection findings will be addressed, even if the inspection result is rated as adequate. (This is to ensure findings are addressed.)

(b) For physical security surveys, the report will address all findings and recommendations regardless of the overall survey rating.

(c) For physical security inspections, the report will be limited to responding to an inspection rating if not adequate. Responding to findings that still result in an inspection rating of adequate is optional.

(4) For surveys, the report will be provided to—

(a) ASCC, as appropriate.

(b) The senior commander, director, or manager.

(c) The garrison chain of command.

(5) For inspections, the report will be provided by the inspected command to—

(a) The supporting garrison or USACE commander or director.

(b) The unit's chain of command.

(c) The next higher USACE headquarters.

b. For surveys, the report will be provided by the inspected garrison commander to—

(1) The installation commander.

(2) The senior commander.

(3) The ASCC.

(4) The garrison chain of command.

c. A copy will be maintained by the surveyed or inspected activity USACE civil works or like projects, or garrison and by the supporting physical security office until at least the next physical security survey or inspection is conducted and the inspection report is signed and "approved" by the responsible commander or director. The report of action taken will address each individual deficiency, and may also include observations and comments.

d. A copy will be provided to the ACOM, ASCC, DRU, or ARNG, as applicable.

e. A formal process will be used to track discrepancy corrections.

f. For surveys after corrective actions are taken, the physical security posture will be reassessed based on—

(1) Mission.

(2) Actual or postulated threats.

(3) Findings of the survey team and correcting actions.

(4) Comparison of findings from previously conducted surveys.

(5) Areas considered over- or under-protected.

g. Report of action will be submitted no later than 30 days after the completed inspection or survey report.

2–17. Report classification

Classify and safeguard completed surveys and inspections per AR 380–5; mark as, at a minimum, For Official Use Only CUI (controlled unclassified information).

2–18. Security engineering surveys

A security engineering survey is an on-site assessment of physical security engineering requirements. Security engineering surveys will be performed when planning new construction or renovations to facilities where there are likely to be physical security requirements. Security engineering surveys may also be requested by the project manager (PM) or equivalent security officer to evaluate existing security.

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

(1) Identify resources requiring protection.

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

(3) Identify protective measures to reduce vulnerabilities.

(4) Determine the cost of proposed protective measures.

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

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

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

c. Personnel to support security engineering surveys are available on a cost reimbursable basis from the USACE Protective Design Center, the USACE Electronic Security Center, or the ARNG program manager (non-reimbursable if for ARNG use) at these addresses—

Commander, U.S. Army Engineer District
Attn: CENWO–ED–S
1616 Capital Avenue, Ste. 9000
Omaha, NE 68102–4901
E-Mail: pdc.web@usace.army.mil
Commander/director, Huntsville Engineering and Support Center
or
Commander, U.S. Army Engineer District
Attn: CEHNC–ED–ME–T
4820 University Square
Huntsville, AL 35816–1822
(email: askessmcx@usace.army.mil)
or
Director, Army National Guard
Attn: ARNG–ARI–FM–ESS
111 S. George Mason Drive
Arlington, VA 22204–2905.

2–19. Inspection and maintenance of containers, vaults, and locks approved by the General Services Administration

a. Personnel who service security containers, security vaults and locks that are approved by GSA will be certified per Federal Standard 809B.

b. Federal Standard 809B requires that any servicing of GSA-approved containers or vault doors, to include neutralization, repair, combination lock servicing, or replacement, will be done only by persons who have successfully completed the GSA Certified Safe and Vault Technician course. The changing of combinations or selection of operator modes for combination locks is exempt from this requirement. Course information is available at http://www.navfac.navy.mil/go/locks or by contacting the DOD Lock Program at Defense Switched Network 551-1212, or 1-805–982–1212.

c. Inspection of the containers, vaults, and locks approved by GSA can be conducted by any security personnel without having attended training.

2–20. Supporting and supported Department of Defense components for physical security

Army commanders or directors, regardless of their unit's location are held to Army standards for protecting assigned resources. Leaders in other Military Departments and defense agencies are recognized to be held to similar standards. To assist commanders and directors in determining the condition of their physical security posture—

a. Supporting DOD components are expected to support Army commanders and directors by, at a minimum, conducting physical security inspections of Army units per Army standards, and recording the results in SMS(CM), or as per paragraph 2–13.

b. Supporting Army garrisons will, at a minimum, conduct physical security inspections of supported Military Departments and defense agencies, and provide the command's results to the supported unit.

2–21. Personnel Reliability Program

a. Determining reliability. The following positions or duties in Army physical policies require a determination of reliability—

(1) Unaccompanied access to arms, ammunition, and explosives per AR 190-11.

(2) Unaccompanied access to controlled medical substances per AR 190-51.

(3) Employment and retention as a DA police officer or DA security guard, per AR 190-56.

b. Commander or director's program. Determining personnel reliability is a commander or director's program. Commanders and directors must be aware of, and concerned with, the reliability at all times of personnel having unaccompanied access to identified areas. A total team effort and interaction is necessary for this program to be successful.

c. Delegation of authority. The responsibility for this program may be delegated to the level of supervision best suited to evaluate program members on a continuing basis. When authority is delegated, the commander or director retains the responsibility to review decisions to qualify or disqualify personnel. The commander or director will issue a written delegation of authority, by memorandum, for a certifying official who will have responsibility for the determination process.

d. Inherently governmental. A decision concerning the reliability of personnel for this duty is inherently a governmental function. Contractors cannot certify their own personnel into these programs. Contractors can be assigned as monitors to help the certifying official continue to evaluate personnel, but ultimately the decision to qualify or disqualify rests with the commander or director, by means of the delegated certifying official.

e. Supporting form. The DA Form 7708 (Personnel Reliability Screening and Evaluation Form), with instructions on use in appendix E, is used to document the reliability determination process as follows—

(1) Personnel data. This includes the Social Security number.

(2) Personnel records check. A qualified personnel official will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information.

(3) Security records check. A security clearance is not required for unaccompanied access to arms, ammunition, explosives, and controlled medical substances. The commander or director may, however, use this check as an additional determination factor. If a security records check is conducted, the reviewing security official will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information, in the official's judgment.

(4) Medical records check. The reviewing competent medical authority (a licensed physician, physician's assistant, or nurse practitioner) will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information in the official's judgment. A DD Form 2870 (Authorization for Disclosure of Medical or Dental information) is required if the records are retained by a non-DOD medical entity. A person is immediately disqualified from the position, or duty, under consideration if the person does not provide such authorization.

(5) Law enforcement records check. This check will be conducted by the supporting Army law enforcement office by a query of the Army Law Enforcement Reporting and Tracking System. A senior law enforcement official will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information, in the official's judgment.

(6) Drug test. A drug test may or may not be required for the PSO and PSI positions and duties. The commander or director may, however, use this check as an additional determination factor. If a drug test is used, a qualified test official will electronically annotate on the DA Form 7708 if the test results in potentially disqualifying information. The DA Form 7708 provides for drug testing results if other policy proponents use the form and need such information.

(7) The supervisor briefing to a prospective person.

(8) Continuing periodic evaluations of an incumbent person.

(9) Suspension or temporary disqualification of an incumbent person.

(10) Disqualification of an incumbent person.

f. Responsibility to inform. Supervisors at all levels have an inherent responsibility to inform the commander or director about all cases of erratic performance or poor judgment by personnel, on or off duty, that could affect duty reliability. All personnel are responsible for reporting to their immediate supervisor any behavior that might affect a co-worker's reliability.

g. Continuous evaluation. It is essential to continually evaluate personnel in this program. Any incident or problem that might be cause for temporary or permanent removal from the program must be promptly reported to the certifying official and supervisors. Those providing medical care and maintaining medical records are required to report any incident or allegation about a person's suitability under this program. Verbal or telephonic notifications will be confirmed in writing.

h. Documenting behavior patterns. To ensure commanders and directors are aware of patterns of behavior that may indicate unreliability, commands and activities should establish a documentation system. It would document discipline of employees, in both supervisor and employee records. These records will be periodically reviewed by certifying officials.

i. Potential duty impairment. Personnel have a continuous responsibility to report all medical treatment and medication that may impair their ability to perform the essential functions of the job to the competent medical authority as it occurs, regardless of whether the treatment was provided through the federal health system or by a private health care provider. The examining physician will make a recommendation to the certifying official concerning the potential impact of the condition, treatment, or medication on reliability. If the examining physician is not in Federal service, then the evaluation findings and the examining physician's recommendation must be forwarded to a physician having Federal status for review and approval.

j. Personnel interview. The certifying official will interview the person to appraise character, judgment, reliability, attitude, emotional and mental maturity, and sense of responsibility. Personnel exhibiting financial irresponsibility will not be selected. The interview will be documented on DA Form 7708, which will be completed per appendix E of this regulation.

k. Annual review. The reliability determination will be reviewed every year in the on-boarding month or upon change of status (for example, departs the unit, criminal activity whether alleged or adjudicated).

2–22. High risk personnel

a. Senior Army civilian and military leaders serve as an extended symbol of our nation’s Army, making them attractive and accessible targets. Some personnel, by virtue of rank, assignment, symbolic value, vulnerabilities, location, or a specific threat requiring additional security to reduce or eliminate risk, are at a greater risk than the general population. These individuals will be formally designated as high risk personnel (HRP), in accordance with guidelines specified in DODI O-2000.22 and the provisions of AR 190–58.

b. Recommendations for physical security requirements identified by a personal security vulnerability assessment, in accordance with DODI O-2000.22 and AR 190–58, will be a priority for validation in management decision package (MDEP) physical security matters (QPSM).

Chapter 3
Physical Security Personnel, Credentials, and Professional Certifications

3–1. Physical security officer

a. A physical security officer (PSO) will be appointed in writing at the battalion and higher, garrison, installation, ACOM, ASCC, DRU, and ARNG command levels. The PSO will be a sergeant (E–5) or above to represent the commander or director when providing physical security briefings and information.

b. At brigade and below organizations, the PSO will have a working knowledge of physical security and operational planning and complete the following:

(1) Within 90 days of assignment on orders, the PSO will complete the following eLearning courses located at http://www.cdse.edu/catalog/physical-security.html. This requirement will be waived if the PSO attended the Army physical security course per paragraph 3–2*c*(3).

(a) Introduction to Physical Security (PY011.16).

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

(c) Physical Security Measures (PY103.16).

(d) Physical Security Planning and Implementation (PY106.16).

c. At the ACOM, ASCC, DRU, ARNG, garrison, installation, and division command level, the PSO will meet the following requirements—

(1) Should complete the Army physical security course, per paragraph 3–2*c*(3).

(2) Can be a Soldier, Department of the Army civilian, or ARNG state technician.

(3) As a civilian, meet the qualifications security administration series 0080 (Physical Security) as published by the Office of Personnel Management (OPM).

(4) In addition for the ARNG, State, or territory personnel directives for physical security specialists also apply.

(5) Civilians not in security administration series 0080 (Physical Security) however, perform the functions of a PSO will submit a deviation in accordance with paragraph 2–3 above requesting to perform the duties.

d. A PSO does not require PS credentials unless they hold the position of a physical security inspector (PSI) as well.

3–2. Physical security inspector

a. See appendix E for the required personnel reliability screening and evaluation process.

b. The local commander or director's representative, or the PM, DES, PSO will select personnel for the position of physical security inspectors.

c. Military inspectors will be—

(1) Qualified in primary military occupational specialty 31B, or 31E if assigned to the U.S. Disciplinary Barracks.

(2) A sergeant (E–5) or above.

(3) Formally trained at the U.S. Army Military Police School Conventional Physical Security/Crime Prevention Course (7H–31D/830–ASI H3).

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

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

d. U.S. Government civilian employees will—

(1) Meet the current OPM 0080 (Physical Security) qualification standards.

(2) Be formally trained at the 7H–31D/830–ASI H3 course.

(3) Be cleared for access to at least secret-level information.

e. PSI credentials will not be issued to contracted persons.

f. Weapons will not be issued to civilian physical security personnel, unless in a theater of operation and per the combatant command or senior commander.

3–3. Management of additional skill identifier H3, physical security inspector credentials, and physical security specialists

a. The ASI H3 skill identifier is awarded per applicable regulations to military police Soldiers after successful completion of the 7H–31D/830–ASI H3 course.

b. Issuance of the physical security inspector identification (ID) card will be on the recommendation of the PM, DES, PSO, or the commander or director of the U.S. Disciplinary Barracks. Issuance of the physical security inspector ID card for commands other than garrisons will be by the PM, DES, PSO, or equivalent senior law enforcement official.

c. The PM, DES, PSO will initiate action to withdraw ASI H3, collect credentials, and remove a person from the physical security program on determination that the person is no longer qualified to perform physical security specialist duties. Disqualification or relief from duty may be based on any of the following—

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

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

(3) Final revocation of a personnel security clearance.

(4) Loss of credentials through neglect.

(5) Any other conduct that may adversely affect a person's continued performance of duties.

d. Physical security inspectors will be suspended from duty when the person either—

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

(2) Has had their security clearance suspended.

(3) The ASI will be removed from active inventory and placed in an historical file when a person has—

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

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

e. Names of Soldiers in the categories listed in paragraph 3–2 will be forwarded to the U.S. Army Human Resources Command (AHRC–EPL–M) for removal of the ASI and annotation in official records. A copy of the action will be furnished to the local military personnel office for inclusion in the Soldier's personnel file. The local commander or director may restore ASI H3 to a qualified person, in accordance with this paragraph.

3–4. Additional training

a. Physical security personnel are encouraged to attend the following additional training—

(1) USACE—

(a) Security Engineering Training Course.

(b) Electronic Security System (ESS) Design Course.

(c) ICIDS Operator/System Administrator Course.

(d) Installation Access Control Point (IACP) Course.

(e) Defense Security Services (DSS) Center for Development of Security Excellence (CDSE) eLearning courses, shorts, and webinars at http://www.cdse.edu/catalog/physical-security.html.

(f) IDS Operator/System Administrator Course for commercial off-the-shelf (COTS) systems employed in SAFs.

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

c. Additional courses available for ARNG personnel include—

(1) The ESS/IDS Certification Course. Successful completion is a prerequisite for the following courses.

(2) The ESS Manager Course.

(3) Access Control Systems (ACS)/Closed Circuit Television (CCTV) 101 Course.

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

a. Overview.

(1) Prior to issuance of the DA Form 4261 and 4261–1, the Command Provost Marshal, Director of Emergency Services, or delegated representative will determine reliability using the process at paragraph 2–21, above, and the supporting DA Form 7708. Instructions for completing the DA Form 7708 are at appendix E. Completion of Part VI of the DA Form 7708 is not required.

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

(3) The combined DA Form 4261–1 is the only authorized credential. Reproducing the credential or use of locally fabricated credentials is prohibited.

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

(5) Social Security numbers on issued DA Form 4261–1 will be immediately redacted. Existing card stock containing a field for the Social Security number will be used until depleted, but the Social Security number field will not be used.

(6) Credentials will be signed by the inspector, authenticated by the PM, DES, PSO, or the commander, or director of U.S. Disciplinary Barracks, and laminated by the issuing authority. For organizations that do not have these command positions, the commander or director will sign the credentials.

(7) Non-laminated credentials are not valid.

(8) Credentials will not be altered in any way except for redacting Social Security numbers. Issuing authorities will establish procedures for annually checking credentials, and will collect and destroy those that have been altered, defaced, or marred.

b. Issuance.

(1) HQDA (DAPM–MPO–PS) will issue credentials by serial numbered lots to the ACOM, ASCC, DRU, and the ARNG, as needed. Requests for credentials will be sent to HQDA (DAPM–MPO–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

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

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

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

(5) Issue credentials for a period not to exceed 48 months from the date of issue.

(6) Commands issuing credentials will provide an inventory report by memorandum for record to HQDA (DAPM–MPO–PS) Division annually.

c. Withdrawal.

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

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

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

d. Reporting information. Issuing authorities will report the full name, rank, and credential number of each person to whom PSI credentials are issued and from whom credentials are withdrawn. This information will be reported in writing

to the PM or PSO, and the cognizant ACOM, ASCC, DRU, or ARNG within 10 days of issue or withdrawal. Withdrawals reported will include a short explanation of the reason for withdrawal.

e. Credentials custodian. A military or civilian credentials custodian will be appointed in writing. The custodian will maintain a control log to account for the issuance, withdrawal, and destruction of credentials.

3–6. Uniforms

a. Military PSIs will wear the duty uniform.

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

c. There is no required duty uniform for civilian personnel.

3–7. Vehicles

Military and civilian inspectors are authorized to use unmarked vehicles of commercial design and colors in the performance of their official duties. The table off distribution and allowances authorizations should provide one vehicle for each two authorized inspectors. Consideration should also be made for at least one vehicle with an off-road capability to help inspect fencing and other rough-terrain physical security protective equipment.

3–8. Professional certifications

a. DOD's Security Professional Education Development (SPēD) Certification Program implements Executive Order 13434, DODD 5200.43, DODI 3305.13, and DODM 3305.13-M. This section applies to all Army civilian employees, active duty Army Soldiers in security positions, members of the Army Reserve, and members of the Army National Guard.

b. It is DOD policy to educate, train, and verify knowledge of individuals working in security positions. This general policy statement applies to all security practitioners and those who allocate 50 percent or more time performing security or security-like duties for the Army as their primary duty, as defined by OPM's Security Administration classification standards.

c. The SPēD Certification Program is part of an all-inclusive effort to professionalize the workforce. The program ensures security practitioners can demonstrate proficiency in a common set of competencies. The purpose of the program is to promote interoperability among the various security disciplines; facilitate professional development and training; and develop a workforce of certified security professionals.

d. The SPēD Certification Program is comprised of three core certifications and multiple specialty certifications, which meet distinct certification needs for security disciplines and responsibilities.

(1) The SPēD Certification Program serves as a valid and reliable indicator of employee mastery of facts, concepts, and principles the DOD community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to protect DOD resources.

(2) The DOD SPēD Certification Program will promote an interoperable and interchangeable DOD security professional workforce by establishing a uniform process of assessing knowledge and skills. It will establish formal and documented processes for assessing and evaluating whether personnel within the security workforce have acquired the knowledge and skills required to perform assigned security tasks. The program also will develop a workforce of certified security professionals capable of providing sound policy-based guidance and support to commanders, directors, managers, supervisors and leaders.

e. The DOD SPēD Certification Program is a third party, nationally accredited workforce certification developed by, and for, the DOD security community. The primary governance functions are: the accreditation body, conferral authority, executive agent, certification governance board, and the DOD and component program office.

(1) Accreditation body: National Commission for the Certifying Agencies.

(2) DOD conferral authority: Office of the Under Secretary of Defense (Intelligence).

(3) DOD executive agent: DSS.

(4) DOD certification governance board: Department of Defense Security Training Council.

(5) DOD program management office DSS CDSE.

(6) Component program management office: Army HQDA G-2, CP 35 and CP 19.

f. The DOD SPēD Certification Program is made up of multiple professional certifications:

(1) Security Fundamentals Professional Certification (SFPC): Provides a recognized and reliable indication of a security practitioner's understanding of foundational concepts, principles, and practices needed to successfully perform functions, implement programs, and pursue missions to protect DOD resources.

(a) Service components and DOD agencies require their military and civilian employees be conferred with SFPC before pursuing any other DOD SPēD certification assessments listed below. The Army was granted an exception to this requirement.

(b) There are certain positions in the Army that will only require the Physical Security specialty certification; however, they must obtain the SFPC prior to obtaining additional certifications beyond the Physical Security Certification.

(2) Security Asset Protection Professional Certification: Provides a recognized and reliable indication of a security practitioner's ability to apply foundational concepts, principles, and practices needed to successfully perform functions, implement programs, and pursue missions to protect DoD resources.

(3) Security Program Integration Professional Certification (SPIPC): Provides a recognized and reliable indication of a security practitioner's understanding and ability to apply risk management and security program management concepts, principles, and practices.

(4) Physical Security Certification (PSC): Provides a recognized and reliable indication of a security practitioner's understanding and ability to apply DOD physical security concepts, principles, and practices.

(5) Industrial Security Oversight Certification (ISOC): Provides a recognized and reliable indication of a security practitioner's understanding and ability to apply DOD industrial security oversight concepts, principles, and practices under the National Industrial Security Program.

(6) Special Program Security Certification (SPSC): Provides a recognized and reliable indication of a security practitioner's understanding and ability to apply DOD special access program policies, principles, procedures, and requirements.

(7) Adjudicator Professional Certification: Provides the recognition and official record of an individual's demonstrated understanding and application of the occupational and technical knowledge, skills, and expertise necessary to proficiently perform essential adjudicator tasks with the exception of due process functions. This is specific to DOD consolidated adjudication facility personnel.

(8) Due Process Adjudicator Professional Credential: Provides the recognition and official record of an individual's demonstrated understanding and application of occupational and technical knowledge, skills, and expertise necessary to proficiently perform essential due process adjudicator tasks. This is specific to DOD consolidated adjudication facility personnel.

g. SPēD certification roles and responsibilities.

(1) Functional chief representative (FCR). Responsible for overall implementation and advocacy of the DOD SPēD Certification Program.

(2) HQDA, CP 19, CPM.

(a) Provide overarching human resource, human capital management expertise and support for Army security policy development and maintenance to help implement the DOD SPēD Certification Program.

(b) Incorporate SPēD Certification Program designations and condition of employment language into all applicable position descriptions, to support DOD SPēD Certification Program core position description/standardized core position description indexing.

(c) Oversee and support enforcement of DOD and Army SPēD Certification Program governance policy across the Army enterprise.

(d) Continually disseminate information about the DOD SPēD Certification Program to the security workforce.

(e) Act as the interface between the DOD SPēD executive agent (DSS), the FCR, and security workforce on topics related to security workforce certification.

(f) Provide certification guidance and support to senior security leaders assigned to ACOMs, ASCCs, DRUs, and FOAs as required.

(g) Educate, support, and assist commanders, supervisors, and employees in complying with the DOD SPēD Certification Programs.

(h) In conjunction with Army SPēD Program manager, develop the Army's Annual Report on Accreditation and Certification and submit to the Director, DSS, for reporting to the Under Secretary of Defense (Intelligence) and the Under Secretary of Defense for Personnel and Readiness, Strategic Human Capital Planning Program Office.

(i) Participate as a voting member on the Army SPēD Waiver Committee to review Army certification waiver requests, in accordance with the SPēD Certification Program Waivers Guidelines managed by CDSE.

(3) Commander, director, or equivalent responsibilities.

(a) Ensure subordinate supervisors of indexed employees recognize that compliance is a condition of employment, per DOD 3305.13–M and this regulation.

(b) Ensure subordinate supervisors of indexed employees monitor certification progress.

(c) Ensure subordinate supervisors of indexed employees provide duty time to their personnel to take certification assessments and complete the required professional development units (PDUs) necessary for DOD SPēD certification bi-annual maintenance.

(4) Supervisor responsibilities.

(a) Ensure indexed civilian employees recognize that compliance is a condition of employment, per DOD 3305.13–M and this regulation.

(b) Ensure indexed employees attain and maintain the requisite certification(s) as annotated on the employee's position description.

(c) Ensure indexed employees are provided adequate time to prepare for, and take, DOD SPēD Certification Program assessments required for their position.

(d) Ensure indexed employees are provided time needed to complete the required PDUs necessary for DOD SPēD Certification Program bi-annual maintenance.

(e) Ensure appropriate action is taken if the individual fails to attain or maintain the certification(s) required for their position as outlined in DOD 3305.13–M. Contact your local Human Resource office for failure to meet a condition of employment.

(5) Employee responsibilities.

(a) Attain the required indexed certification(s) within 24-months of entry on duty or assignment start date.

(b) Timely completion and submittal of required PDUs and substantiating records to the DOD SPēD Certification Program Management Office as instructed by the DOD SPēD Certification Program Candidate Handbook.

(c) For guidance concerning the DOD-approved PDU categories and the DOD SPēD certification maintenance guidelines, reference the current version of the SPēD Certification Maintenance and Renewal Procedures at http://www.cdse.edu.

(d) Security Training, Education, and Professionalization Portal (STEPP) is the system of record for the DoD SPēD Certification Program.

(e) Establish and maintain a STEPP account with Defense Security Service.

(f) Maintain up-to-date contact information within the DSS STEPP profile.

h. General program guidance.

(1) DOD 3305.13–M requires components to identify security practitioners and designate or "index" individuals to a SPēD certification. Position descriptions, not the duties of the individual, will be indexed. Position descriptions and vacancy announcements will contain the following verbiage: "The incumbent is required to attain and maintain the (enter SPēD Certification here) within two (2) years of entry duty. Failure to obtain this certification within the required time may subject the incumbent to adverse action."

(2) Security professionals occupying a SPēD-indexed position prior to indexing date are not required to achieve certification unless they move to another position with a certification requirement. All new employees will be required to achieve certification(s) within two (2) years as a condition of employment once the program is implemented within Army. The program is implemented effective 20 March 2019 for occupation 0080 in both CP35 (Intelligence) and CP19.

(3) Implementation in the Army is identified as a position description coded with a SPēD Certification as a condition of employment.

(4) In instances where the employee is assigned to a position requiring more than two SPēD Certifications, the employee will have an extra year per certification to meet program requirements. For example: employees must obtain two of the indexed SPēD Certifications within the standard 2-year compliance window and the additional certification may be obtained during the 3rd year of employment without adverse action or waiver request.

(5) Army 0080 ACTEDS interns at a minimum, will need to attain the PSC for CP19 interns and the SFPC for CP35 interns by completion of their internship. Additional certifications can be included in their intern development plan, but should be tailored to the certifications aligned with the position the intern will transition to upon completion of their internship.

i. Certification indexing.

(1) Indexing definition. The process of aligning one or more DOD SPēD certification to a specific job position is based upon the duties and responsibilities outlined in the position description.

(2) Positions indexed. All Army civilian employees performing security work (as defined by OPM 0080 occupational series classification standards) as a primary duty (50 percent or greater) will have the appropriate certification(s) aligned to their position.

(3) Army DOD SPēD Certification indexing. The positions requiring certification will be identified, indexed, and the position descriptions updated to reflect the appropriate certification level. The positions will be indexed, based on the duties and responsibilities of the position. In order to decrease the effort required on part of the functional community

managers and unit commanders, the CPM will make initial recommendations on the 0080 positions. Those initial recommendations will be staffed to the functional community managers and unit commanders to validate. After the final determination has been made, the Civilian Human Resources Agency will input the certification requirement into the appropriate human resources systems, and certification will then become a condition of employment.

j. DOD SPēD Certification Program renewal standards.

(1) Only one certification maintenance expiration date will exist for each certification holder.

(2) All existing certification holders with more than one certification will have one static certification expiration date based on the most recent expiration date. Renewal cycle will be calculated as "most recently acquired certification expiration date + 2 years."

(3) A certification holder must submit a certification renewal form prior to their expiration date to fulfill certification maintenance requirements.

(4) A certification holder is responsible for entering 100 PDUs of professional development activities that meet the current maintenance guidelines and categories.

(5) A certification holder must accrue 100 PDUs within 2 years from their static conferral date to successfully meet the professional development requirement.

(6) At least 50 of the 100 PDUs must be acquired through approved professional development activities focusing on topic areas related to security. The remaining PDUs can be non-aligned with security; however, they must satisfy one or more of the professional development categories:

(7) If the certification holder has more than one certification and 100 PDUs cannot be achieved by professional development activities, the certification holder must achieve a passing score on the most recently conferred certification. Applies to SFPC, SAPPC, SPIPC, and PSC.

(8) ISOC and SPSC expirations are tied to SFPC and do not have to be independently maintained.

(9) A certification holder will be eligible to retest 180 days prior to the expiration date. The certification renewal eligibility to retest form will not be visible to the certification holder before this period is reached. A certification holder will only be able to retest their most-recently conferred certification for maintenance.

(10) A certification holder who does not accrue 100 PDUs or successfully retest by their biennial renewal date will have their certification status changed to "expired." One "expired" certification will put all other certifications into "expired" status.

(11) Refer to the most current version of the SPēD Certification Maintenance and Renewal Procedures for additional guidance concerning SPēD certification maintenance requirements.

k. SPēD Certification Program waivers and appeals.

(1) Certification candidates must coordinate with Army SPēD Program manager to request reasonable extensions for documented reasons. These reasons include deployments, hospitalization, or medical leave, and other extraordinary reasons that would prohibit an individual from meeting the following requirements:

(a) Certification attainment.

(b) Certification maintenance.

(2) There are no other waivers. Any extension granted by the approving authority will be based on the circumstances applicable to that candidate. There should be no waivers accepted or approved if an individual's certification has expired.

(3) Certification candidates and certificants must submit all waivers to DOD SPēD certification requirements, in accordance with this regulation to: usarmy.pentagon.hqda-dcs-g-2.list.sped-waivers@mail.mil.

(4) Army employees seeking a waiver must fill out the waiver request form located at http://www.cdse.edu/documents/sped/waiver_form.pdf. The form must provide sufficient explanatory detail why they cannot complete their certification maintenance requirement within the regularly scheduled 2-year window. Army employees seeking a waiver will furnish supporting documentation (such as SF-50, orders) or a memorandum signed by their supervisor.

(5) Army SPēD waiver committee, consisting of the Army SPēD Program manager, CP19 CPM, and CP35 representation will review the waiver submission, including supporting documentation, and then accept or reject the request.

(a) Approved waiver period will be tied to the length of circumstance, but will not exceed 180 days.

(b) Notification of all decisions will be sent to the individual within 15 working days of receipt of the request.

(c) Army SPēD Program manager will simultaneously provide the DOD SPēD Certification PMO with documentation of the decision and all support material submitted with the waiver request.

(6) In the event a waiver is denied, DOD Manual 3305.13-M provides candidates and certificants 90 days to file an appeal.

(7) All appeals must be submitted within 90 calendar days from the date of receiving an appealable decision or after completing a certification assessment.

(8) Grounds for appeal include:

(a) Examination results.
(b) Candidate registration.
(c) Test taking protocols.
(d) Eligibility related to cheating, alleged violation of professional rules of conduct or the law, or inaccurate information on the application form.
(e) Certification maintenance and PDUs.
(f) Certification disciplinary matters.

(9) Appeals packages must be submitted to the DOD SPēD Certification PMO using the designated secure electronic form or application. The following information must be included in the submission:
(a) Appellant's name.
(b) Appellant's candidate ID.
(c) Appellant's work telephone number.
(d) Appellant's work email address.
(e) Appellant's work address.
(f) Command, agency, component, or company.
(g) Unit (if applicable).
(h) Grounds for appeal.
(i) Documentation supporting the appeal.
(j) Description of the event being appealed (including, but not limited to dates, locations, information relevant to the appeal).
(k) Witness information and statement(s) (include witness name and contact information, and a description of the relevance to the appeal).
(l) Desired outcome of the appeal.

(10) Candidates and certificants can find additional information regarding the certification appeals process at http://www.cdse.edu/help/certification-appeals.html.

Chapter 4
Physical Security Resources

4–1. General
Physical security resources are provided to protect Army critical assets, resources, and capabilities including national security information and materiel. Although the consequences of a loss of a critical asset or resource to a threat action cannot be totally mitigated, the intent of physical security resourcing is to achieve no greater than a moderate level of risk to the Army mission. Commanders and directors may request commercial solutions if DA standardized equipment is not available or does not meet a technical requirement. Commands will forward an operational needs statement to the DA Staff or TRADOC user representative when there is a need to develop standardized equipment. Once a component or system is developed or adopted from commercial sources it is considered standardized and may be adopted by all DOD components to satisfy Joint operational requirements.

4–2. Management Decision Package physical security matters
The MDEP QPSM resources the physical security measures necessary to protect Army installation and SAFs from threats to readiness to generate, project, and sustain Army forces. This includes dollars and manpower to control access to installations or SAFs; protect arms, ammunition, and explosives; nuclear, chemical, and biological material and other critical assets or resources, and to perform the Army Physical Security Program. Allowable obligations include: civilian pay, equipment acquisition, sustainment, and maintenance. The MDEP QPSM resources operations and maintenance; procurement; and research, development, test, and evaluation of physical security equipment; site improvements; security management and planning staffs; and security forces and technicians necessary to protect the warfighting readiness for the Regular Army, U.S. Army Reserve (USAR), and Army Reserve National Guard (ARNG). See DFAS-IN 37-100 for more information on this MDEP.

4–3. Requirements and resources
a. The MDEP QPSM is generally not used for activities organized under DOD or DA business rules that require resourcing by other than the Army base program. It is also not intended for commercial businesses, and research, development, test, and evaluation activities.

b. PSOs will identify requirements through the planning, programming, budgeting, and execution system. Army commands will review and validate subordinate unit physical security requirements in Schedule 75 of the Automated Schedule and Reporting System.

c. General officer quarters may have physical security requirements, but these quarters are usually resourced with MDEP Army Family Housing Operations. The use of MDEP QPSM for these quarters will be determined on a case-by-case basis.

d. Planning for lifecycle replacement, maintenance, and repairs of equipment installed with military construction (MILCON) funds, which are QPSM requirements should be considered when planning physical security resources.

e. Resourcing lifecycle replacement, maintenance, and repairs of equipment installed with MILCON funds and then considered real property will be funded with sustainment, restoration, and modernization funds.

f. The MDEP QPSM will be used to provide adequate physical security to—

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

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

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

(4) The military banking facilities outside the continental United States (OCONUS), per DOD 7000.14-R.

(5) The military postal system per DODM 4525.6-M.

(6) Child development centers per AR 608-10.

4–4. Physical security for military construction

a. Military construction projects will be reviewed at the conceptual state and throughout the design stage. Current risk- and threat-appropriate physical security capabilities will be incorporated with construction requirements and design. Significant changes in risk or threat occurring during the construction process may require a revised cost and risk analysis.

b. Commands will use the DD Form 1391 and coordinate with the USACE Electronic Security Center, the Protective Design Center, and their local PSO office to ensure physical security protective measures are planned.

c. Qualified PSOs with the H3 identifier in accordance with paragraph 3-3, will ensure physical security requirements for military construction are identified for planning purposes, per AR 420–1. In general, construction funds PSE such as fencing, security lighting, vehicle barriers, warning signs, and signaling devices.

d. MILCON funds resource the equipment installation, but not the actual equipment purchase. Commands will ensure that PSE requirements not resourced with MILCON funds are programmed.

e. Equipment requirements unique to the command will be annotated in construction documents but are not resourced with MILCON funds.

f. A qualified command PSO will coordinate with the master planner to ensure physical security requirements are identified in construction documents and the DD Form 1391 in Tab E, furnishing and equipment data.

g. Physical security requirements not resourced with MILCON funds will be coordinated through the appropriate IMCOM region and installation master planer for the integrated process team.

h. For the ARNG, engineering personnel for Joint-use facilities managed by the ARNG and for other ARNG facilities will ensure that storage of AA&E meets minimum physical security criteria such as for IDS, locks, hasps, and lighting, as necessary, for the category of AA&E involved. Maintenance of physical security measures will be planned and executed by engineer personnel, when the occupants accept the new facilities.

i. Planning for physical security requirements for Army Reserve installation and SAF construction projects, and for physical security requirements not resourced with construction funds is a coordinated effort between the Army Reserve Installation Management Directorate, the USAR installation or regional support command, and USARC G-34 Physical Security Branch.

4–5. Physical security for Corps of Engineers' civil works and like projects construction

Physical security funding requirements for USACE civil works and like projects construction are identified per USACE's Engineering Circular (EC) 11-2-2##. The EC provides policy for the development and submission of the Corps of Engineers direct civil works budget and work plan for each fiscal year. As a result, this document is revised and issued annually with a new EC number suffix (EC 11-2-206 for fiscal year 2016, EC 11-2-208 for fiscal year 2017, and so forth).

Chapter 5
Security Identification Cards and Badges

5–1. Purpose
Security ID cards and badges provide a visual means to determine if the bearer is authorized to be in a certain restricted area(s). The intent of using security ID cards and badges is to combine their use with physical protective measures and other security procedural measures to increase safeguards to Army resources against espionage, sabotage, damage, destruction, and theft by controlling personnel movement in restricted areas.

5–2. General
a. The DOD CAC may be used as a credential to provide access to Army facilities. The CAC also may be used as a security ID badge when authorized by local command policy. The CAC is a controlled item and will not be used for temporary badge issuance exchanges.

b. Determination will be made by local commanders or directors if security ID cards and badges are to be used in addition to other required ID cards for military personnel, DOD Civilian employees, contractors, and visitors entering installations, buildings, and other areas.

5–3. Minimum security identification card and badge requirements
a. Security cards and badges will be designed and managed per AR 380-5, controlled, and accounted for, and will contain—

(1) A passport-style photograph for personnel who have been granted privileges for continuous access.

(2) For visitors, the term VISITOR will be prominently displayed and the term ESCORT REQUIRED or ESCORT NOT REQUIRED.

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

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

5–4. Computerized card and badge systems
a. Systems that generate a personal identification number (PIN) for security cards and badges will be programmed to—

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

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

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

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

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

(1) Every 3 years for limited and exclusion restricted areas however, CAC used in accordance with HSPD-12 for access to limited and exclusionary areas will be audited every 3 years.

(2) Every 5 years for controlled restricted areas. This requirement does not apply to issuance of the DOD CAC, but is only for security cards and badges issued to supplement the CAC as required by the responsible authority.

(3) Immediately when believed to be comprised.

d. A new PIN will be requirement to be changed if compromised or subjected to compromise and when a replacement card or badge is issued.

Chapter 6
Restricted Areas

6–1. General
a. This chapter provides requirements on the definition and designation of restricted areas within the United States. OCONUS, the commanders and directors may use information in this chapter to set local procedures, according to U.S. and host nation agreements.

b. Army installations, facilities, SAFs, operational areas, and some of USACE's civil works and like projects are restricted areas. At a minimum, the type of restriction is the controlled level (see "restricted area" in the glossary).

c. Minimum requirements for controlling access to restricted areas will be per this regulation.

6–2. Command authority

a. DODI 5200.08 authorizes military commanders and directors to issue regulations to safeguard DOD property and places under their command. This authority is derived from Section 797, Title 50, United States Code (Section 21 of The Internal Security Act of 1950). In accordance with AR 600-20, command of Army installations or SAF is exercised by an SC. The SC's command authority includes all authorities inherent in command, including the authority to ensure the maintenance of good order and discipline for the installation. Commanders and directors of military installations and SAFs have the authority to publish and enforce rules.

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

6–3. Designation of restricted areas

a. Commanders and directors of installations, SAFs, and facilities will designate them, in writing as restricted areas.

b. Unit commanders will designate areas under their control as restricted per AR 190-11, AR 190-17, AR 190-54, AR 190-59, AR 380-40, and other policies as applicable. Lists of unit-restricted areas will be provided to the installation or garrison commander.

c. Responsible USACE commanders and directors of USACE laboratories, centers, FOAs, divisions, and districts (including civil works and like projects) will designate, in writing, areas under their control as restricted areas based on documented analysis and decision-making, defined herein, or per AR 190-11, AR 190-17, AR 190-54, AR 190-51, AR 190-59, AR 380-40, and other policies as applicable. List(s) of restricted areas will be provided to the next higher headquarters and included as a separate annex in the site-specific security plan.

d. The type restriction will also be determined: controlled, limited, and exclusion, respectively each type is more restrictive.

6–4. Prohibited actions

A summary of pertinent sections of Title 18 of the United States Code follows concerning the prohibited acts announced on IACP signage, and signage placed at controlled entrances to restricted areas at other DA resources, facilities, activities, buildings, and so forth, that are not on an installation, depicted in figure 6–1.

a. 18 USC 795 prohibits photographing and sketching defense installations, and other DA resources, facilities, activities, buildings, and so forth, that are not on an installation, without permission from the senior commander or designated representative, through the Public Affairs Office.

b. 18 USC 797 prohibits publication and sale of photographs of defense installations, and other DA resources, facilities, activities, buildings, and so forth, that are not on an installation, without permission.

c. 18 USC 1382 restricts entering or reentering military, naval, or Coast Guard property for any purpose prohibited by law.

6–5. Prohibition on commercial image collection and surveillance

a. Commercial imaging surveillance by photography or video recording is prohibited at Army locations. Written procedures will be established and coordinated with supporting legal and public affairs offices, at a minimum. Procedures will establish rules for noncommercial imaging, such as for photography or video recording by Family members, and commercial imaging of events such as graduations and weddings. Procedures approved by the responsible commander or director will be included as a separate annex to the physical security plan.

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

c. Immediately report cases where access has been granted to commercial organization and/or installation imagery is available on a website.

d. Coordinate efforts within installation level—and other non-standard installation agency established force protection—working groups, to provide situational awareness and promote an integrated approach to counter this potential vulnerability.

6–6. Perimeter controls for installations and SAFs

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

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

c. Other fencing material may be used for stand-alone facilities where local ordinance or legal jurisdictions do not allow for chain-link fencing. Where no reasonable type of barrier material is practical, such as along a shoreline, surveillance will be implemented in conjunction with the Force Protection Condition (FPCON) System.

d. Perimeter control requirements for USACE civil works and like projects will be per AR 190–51.

6–7. Posting of restricted areas

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

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

c. Signs will be posted per figure 6–1 at IACPs and facility entry control points and at and other DA restricted area resources, facilities, activities, buildings, recreational areas operated and solely used by DOD personnel, but may located on non-Federal property, and so forth, that are not on an installation. The following declarations, individually or in combination, may be added where applicable—

(1) Deadly force authorized.

(2) Area patrolled by military working dog teams.

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

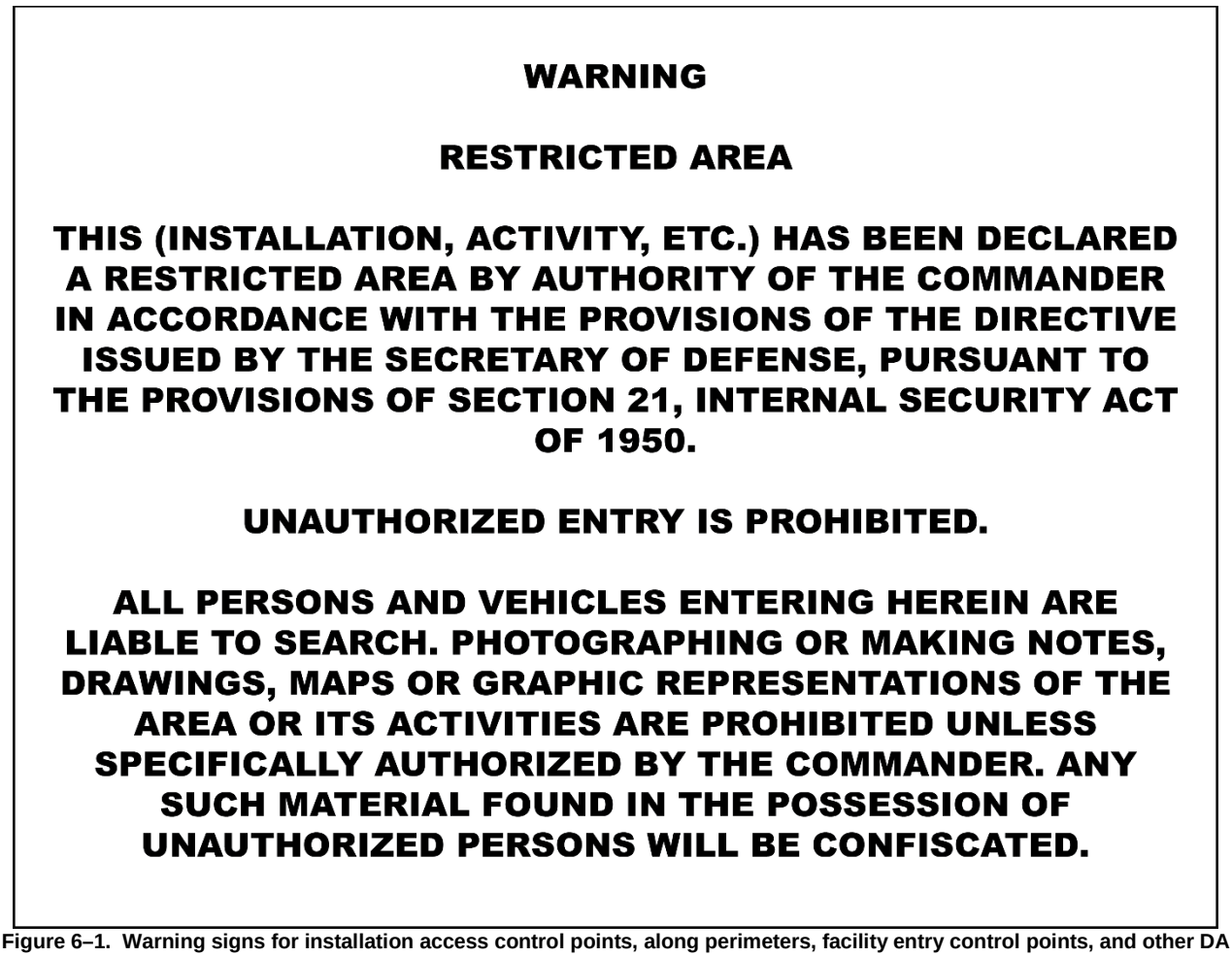

Figure 6–1. Warning signs for installation access control points, along perimeters, facility entry control points, and other DA restricted area resources, facilities, activities, buildings, that are not on an installation

d. Signs will be posted along property perimeters in sufficient numbers so the warning can be readily seen and understood by approaching persons.

e. All signs will be posted in English and the host nation language. The warning notice is also recommended to be written in other languages predominant to the area, as a safety and legal precaution.

f. Current warning signs meeting the commander's or director's intent to protect the area do not have to be replaced solely to achieve figure 6–1. Signs, when replaced due to no longer being serviceable, will be to figure 6–1 standards.

g. There is not specific font or size required for warning signs; however, signs should be easily readable from a reasonable distance no less than 50 ft.

h. Guidance for signs can be found in UFC 3–12–01.

6–8. National Defense Areas

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

b. Establishing a National Defense Area temporarily places such non-Federal lands under the effective control of DOD and results only from an emergency event.

c. The senior DOD representative at the scene will define the boundary, mark it with a physical barrier, and post warning signs. Every reasonable attempt will be made to obtain the landowner's consent and cooperation in establishing of the

National Defense Area. Military necessity, however, will determine the final decision regarding National Defense Area location, shape, and size.

d. The authority to establish a National Defense Area includes the authority to deny access to it. It also includes the authority to remove persons who threaten the orderly administration of the National Defense Area. Any use of force employed to enforce this authority will be per AR 190–14.

6–9. Procedures for restricted area violations

a. The standard and nonstandard installation, or garrison, commander or director will cause any person who enters a restricted area without authority to be immediately brought before proper authority for questioning.

b. The person may be searched per AR 190–30. Any notes, photographs, sketches, pictures, maps, digital images, media, and files or other material describing the restricted area may be seized.

c. Persons brought before proper authority for questioning will be advised of their rights per AR 190–30. Questioning will be conducted without unnecessary delay.

d. The person will be warned against reentry and released if it is determined that the person was unaware of the restriction and did not acquire or intend to acquire knowledge of sensitive or classified information.

e. The actions below will be taken if it appears that the person knowingly entered a standard or nonstandard installation restricted area, or may have acquired or intended to acquire sensitive or classified information by entering, or may have committed some other offense—

(1) Persons not subject to the Uniform Code of Military Justice (UCMJ) will be taken to civilian law enforcement officials. In the United States, the nearest FBI office will be notified and the person will be turned over to the nearest U.S. Marshal. If the person cannot be turned over to a U.S. Marshal within a reasonable period of time (generally 3 to 4 hours), the person will be taken before an appropriate State or local official (see 18 USC 3041). As soon as possible, the agency to which the person is transferred will be given a written statement of facts with the names and addresses of witnesses, and pertinent exhibits as may be available.

(2) Persons subject to the UCMJ will be turned over to their command or the proper military law enforcement official.

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

g. Commanders and directors OCONUS will coordinate with host nations per status of forces agreement for the handling of persons who enter restricted areas without authorization.

h. The responsible commander or director for restricted areas not on a standard or nonstandard installation or garrison will cause any person who enters a restricted area without authority to be immediately reported to local law enforcement or facility security officer (guard) for action as required for any trespasser. The responsible commander or director will establish and follow the agency's protocol for upward reporting to their next higher headquarters. A restricted-area-violation standard operating procedure will be developed and included as a separate annex to the physical security plan. The plan should clearly define who has the authority to apprehend, detain, or question the perpetrator, and define differing protocol for those that cannot.

Chapter 7
Physical Security Councils, Working Groups and Boards

7–1. Purpose

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

a. Purpose. The PSC will be a forum for the commander or director to gain involvement from subordinate commands and tenant organizations in physical security program design and implementation.

b. Functions. As appropriate at each command level, the PSC will—

(1) Provide guidance on how to develop and distribute the criminal threat assessment.

(2) Coordinate development of the command, installation, and tenant physical security plans to synchronize.

(3) Evaluate the effectiveness of the physical security program.

(4) Evaluate policy compliance.

(5) Recommend resource priorities for the commander or director.

(6) Analyze the collective effects of observations from inspections, surveys, exercises, and recommend remedial measures.

(7) Review visitor control procedures.

(8) Evaluate crime prevention efforts.

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

(10) Develop security education requirements.

(11) Review existing regulations, directives, and plans for consistency.

(12) As needed, coordinate with the USACE Protective Design Center on a reimbursable basis for the review, proper application, and implementation of facilities standards and criteria to meet physical security and antiterrorism requirements.

(13) As needed, coordinate with the USACE Electronic Security Center on a reimbursable basis for the review, proper application, and implementation of electronic security systems.

c. Composition.

(1) The senior PSO or designated representative will chair the PSC.

(2) Key staff directorates at all command levels will be PSC members. The PSC should also include tenant organizations at the installation or garrison level.

7–2. Army Physical Security Enterprise and Analysis Group

a. Purpose. Provide executive oversight, guidance, synchronization, collaboration, and coordination amongst the funding, requirements, acquisitions, and development lines of effort to transition PSE to the mission owner, and to provide material solutions to protect the force and assure the mission.

b. Lines of effort. The Army Physical Security Enterprise and Analysis Group (APSEAG) has four lines of effort that must be synchronized, through collaboration and coordination, amongst interested stakeholders: Resourcing, Acquisition, Requirements, and Development.

(1) Resourcing: Leverage the planning, programming, budgeting, and execution process in partnership with both DOD and Army organizations to acquire, allocate, and manage resources for APSEAG efforts.

(2) Acquisition: Leverage the Defense Acquisition System in partnership with the appropriate Program Executive Office and program managers as a means to transition PSE to appropriate mission owners.

(3) Requirements: In partnership with TRADOC, leverage the Capability Base Assessment Process articulated in the Joint Capabilities Integration and Development System (JCIDS) manual, in partnership with the mission owner, to determine strategic and operational materiel requirements.

(4) Development: Leverage partnerships with U.S. Army Research, Development, and Engineering Command (RDECOM), Army Research Office, USACE, academia, sister Services, other government organizations, and commercial entities to develop, exploit, and/or demonstrate innovative advances to ensure the Army and DOD's PSE technology.

c. Functions. Serve as a flexible mechanism to support the APSEAG framework, comprehensively addressing PSE policy issues, shaping program planning, supporting the Army program objective memorandum process, and ensuring a unified effort among all PSE elements.

(1) Provide direction to Army PSE research, development, and acquisition programs.

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

(3) Provide priority recommendations to DOD and Army governances and organizations.

(4) Coordinate continuous assessments of Army PSE development programs in inventories.

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

(6) Collaborate with other government and defense organizations concerning PSE matters, and provide representation to the working groups established per DODI 3224.03.

(7) Ensure Army PSE exploratory development initiatives are incorporated by the mission owners.

d. Composition.

(1) The Physical Security Division Chief, on behalf of the PMG, will chair the APSEAG.

(2) One core member or advisory representatives (O–4, O–5, or CE) will be provided by each of the following organizations—

(3) Core participants.

(a) ASA (ALT).

(b) ACSIM.

(c) DCS, G-3/5/7.

(d) TRADOC (MSCoE).

(e) Army Materiel Command (RDECOM).

(f) USACE.

(g) IMCOM.

(4) Advisory representatives.

(a) ASA (IE&E).

(b) ASA (M&RA).
(c) ASA (FMC).
(d) CIO, G–6.
(e) DCS, G–1.
(f) DCS, G–4.
(g) DCS, G–8.
(h) Forces Command.
(i) Other organizations, at the chair's invitation.

e. Administration.

(1) The APSEAG will meet quarterly, or more frequently at the call of the chair.

(2) Execution of the APSEAG will be in accordance with the APSEAG Charter.

(3) Correspondence will be sent to the OPMG, Office of the Provost Marshal General, Physical Security Division, Room MF748, 2800 Army Pentagon, Washington, DC 20310–2800.

f. Subgroups. Groups subordinate to the APSEAG will be established as needed to address specific PSE material solution efforts.

Chapter 8
Army Installation and Facility Access Control

8–1. General

a. This chapter prescribes general policies and requirements for controlling access to Army standard installations (defined as IMCOM full service domestic garrisons) and nonstandard installations. These are installations not primarily supported by IMCOM but may include Army Material Command facilities that are Government-owned, Government-operated and Government-owned, contractor-operated. Also included are USACE, USARC, and ARNG installations, as well as SAFs in the continental United States (CONUS) and OCONUS. (All of these will be referred to as "installations" for the remainder of this chapter.) Installation access control is a critical aspect of the Army Physical Security Program and the Army Insider Threat Program. Commanders and directors responsible for installation security will comply with the policy in this chapter to vet personnel for access to Army installations against authoritative U.S. Government databases, to prevent unauthorized access and detect and deter potential criminals, terrorists, or other security and insider threats. Commanders and directors will employ access control measures at the installation perimeter to ensure security and protection of personnel and resources.

b. IACPs (for standard and nonstandard installations and some SAFs) and a controlled perimeter are fundamental to the Army's defense-in-depth approach to physical security. The IACPs will be located at the outermost boundary of the installation, or cantonment area of installations, where security checks will be performed on personnel, vehicles, and materials before potential threats can gain close proximity to Army resources. The IACPs consist of both passive and active barriers arranged as an integrated part of a contiguous, controlled perimeter.

c. The IACPs are designed to defeat vehicle as well as pedestrian threats, as prescribed in the Army Standard Design for IACPs (Appendix F, OPMG Criteria) and to ensure safety of motorists, pedestrians, and guards. (See also UFC 4-022-01, in app A of this regulation.) The IACPs consist of the physical infrastructure along with manpower, technology, and operational procedures that commanders and directors employ to control access to Army installations. The IACPs are identified by usage type as shown in table 8–1.

d. In locations where SAFs do not yet have an IACP capability established, the following is required at a minimum:

(1) Control access to the SAF at the outermost controlled boundary (or building entrance if the SAF is a single building without a fence).

(2) At multibuilding SAFs with a contiguous perimeter, perform security checks at the outermost controlled boundary entrance before allowing access to any building within the SAF property.

Table 8–1
Installation access control points usage types

Classification	Operational hours	Preferred operation
Primary	24/7, open continuously	Regular operations for DOD card holders entering in vehicles. Visitor processing and pass issuance capacity. Could also be designated as truck and delivery ACP.
Secondary	Regular hours, closed at times	Regular operations for DOD card holders and visitors with pass. Could also be designated as truck and delivery ACP.
Limited use	Only opened for special purposes	Tactical vehicles, construction equipment, HAZMAT, special events, range access, emergency access, and so forth.
Pedestrian access	Varies	Pedestrians only. Could be located near installation housing areas, near schools, or as part of a primary or secondary ACP.

8–2. Visitor control program

a. Commanders and directors will establish and maintain a visitor control program to ensure only authorized individuals enter the installation. Commanders and directors will not grant visitors unescorted installation access without the required identity proofing, vetting against the National Crime Information Center Interstate Identification Index (NCIC-III), the Terrorism Screening Data Base (TSDB) and determination of a valid purpose for entry for all personnel who do not possess a CAC, another Federal personal identity verification card, or other DOD ID card.

b. The visitor control program will include a process to verify a person's need to access the installation. CAC holders, military retirees, and military Family members have an inherent official purpose and therefore are authorized to access Army installations. This inherent official purpose does not apply to "restricted access" areas on the installation, unless properly cleared.

c. Non CAC-holding visitors, contractors, vendors, and other personnel as described in paragraph 8–4 below, must have a need validated by a DOD component for one-time, intermittent, or routine physical access to an Army installation. The process will include procedures for—

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

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

(3) A process to identity proof personnel desiring access and vet their identity personnel records to determine fitness for unescorted access—

(a) CAC holders are already identity proofed and vetted to DOD personnel security standards.

(b) Persons possessing other DOD-issued ID cards such as retirees and dependents are also considered identity proofed and vetted for unescorted access.

(c) If a retiree, or DOD ID card holder, wishes to gain employment on the installation as a contractor, then that person's "status" will change to a contract employee, which triggers the requirement for an employment background check and an NCIC-III check for access to the installation. Contractors without a CAC, working at RC SAFs, will undergo an employment background check and local records check provided on a DD Form 369 (Police Records Check) or local law enforcement form. The antiterrorism operations security coversheet for contracts also states this requirement.

(d) Persons possessing Federal personal identity verification (PIV) credentials that conform to Federal Information Processing Standards Publication 201-2 (Personal Identity Verification for Federal Employees and Contractors) are adjudicated by Government security specialists, in accordance with national agency check with inquiries standards, or OPM Tier I standards, and are considered identity proofed once the PIV can be verified electronically. This is done via the Defense Manpower Data Center (DMDC), the AIE for installations, or other authorized system for SAFs. Other requirements for access such as fitness and purpose still apply.

(e) All other non-USG ID card applicants will provide a valid and original form of ID (State driver's license, passport, and so forth, which complies with Public Law 109-13 (The REAL ID Act of 2005)). This is to prove identity (for enrollment into the AIE database if available) and issue a visitor pass or card. Security personnel processing an applicant will screen documents for evidence of tampering, counterfeiting, or other alteration.

(f) Non-DoD visitor personnel OCONUS will have an internationally acceptable ID document such as a passport, national ID used for international travel, or other suitable ID for identity proving, as outlined in the host nation agreement.

d. Commanders and directors will oversee execution of these procedures for vetting non-DOD affiliated personnel (visitors and non CAC-eligible contractors):

(1) Conduct a check of the NCIC-III and the TSDB on non DOD-affiliated visitors 18 years of age and older to determine if the person requesting unescorted access presents a potential threat to the good order, discipline, or health and safety on the installation. Commanders and/or directors of installations are authorized to conduct random ID checks and vetting of persons requiring access to their assigned installations, as necessary and appropriate. The FBI permits the use of NCIC-III to vet non-DOD personnel for the security of military installations. The Interstate Identification Index contains automated criminal history record information. Implementation of the TSDB query is required when the capability becomes available to DOD.

(a) Procedures: the NCIC-III and "persons" files checks are accomplished by using the "QWI" inquiry under the purpose code C. The QWI is an NCIC inquiry message which provides the authorized user with the capability to access both the NCIC-III (for criminal history) and NCIC persons files simultaneously with one inquiry. The NCIC persons files includes wanted persons, known or appropriately suspected terrorist (KST) list, missing person file, foreign fugitive, wanted person, gang, protection order, immigration violator, identity theft, supervised release, violent person, protective interest files and the National Sex Offender Registry. This requirement applies to all unaffiliated personnel (visitors) not in possession of one of the ID cards listed in paragraph 8–4*a*, below.

(b) Vetting against NCIC-III is a law enforcement function. It must be overseen by law enforcement personnel and must conform to the requirements established in the FBI Criminal Justice Information Services (CJIS) security and specific State policy guidelines.

(c) Army law enforcement personnel will have direct oversight of contractors if they are employed for NCIC administrative duties to include processing of visitors or other contractors in accordance with the requirements in FBI CJIS and State security policy. Army law enforcement personnel will supervise contractors and ensure they are properly trained and certified by the State to conduct NCIC-III checks. However, contractors may not make fitness determinations. Only Government personnel that are designated in writing by the senior commander are authorized to make fitness determinations. Designations will be in writing by duty position and codified in local guidance.

(d) All personnel operating NCIC terminals must be in compliance with FBI CJIS and an individual State's policies regarding security awareness, training, and certification and carry out these actions:

(2) Conduct a check of records in the TSDB when available. The TSDB is the U.S. Government's authoritative consolidated database that contains terrorist identifiers concerning individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to, terrorism or terrorist activities.

(3) Use the adjudication standards in paragraph 8–5.b to vet non-DOD affiliated personnel (visitors and uncleared contractors) and recommend disposition (allow entry, deny access and/or process for waiver).

e. Commanders and directors will conduct similar records checks for non-U.S. persons, per status of forces agreements, and other theater policies. When available at OCONUS locations, NCIC-III vetting requirements are the same for U.S. persons.

f. Commanders and directors will provide local access ID (access passes or cards) for visitors and others requiring unescorted access as follows—

(1) Persons receiving local access ID must have a validated need to enter and must conform to identity proofing, vetting against NCIC-III, and fitness determination requirements provided in paragraph 8–4, below.

(2) Implement procedures to issue, revoke, retrieve, or turn-in expired local access ID.

(3) Register personnel issued local access ID in an installation access control database that records fitness determination decision, date of issuance and expiration, revocation, and other information necessary to track and account for visitor processing. These capabilities are already provided to installations using automated installation entry (AIE).

(4) Local access IDs will only be issued for routine physical access onto the single installation or facility where it is issued.

(a) However, individuals who have been previously vetted and issued a local access card at another installation, that is enrolled in DMDC's Identity Matching Engine for Security and Analysis (IMESA) through AIE or Defense Biometric Identification System (DBIDS), can be automatically registered at another IMESA installation by presenting this same credential for access at the ACP as long as they provide a valid need for access.

(b) Installations with unique mission requirements may choose not to implement automatic registration and instead require individuals who have not previously registered at that installation to be processed through the Visitor Control Center (VCC) at their first visit.

(5) Local access IDs should be issued for no more than 1 year or until the expiration date of the documents used to support the issuance (most repeat visitor access situations require either a 90-day pass for short term or a 1-year credential rather than relying on repeated NCIC-III vetting for single day passes).

(6) The terms "visitor," "escort not required," or "escort required" will be prominently displayed along with an expiration date on all local access IDs.

(7) For long term badges (up to 1 year), incorporate features to local access IDs that decrease the likelihood of forgery such as:

(a) Including a digital photograph of the holder including a unique identifier such as an embossed seal or other similar device to enable quick visual determination of authenticity.

(b) Laminating or otherwise increasing tamper resistance.

(c) Inventory and account for visitor IDs on a regular basis.

(d) Randomly validate issued IDs to ensure authenticity and monitor expiration dates and times.

g. Commanders and directors at installations with AIE can use the person's REAL ID-compliant State driver's license as their installation access credential once the person has been vetted and registered into the AIE database. (PL 109-13 (The REAL ID Act of 2005).) AIE has the capability to link the person's state driver's license to the electronic access control database, therefore eliminating the need for an installation to produce an installation short or long-term access credential.

h. Commanders and directors will ensure the Privacy Act Statement shown in figure 8–1 will be conspicuously posted in the Visitor Control Center and all locations where personnel ID information is being collected to conduct vetting procedures.

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 9397 (SSN); Title 10 U.S.C. Section 3013; DoDD 8500.1

PRINCIPAL PURPOSE(S): To provide installation commanders and law enforcement officials with the means by which information may be accurately identified to determine if an applicant meets authorized access requirements. Use of SSN is required to make positive identification of an applicant. Records stored in the Automated Installation Entry (AIE) System are maintained to support Department of the Army physical security and information assurance programs and are used for identity verification purposes, to record personal data registered with the Department of the Army, and for producing installation management reports employed by security officials to monitor individuals accessing Army installations. Other acceptable identification e.g. Common Access Cards (CAC), EDI PI will be used to distinguish individuals who request entry to Army installations.

ROUTINE USE(S): The "DOD Blanket Routine Uses" are set forth at the beginning of the Army compilation of systems of records notices.

DISCLOSURE: Voluntary; however, failure to provide the requested information will result in the denial of an authorized access pass (or equivalent) and denial of entry to Army installations.

Figure 8–1. Privacy Act Statement for a Visitor Control Center

8–3. Automated installation entry visitor pre-screen for access control point security

a. Installations fielded with AIE have a non-DOD affiliated (visitor) pre-screen capability that provides a complete, quick NCIC-III check using States' National Law Enforcement Telecommunication Systems (Nlets) connections at an AIE registration station screen or handheld scanner. This capability is authorized for use subject to the following conditions:

(1) At no time will a unit mission tasking Soldier use the AIE pre-screen component that uses Nlets for criminal history screening (NCIC-III) of non-affiliated personnel (visitors).

(2) This component provides law enforcement sensitive information, so it can ONLY be used by law enforcement personnel and the Department of Army security guards (DASGs) that meet the following requirements:

(a) Completed all required State-provided NCIC and Nlets training.

(b) Successfully passed the State's certification test required from the State CJIS security official (if required by the State).

(c) Established individual Nlets account settings which grant permission to make Nlets queries.

(d) Can properly log into the AIE system via VCC registration station or handheld scanner.

(e) AIE system administrator has enabled this capability.

b. It is a criminal offense for inappropriate persons to fraudulently use an authorized user's account for accessing information through Nlets.

c. Detailed NCIC-III results are not sent to the registration station screen or handheld scanner. Instead, pre-screen findings are sent to a national level analytical engine for comparison to the Army Adjudication Standards depicted in paragraph 8–5*b* below. In turn, the analytical engine sends only a pass (green), fail-deny (red), inconclusive (amber) or fail-detain (red-active warrant) notification which indicates the following:

(1) Pass (green): person does not have derogatory information which would prohibit entry to the installation based on the Army Adjudication Standards. Person will be registered into the AIE database and a visit expiration date indicated, based on the purpose of the visit or unescorted access on either an AIE installation access pass or linked to the person's State driver's license.

(2) Fail-deny (red): deny access, person has derogatory information in NCIC-III based on the Army adjudication standards. The visitor can go to the Visitor Center for screening at an NCIC terminal, where a text response from a NCIC-III check will provide the reason(s) for the red light given for the in-lane pre-screen.

(3) Inconclusive (amber): deny access, inconclusive information from Nlets. The visitor can go to the visitor center for screening at an NCIC terminal by an operator.

(4) Fail-detain (red-active warrant): apprehend. An active warrant exists for the visitor, reason will be displayed under the information tab; will require law enforcement adjudication, similar to a felony traffic stop.

8–4. Personnel authorized unescorted access

a. Personnel in lawful possession of a valid form of the following ID cards are authorized unescorted access onto Army installations:

(1) DOD CAC.

(2) DD Form 2S (RES) (Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)); DD Form 2S (RET) Blue (United States Uniformed Services Identification Card (Retired) (Blue)); or DD Form 2S (RES RET) (United States Uniformed Services Identification Card (Reserve Retired) (Red)).

(3) DD Form 1173 (Uniformed Services Identification and Privilege Card); DD Form 1173–1 (Department of Defense Guard and Reserve Family Member Identification Card); DD Form 1173–1S (PRIV) (United States Uniformed Services Identification and Privilege Card) (Reserve Dependent) (Red); or DD Form 1173S (PRIV) (United States Uniformed Services Identification and Privilege Card (Dependent) (Tan)).

(4) DD Form 2765 (Department of Defense/Uniformed Services Identification and Privilege Card) (Tan).

(5) Retired DOD Civilian ID card. Retired DOD Civilians are eligible for the DOD Civilian Retiree ID Card. This card provides them with a trusted credential to identify their affiliation with DOD and establish their identity for entering DOD installations to access Morale, Welfare, and Recreation (MWR) facilities. This is an optional card that can be issued for civilian retirees that use base MWR facilities. If retirees already have retiree cards from their DOD service component or agency, they do not need this card. This card does not convey any additional privileges and is valid for and renewable every 8 years. Civilians who have retired from any DOD service component or agency can get the card when they are in receipt of their DOD retirement pay. Civilian retirees from other Federal agencies are not eligible.

(6) Blue striped CAC (for non-U.S. citizens). Since July 2015, all CACs have been issued with an affiliation color code in a white circle under the expiration date, including "W" for white, "G" for green, and "B" for blue. These changes are meant to make it easier for visually color-impaired security officials to identify bearers who are military, Government, contractor civilians, or foreign nationals. The new format will only be issued for new and expiring cards. The blue striped CAC (for non-U.S. citizens) is a valid DOD ID credential and may be used for unescorted installation access. These CACs state "Identification Card" on the bottom front of the card. Blue striped CACs must be registered in AIE to associate the person with the local installation. Installations without AIE will perform a visual check of the card and picture to authenticate before allowing access. Dependents of blue striped CAC holders can receive an installation pass. Newly hired foreign national personnel will be issued an AIE local pass (up to 6 months) while they wait for their CAC application to be approved. When the new hire person receives their blue-striped CAC, replace their installation pass by registering their blue-stripe CAC in AIE. The foreign identification number is the number the Defense Enrollment Eligibility Reporting System (DEERS) generates and assigns to non-U.S. citizens in conjunction with issuing a blue striped CAC or Teslin card (such as, dependent wife, DD Form 1173). If anyone with a blue striped CAC has an issue with their computer certificate or other computer or CAC related issue, they need to go to the ID card office that issues CACs.

b. Non CAC-holder contractors and vendors.

(1) Contractors and vendors requiring physical access to a single Army installation or facility, but who do not require access to a DOD computer network, will have a Government-employee sponsor to provide the contractual agreement with a cover memorandum signed by a verifying officer vouching for the need for long-term access to the installation. The expiration date of the issued card will be the end date of the contract or visit, or the expiration date of the sponsor's access control card, whichever occurs first. Sponsors will be held responsible for notifying the DES (or appropriate local installation access issuing office) of terminated contract employees and for turn in of expired or revoked ID.

(2) Contractors will be processed through the Contractor Verification System for issuance of a CAC, if physical access to multiple Army installations and/or access to a DOD computer network is required.

(3) Non CAC-eligible contractors will be issued local access ID that will only be used for physical access onto the single installation or facility where it is issued. Commanders and directors will use a locally produced, temporary issue, local access ID system pass with expiration date, or a pass issued by AIE or the DBIDS, if available.

c. Other personnel requesting long-term recurring installation access. The personnel listed below are recognized as having a valid requirement for long-term, recurring access to Army installations. Commanders and directors will vet the personnel below against NCIC-III (and TSDB when available) and issue a local access ID card for 1 year or less, or for long-term access as follows:

(1) Family care providers. Unit commanders and directors will use the Family care plan per AR 600–20 to review and validate requests by Soldiers for installation access for Family care providers after completion of initial identity proofing and vetting.

(2) Army volunteers. The director of an activity will review and validate requests to grant unescorted installation access for Army volunteers and forward the request to the senior law enforcement official after completion of initial identity proofing and vetting.

(3) Gold star and next of kin survivor Family member unescorted access. The "survivor access card" will be used for both gold star Family members and next of kin survivors. The Army's AIE system will issue an AIE card marked "Survivor." Installations where AIE is not yet fielded will continue to issue the DA Form 1602 (Civilian Identification Card) with "Survivor" typed in the status block.

(a) A gold star Family member is a survivor of a Service member who has lost their life during any armed hostilities in which the United States was engaged and authorized to wear the "Gold Star Lapel Button," in accordance with AR 600–8–22.

(b) The next of kin Family member is a survivor of a Service member who lost their life while serving on active duty. This includes service members who lose their lives while assigned to a reserve or National Guard unit in drill status. Eligible survivors are the remarried widow or widower (widows and widowers are eligible to retain their dependent ID card), parent, child, stepchild, child through adoption, brother, half-brother, sister, and half-sister of the deceased Service member.

(c) Procedures: The survivor Family member will contact the installation level Survivor Outreach Services (SOS) support coordinator, who will receive and review requests for access card(s) and verify eligibility. The SOS support coordinator will forward the request to installation access control to be vetted, in accordance with paragraph 8–5 for unescorted installation access. When vetting is successfully completed, the survivor access card will be issued for a 3-year period. No additional vetting is required during the 3-year period. Survivors who have previously been vetted and issued a survivor access card at another installation that is enrolled in DMDC's IMESA, through AIE or DBIDS, can be automatically registered at another IMESA installation. This is done by presenting this same credential for access at the ACP, without undergoing vetting again at the VCC as long as they provide a valid purpose for entry.

(d) Commanders will support access by Family members who are gold star and next of kin survivor members to the extent practical, but this does not apply to critical sites whose mission does not allow access of unescorted non-DOD personnel, or during periods of elevated security where additional screening is required.

(4) Transportation worker identification credential (TWIC) holders may be granted unescorted access to the installation after completion of identity proofing and initial vetting using NCIC-III and the TSDB and based on a valid purpose for entry to deliver commodities, provide services, or other actions approved by the commander or director. Additional documentation should be provided such as a commercial driver's license, government bill of lading or other documentation identifying a requirement or need to enter the installation. Once initial vetting is completed, and the TWIC holder is registered into the IMESA via AIE or DBIDS, continuous vetting is accomplished via the IMESA, which authorizes use of the TWIC as an identity credential for future installation access without additional initial vetting until TWIC expiration. This process is only authorized at AIE or DBIDS installations connected to the IMESA for continuous vetting.

(5) The veteran's health identification card (VHIC) is issued to veterans by the Veteran's Administration (VA) as a form of ID for appointments at VA care facilities. Veterans may request long-term access to the installation using the

VHIC after completion of identity proofing and vetting. Three options are available if a Veteran fails to meet access control adjudication standards for unescorted access—

(a) Submit a waiver to the garrison commander or director, as specified in paragraph 8–5.

(b) Change to a VA medical clinic that is not located on an Army installation.

(c) Arrange to be escorted by a DOD ID card holder.

(6) Privatized housing and lodging personnel.

(a) General public tenants are civilians with no DOD or Federal government affiliation.

(b) General public tenants that lease military housing privatization initiative housing will be vetted before being granted unescorted access to an installation.

(c) Installation access expiration dates will be based on the signed lease terms and will align with the end of the tenants' lease.

(d) Non-DOD personnel requesting to stay in privatized lodging on an installation will be vetted against NCIC-III, in accordance with paragraph 8–5, before granting unescorted access to the installation. They will be issued installation access based on signed lease terms.

(7) Non-profit, non-governmental organizations. These organizations that provide support for Soldiers and their Family members will be granted long-term access after being vetted, in accordance with paragraph 8–5, to access the installation.

(8) Official foreign visitors. The following official foreign visitors will be granted unescorted access and are exempt from a check of NCIC-III and TSDB records, in accordance with paragraph 8–5, unless otherwise directed by the senior commander or director:

(a) Official foreign visitors subject to the provisions of AR 380–10 (for example, foreign liaison officer, foreign exchange personnel, and cooperative program personnel) will be granted unescorted visitor status. The Foreign Visit System-Confirmation Module will be used to confirm that a proposed official visit by a foreign government representative has been approved through the Foreign Visit System and to record the arrival of such visitors. The module is available at http://spanweb.dtsa.mil/systems/fvs-cm.

(b) For visitors subject to the provisions of AR 12–15, the sponsoring U.S. Government office will provide documentation to the senior law enforcement official, or equivalent, that such visitors have been security screened per the policy's requirements.

(9) West Point student Family members. Senior commanders and directors can approve credentials for West Point student Family members for up to 4 years upon completion of initial identity proofing and vetting, in accordance with paragraph 8–5. Upon graduation or dismissal from West Point the Family member status will be revoked and further access to the installation will require individuals to process onto West Point through normal visitor control program.

(10) Consideration for extended visitor passes, other than stated above, are done on a-case-by-case basis and commands must request in writing using the security criteria deviation process in paragraph 2–3.

d. Search procedures and random antiterrorism measures apply to all personnel, regardless of the type of access control card they possess.

8–5. Fitness adjudication standards and procedures for installation access control

a. General.

(1) This policy describes the minimum Army standards for controlling unescorted access to Army installations for visitors, uncleared contractors, and other persons not eligible for a CAC or other form of ID listed in paragraph 8–4*a*. These standards provide the framework for determining the potential threat to good order and discipline and/or health and safety on the installation and fitness of such persons for unescorted access to an installation. A similar records check will be conducted at OCONUS locations per status of forces agreement and other theater regulations.

(2) Fitness for unescorted access to Army installations will be determined by an analysis of information obtained through authoritative government data sources. The sources, at a minimum, include the NCIC-III and TSDB (when available) to determine if granting unescorted access to a person presents a potential threat to the good order, discipline, or health and safety.

(3) Only U.S. Government officials designated by the senior commander will conduct the fitness determination. The designation will be in writing by duty position and annotated in local policies and procedures.

b. Unescorted access determination. Army senior commanders, in the absence of an approved waiver, deny persons access to installations based on information obtained from the results of a NCIC-III check, using the "QWI" under purpose code C, and the Terrorist Screening Data Base when available. These government-authoritative data source checks give an indication if a person may present a threat to the good order, discipline, and morale of the installation. This information includes, but is not limited to a person who has:

(1) NCIC-III contains criminal arrest information about the individual that causes the senior commander to determine that the person presents a threat to the good order, discipline, or health and safety on the installation.

(2) A claimed identity that cannot be verified based on the reasonable belief that the person submitted fraudulent identity information in the attempt to gain access.

(3) Current arrest warrant in NCIC, regardless of the offense or violation.

(4) Current bar from entry or access to a Federal installation or facility.

(5) Conviction of crimes encompassing sexual assault, armed robbery, rape, child molestation, production or possession of child pornography, trafficking in humans, or drug possession with intent to sell or distribute.

(6) Conviction for espionage, sabotage, sedition, treason, terrorism, or murder.

(7) Being registered as a sex offender.

(8) Felony conviction within the last 10 years regardless of the offense or violation.

(9) Felony conviction for a firearms or explosives violation regardless of when the conviction occurred.

(10) Engaged in acts or activities designed to overthrow the U.S. Government by force.

(11) Been identified in the NCIC KST file or TSDB report as known to be, or is suspected of being, a terrorist or belonging to an organization with known links to terrorism or support of terrorist activity. Installation access control personnel will strictly follow the FBI's published engagement protocols.

c. Procedures for TSDB notifications:

(1) The KST list is derived from the TSDB, maintained by the FBI's Terrorist Screening Center (TSC). KST "hits" may be received either during initial vetting using QWI inquiry of non-DOD affiliated personnel or at installation access control points using AIE or DBIDS systems connected to Identity Matching Engine for Security and Analysis (IMESA), which checks TSDB as part of continuous vetting.

(2) DOD and FBI have jointly agreed to engagement protocols for responding to KST and/or TSDB hits. The TSC labels terrorist suspects with various handling codes. These codes will be attached to the KST-TSDB hits sent to the installation. Army installations and agencies that receive IMESA-accessed TSDB information are required to strictly follow the handling code procedures given in the IMESA alert and response.

(3) At no time during an encounter will the subject of a KST-TSDB hit be notified, directly or indirectly, that he or she is on a watch list. This procedure is key to fulfilling our responsibilities to FBI agreement for sharing KST-TSDB data with DOD. Only personnel trained and certified to access and use TSDB information (NCIC trained and certified) will be authorized to handle TSDB information in the DOD IMESA process. Installation law enforcement activities must retain all personnel training records for as long as the member has access to the system and up to the period of the next audit.

(4) Following the encounter, installation access control personnel will report the incident to the Army Threat Integration Center, available 24/7 at commercial: (703) 695–5300 or Defense Switched Network: (312) 225–5300, or by email at: usarmy.pentagon.hqda-dcs-g-2.list.dami-artic@mail.mil and OPMG at usarmy.pentagon.hqda.mbx.opmg-ps@mail.mil.

d. Active warrant processing.

(1) If an active warrant is identified during visitor vetting, a warrant confirmation message (also known as a "hit" confirmation) is sent via NCIC to the agency that entered the warrant.

(2) Per system requirements, the agency has to respond to the warrant confirmation response with a verification that the warrant is, or is not, active.

(3) A message from the originating agency, indicating an active warrant, will have instructions to either hold the individual or instructions to advise the individual of the warrant and release from custody. In situations where the warrant is confirmed to be active and extradition is requested, installation security personnel (DA police, security guards, or military police) will detain the individual for the law enforcement agency.

(4) Persons with an active, confirmed warrant can be detained up to 3 hours pending the arrival and release to the extraditing agency. If the extraditing agency is unable to send an officer within 3 hours, arrangements with local law enforcement should enable custody transfer until the detainee can be released to the extraditing agency.

(5) If a U.S. person OCONUS is found to have an active warrant, the procedures above will be followed. However, in a case where the warrant is issued from CONUS, commanders and directors must develop procedures to hold, secure, and transfer individuals as required.

(6) If an active warrant (security alert) is detected at an ACP, via AIE continuous vetting, in addition to the procedures listed above, installation law enforcement personnel will notify their respective Installation Personnel Security Office (PERSEC) of the incident, for possible security clearance action.

e. Installation access denial waiver process.

(1) Senior commanders will use the following waiver process if an uncleared contractor is denied access based upon derogatory information obtained from an NCIC or NCIC-III check, but only if the person requests a waiver. Access control

personnel will issue instructions to the denied person on how and where to submit a waiver if one is requested. The instructions will advise the person to perform the following actions—

(a) Obtain a certified copy of their complete criminal history to include all arrests and convictions.

(b) Obtain a letter of support from their U.S. government sponsor. The letter must indicate that the sponsor requests that the person be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visits. If a contractor employee is terminated, the sponsor must inform the senior commander so that unescorted access to the installation is no longer authorized.

(c) Submit a letter requesting the access denial be waived, to the Government sponsor who will be responsible for submitting it to the senior commander. The letter must include all offenses, plus an explanation why the conduct should not result in denial of access to the installation. Other factors that the sponsor/the requesting individual should address are the —

1. Nature and seriousness of the conduct.
2. Specific circumstances surrounding the conduct.
3. Length of time elapsed since the conduct.
4. Age of the person at the time of the incident or conduct, and
5. Proof of efforts toward rehabilitation.
6. Current mailing address or email address for Army communications.

(2) The government sponsor will review the person's information for completeness and determine whether to endorse the request for a waiver.

f. If the government sponsor endorses the waiver letter, he/she will provide a letter of recommendation for the person. The letter must address the relevant conduct that caused the denial and indicate why the conduct should not prohibit the person from being granted unescorted access to the installation. The government sponsor will submit the letters to the senior commander.

g. Personnel without a government sponsor will apply the criteria in paragraphs 8-5*e*(1) and (2) when submitting a waiver request.

h. The senior commander will render a determination in line with good order, discipline, and health and safety on the installation. The senior commander will provide a copy of the determination to the person.

i. The results of the senior commander's decision will be provided to the installation Directorate of Emergency Services or Provost Marshal Office (PMO) to update applicable access control databases.

j. Persons who had a waiver request denied may request reconsideration from the senior commander 1 year after the date of the commander's decision. Persons may request reconsideration earlier if they can present significant information that was not available at the time of the original request or show that the basis for the original denial was overturned, rescinded or expired.

k. Commanders of installations and SAFs report initial vetting and continuous vetting denial results on a quarterly basis through the secure portal located at https://army.deps.mil/army/sites/pmg/team/ps/pages/installationdata.aspx, in accordance with appendix J.

8–6. Additional security instructions concerning contractors

Commanders and directors will review installation access control procedures and ensure law enforcement, security forces, and supporting contracting personnel take action to prevent access by unauthorized contracted persons as follows—

a. Comply with contractor vetting requirements per AR 525–13. Compliance will include implementing a verification process to determine the trustworthiness of a contractor or subcontractor. The process should be done by ensuring that contracts require background checks to meet installation access requirements. Installation access vetting will be accomplished by the PM, DES, or PSO service that vets non-DOD-affiliated personnel using NCIC and the TSDB. A similar records check will be conducted at OCONUS locations per status of forces agreement and other theater policies.

b. Ensure that activities requesting access for contractors complete an antiterrorism risk analysis and that security measures are considered before the requirements package is sent to the contracting officer. The contract will be reviewed to ensure the—

(1) Contracted workforce is compliant with all identity-verification requirements.

(2) Reason for access is validated by the requiring activity.

(3) Type of access and privileges are appropriate.

(4) Period of access is specified.

c. Contracting officers or their representatives will conduct a compliance review of existing services contracts and all new service contracts. This ensures that contracts exceeding the simplified acquisition threshold—and which do not meet

one of the exceptions specified in Federal Acquisition Regulation (FAR) 22.1803—will include FAR 52.222-54. The FAR 52.222-54 requires the contractor to enroll in the E-Verify program within 30 calendar days of contract award.

d. Contractors are also required whether already enrolled in E-Verify or newly enrolled to verify the employment eligibility of all new employees and employees assigned to the contract within the specified time limits mandated by the FAR clause. Commanders and directors will coordinate with the contracting officer for remediation actions if compliance violations are suspected or identified.

8–7. Escorted personnel

Personnel not affiliated with the DOD who are not vetted against NCIC-III or OCONUS procedures will—

a. Be escorted at all times while on the installation in accordance with local policy by an Army person authorized to escort and be accompanied for the duration of the individual's visitation period. Army personnel authorized to escort visitors include uniformed Service members and spouses, DOD employees, CAC-holding contractors, retired Service members and spouses, and retired civilian personnel.

b. Be in possession of a valid, REAL ID-compliant, State driver's license, State ID card with photo, a valid U.S. passport, or a valid passport from other countries cleared by the State Department, and will present it to request access to an Army installation.

c. Non-DoD visitor personnel OCONUS will have an internationally acceptable ID document, such as a passport or national ID used for international travel.

d. The number of personnel allowed to escort at any one time will be determined by the local installation's commander, director, or designated representative.

8–8. Trusted Traveler Program

The purpose of a Trusted Traveler Program is to expedite access for Service members and dependent spouses, DOD employees, and retired Service members and spouses; maintain efficient vehicle throughput; mitigate traffic congestion on adjoining highways; and allow trusted travelers to vouch for occupants. The program allows a uniformed Service member or government employee with a valid DOD CAC, a military retiree (with a valid DOD ID credential), or an adult dependent 18 years or older (with a valid DOD ID credential) to present their ID credential for access to the installation while simultaneously vouching for any vehicle occupants.

a. Commanders and directors may establish a Trusted Traveler Program for use during FPCON NORMAL, ALPHA, and BRAVO, as local security conditions permit.

b. The program is governed and implemented locally and may not be recognized by other installations.

c. The number of personnel a trusted traveler is allowed to sponsor at any one time will be determined by the local installation commander, director, or designated representative.

d. Persons identified as trusted travelers are responsible for the actions of all occupants for whom they sponsor and for meeting all requirements for escort, as established by the Army or installation commander or director.

e. The Trusted Traveler Program applies to the outermost perimeter of the installation. It does not apply to accessing facilities or areas inside the installation.

f. Trusted travelers cannot vouch for persons with foreign passports or ID cards, who must instead be cleared per paragraph 8–2.

g. Vehicle occupants that are sponsored by the trusted traveler must be 18 years of age or older and be in possession of: a valid picture ID card such as a REAL ID-compliant State driver's license, State ID, DD Form 1173 (Uniform Services Identification and Privilege Card), DD Form 2 series, or passport, issued by an authoritative state or federal agency so they can be readily identified.

h. Occupants under the age of 18 that do not possess a valid picture ID card may be sponsored by an adult occupant of the vehicle that is cleared to enter the installation.

i. Commanders and directors, at their discretion, may suspend the Trusted Traveler Program based on the local threat or may revoke individual trusted traveler privileges.

j. The program will be suspended at Force Protection Condition levels Charlie and Delta. Commanders and directors will ensure the Installation Area Access Control Plan reflects procedures when the Trusted Traveler Program is suspended.

k. DOD contractors in possession of a CAC, in accordance with paragraph 8–4, although authorized unescorted access, are not authorized trusted traveler privileges.

l. Commanders will implement policies to remove the trusted traveler status of any ID cardholder engaged in conduct that is detrimental to good order and discipline on the installation. This would include those personnel who are subjects of a criminal investigation.

8–9. Personnel performing security functions at installation access control points will conduct the following procedures—

a. Validate personnel identification. Verify the identity of all personnel entering an installation by visually examining CACs, Teslin cards, and locally produced, temporary visitor passes to include—

(1) Visually matching the photograph with the face of the person presenting the ID card. Installations using AIE can do this by checking the digital photo on the AIE monitor or handheld.

(2) Verifying authenticity by visually checking the anti-counterfeit or fraud protection measures embedded in the ID card, or authenticating ID cards, using automated means at installations where AIE is fielded. At locations where AIE is fielded, commanders or directors may authorize non-USG visitors and contractors to use their REAL ID-compliant State driver's license as an access credential once they are vetted against NCIC-III and registered into the AIE database. Use of REAL ID-compliant State drivers' licenses as a local credential will allow an installation to transition and eliminate the need for locally issued, short-term passes and long-term badges for installation access.

(3) Confiscating expired, defaced, or damaged credentials in accordance with inter-Service instruction AFI 36-3026, for return to the issuing office.

b. Screen vehicles and persons for unauthorized weapons and contraband. Consider random inspections and using military working dogs, and other screening technology, when available. Inspect private and commercial vehicles per prevailing force protection condition measures and security directives.

c. Assess potential threat behavior. Assess personnel in vehicles and pedestrians for suspicious or threatening activity per Training Support Package (TSP) 191-5323. Personnel will be denied access if they are observed acting in a suspicious or threatening manner.

d. Employ automated access control systems.

(1) Senior commanders and directors will implement AIE when available. AIE is the Army physical access control enterprise system being fielded, per Army requirements and specifications, to automate authentication of personnel ID against DOD-authoritative databases. At increased threat levels, the AIE system will enable adaptation of increased authentication requirements. When AIE is installed, commanders and directors will ensure all eligible installation personnel are registered in the system.

(2) ACP guards will employ AIE pedestal-mounted card readers, or handhelds, to scan CAC, Teslin, AIE access badges, State driver's licenses (if an individual has been initially vetted and registered into the AIE database), and other authorized credentials. These AIEs will vet individuals entering, against the local database and DMDC's IMESA, to authenticate credential against DEERS, any NCIC wants and warrants, debarments, basic-training failures, and DOD local population databases, for any derogatory information. The NCIC wants and warrants are updated in IMESA every 24 hours, and debarments and basic-training failures every hour, so security personnel at the ACP get a current security check against individuals every time they are scanned at the IACP.

(3) As soon as AIE indicates a security alert when an individual scans their credential, immediate adjudication procedures will take place with installation law enforcement to adjudicate the security alert and process the individual, if necessary. AIE security alerts will be recorded and reported to higher headquarters on a monthly basis.

e. Garrison commanders and directors may deny access to the installation through a debarment order. The AIE, DBIDS, and installation access control system (IACS) are authorized DA access control systems that can use and maintain debarment information. See AR 190-45 concerning administration of expelled or barred persons. The OCONUS use of the DBIDS or the IACS may continue to operate and incorporate system updates as required.

f. Emergency response vehicles.

(1) During an emergency response, if notified by civilian authorities in advance, the DES or senior law enforcement representative can waive basic requirements (identity proofing, fitness, purpose) for first responders responding to the emergency.

(2) Installation DES will coordinate a plan with responding organizations that includes procedures for radio notification of emergency access before arriving at the IACP and incorporate procedures into civilian-military training scenarios.

(3) DES should consider designating certain access control points for use by in-bound emergency response vehicles, in the installation plan and training scenarios.

8–10. Accepting law enforcement credentials for access to Army installations during non-emergency situations

a. The number of various credentials issued by various agencies makes it virtually impossible for someone working an IACP to know if the credential is legitimate.

b. Law enforcement credentials will not be accepted as installation access credentials by any person in civilian clothes operating an unmarked vehicle. DOD law enforcement personnel must present their CAC. Other Federal agents must

present their federally issued PIV, which can be scanned by AIE and verified against the certificate revocation list held at the Defense Manpower Data Center, as opposed to law enforcement credentials.

c. Law enforcement officials who do not have a DOD-issued CAC, a federally issued PIV, or if the installation cannot scan or verify the PIV, they will be vetted using their REAL ID-compliant State driver's license. This will be checked against NCIC-III for proper identify proofing and vetting. After initial vetting, the person can be enrolled into the AIE database by linking their driver's license as a credential, or they can be issued an installation's long-term access badge.

8–11. Special event access control

a. Senior commanders and directors with installation security responsibilities will clearly define access-control measures required to manage special events, circumstances, and activities on the installation. They will define the measures in the Installation Area Access Control Plan, per paragraph 8–17.

b. Senior commanders and directors may waive NCIC-III vetting for personnel attending during special events, activities, and circumstances, if it is impractical.

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

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

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

(3) Directing, at a minimum, persons without a DOD access control credential per paragraph 8–4 to the specific gate(s) where security measures are conducted prior to entrance onto the installation.

d. AIE hand-held visitor pre-screening that uses Nlets can be used. Depending on the FPCON System or local threat, random vehicle checks by military working dog teams and magnetometers should be considered.

8–12. Instructions for car-sharing service drivers

a. All taxi drivers and ride-sharing drivers (such as Uber, Lyft, and so forth) must present a driver's license and show proof of insurance, and all vehicles must be properly registered.

b. Visitors, including taxi and ride-sharing vehicle drivers, must undergo identity proofing and vetting against NCIC-III and TSDB when available, in accordance with paragraph 8–5, to determine fitness. Although drivers for ride-sharing services or taxis would then have a valid credential after proper vetting, their purpose would still need to be established for each visit, which can be accomplished by showing the ride sharing hail on a smartphone or identifying the person and building for the pickup. This applies whether they present an AIE hard card or pass, or a registered REAL ID driver's license.

c. Trusted Traveler also does not apply to a ride-share driver travelling with a Service member to enter the installation as "escorted," without going through the visitor control protocol, because they will no longer be escorted after dropping off the Service member at the destination.

8–13. Bus and school bus access

IACP guards will board the bus and check all personnel to ensure there is no duress situation, either scan or inspect their ID, and then allow the bus to proceed. All personnel (with the exception of students on an authorized school bus) who fail to provide the required ID will disembark the bus and wait for the bus to return.

8–14. Instructions for on-post medical treatment facilities

a. Some Army hospitals are also community hospitals that provide treatment for non-DOD personnel that have not been vetted for installation access because they are transported by emergency vehicle directly to the hospital.

b. The medical staff will notify garrison law enforcement personnel—

(1) Of patients that were not vetted for installation access due to being transported by emergency vehicle.

(2) Of patients brought in for treatment that are the subject of a crime or pending an interview by a civilian law enforcement agency before the patient is released.

(3) If a patient is absent from a location defined by the patient's privileged status, regardless of the patient's leave or legal status.

(4) If a patient leaves the hospital against medical advice.

8–15. Installation access control point automation design requirements

a. Commanders and directors will implement AIE when available. Deviations from the Army AIE standards and specifications are not authorized without written approval from HQDA (DAPM–MPP–PS). Army organizations will not procure or field automated IACP systems of any type on Army property without prior written approval from HQDA (DAPM–

MPP–PS). HQDA (DAPM-MPP-PS) must approve the use of DBIDS at specific installations until AIE is fielded at the location. All Army IACP automation must be compliant with FIPS 201, DODI 1000.25, DODI 5200.08, and DODI 8520.02. All IACP automation must meet Department of Defense Information Risk Management Framework requirements, DOD privacy policy, and the Freedom of Information Act.

b. The PdM-FPS and USACE will execute the HQDA centrally managed IACP program, per written direction from HQDA (DAPM–MPO–PS). Report AIE system performance problems to the AIE Help Desk at 877–640–6597, or email at: c4isrsystemssupport@csra.com.

c. Installations using commercial systems or services to simplify installation access control will not employ it for initial vetting, in lieu of NCIC-III vetting, for determining fitness for access. All information gleaned from these open source systems must be verified with authoritative government sources before access is approved or denied. Commercial companies cannot perform functions that must be performed by the government (such as, inherently governmental functions). Contractors can legally receive information and make recommendations to government officials, but they cannot perform adjudicative decision-making functions (such as deciding to grant or deny access credentials). Commercial companies also cannot perform background checks not required or authorized by Army or DOD policy, or maintain personal identification information data beyond their approved system of records notices, which are required under the Privacy Act of 1974, 5 USC 552a. These commercial systems or services, when operating in accordance with all such requirements, will no longer be authorized once AIE is fielded at a specific location.

8–16. Installation access control point construction standards

a. All new MILCON and MILCON-funded renovations and improvements to installation access control points (ACP) will be reviewed during initial planning and construction with the U.S. Army Corps of Engineers PDC and the COS.

b. Facility construction and road work for IACPs will be executed per the Army standard for ACPs, exception being USACE civil works and like projects ACPs which are not eligible for Direct Army funding. Deviations from the standard are not authorized without prior written approval from ACSIM per AR 420–1. The Army ACP standards and standard design can be found at https://mrsi.erdc.dren.mil/cos/nwo/acp/.

c. Planners will coordinate with USACE PDC and the Surface Deployment and Distribution Command Traffic Engineering Agency (SDDCTEA) to perform traffic engineering studies on IACP projects and coordinate with state and local authorities and the US Department of Transportation, as needed, during all phases of an IACP project.

d. For OCONUS installations, designers will coordinate with USACE PDC and COS, along with host nation government agencies per the appropriate status of forces agreement.

8–17. Installation area access control plan

a. An area access control plan will be implemented containing clearly defined access control measures required to safeguard facilities and accomplishment of the mission. This plan will be synchronized with installation antiterrorism plans. RC and USACE SAF area access control plans will address facility entry access to buildings located on RC and USACE SAF property. Tenant unit commanders and directors will provide their unique requirements, as necessary, for inclusion in the installation access control plan. The plan will contain, at a minimum—

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

(1) The use of physical and/or natural barriers, access control points, electronic security systems, and security forces deployed to detect, delay, and deny entry to unauthorized personnel or vehicles at the activity perimeter.

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

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

(1) Armed sentries.

(2) Active vehicle barriers (AVBs) capable of stopping unauthorized entry of suspect vehicles per the Army Standard for Access Control Points included with the Army's ACPs standard design. The type, placement, and commissioning of AVBs to ensure ACP operational security and safety will be coordinated with USACE PDC.

(3) Search procedures to detect explosives and other prohibited items.

(4) Procedures to reject unauthorized personnel or vehicles that have penetrated the installation perimeter.

(5) Procedures to close IACPs when throughput falls below 100 vehicles per hour during certain time periods, except those designated as primary ACPs.

(6) Procedures for closing all nonoperational IACPs, to include locking them with approved locking devices or having barriers installed that preclude vehicle and pedestrian entry and exit.

(7) Unmanned "egress only" IACPs are not authorized. Requests for an exception to this policy must receive an endorsement from the USACE COS for ACPs before submitting to OPMG for consideration.

(8) Procedures to govern the degree of control required over personnel and equipment entering or leaving the installation and restricted areas within it. This will include a description of access control measures in use and the method for establishing authorization for entering and leaving each area, as it applies to both personnel continually authorized access to the area and to visitors, including any special provisions concerning nonduty hours.

(9) Use of local access ID and military ID cards, CAC and DBIDS cards, to include—

(a) Details of where, when, and how they will be displayed for access control.

(b) Procedures to be followed in cases of loss, theft, forgery, or damage.

(c) Replacement procedures.

(10) Procedures for inspecting persons, their property, and vehicles at entry and exit points of installations and restricted areas including—

(a) When and how frequently inspections are conducted, and whether they are random or mandatory for all.

(b) Legal review by the appropriate legal advisor prior to issuance.

(c) Use of RAM within existing security operations to reduce patterns, change schedules, and visibly enhance the security profile of the installation.

(d) Emergency plans for increased vigilance and restricting access at installations for national emergencies, natural and manmade disasters, heightened FPCON System levels, significant criminal activity, civil disturbance, and other contingencies that would seriously affect the ability of installation personnel to perform their mission.

(e) Process for coordinating with local, State, Federal, or host country officials, as well as tenant organizations, to ensure integrity of restricted access to the installation and reduce the impact on primary missions and surrounding civilian communities.

(11) Maintenance of adequate physical barriers installed to control access.

(12) Designation of posts, personnel, equipment, and other resources to enforce restricted access and response to incidents.

(13) Process for removal of, or denying access to, persons who are not authorized or are a threat to order, security, and discipline.

(14) Annual exercise of contingency plans, including systems for alerting and evacuation of personnel.

(15) A mechanism to keep appropriate personnel informed of the plan and their responsibilities.

(16) The number, design, and placement of IACPs, to include gatehouses, approach routes, barriers, sentry posts, and vehicle control devices, will be coordinated with USACE PDC and COS to ensure they are constructed per the Army Access Control Point Standards and Army Standard Design.

(17) The number of vehicular IACPs should be kept to a minimum, and plans should consider—

(a) Traffic volume.

(b) Traffic patterns to limit high-speed approaches to IACPs.

(c) The IACP designated for employees only, with others reserved for visitors and delivery vehicles.

(d) Perimeter protection measures adjacent to IACPs.

(e) Response planning for gate runners.

(f) Protection against reverse entry and ramming attacks.

(g) Protected guard positions.

(h) Controlled parking areas for visitor parking and use in vehicle inspections that are inside jurisdictional boundaries, but preferably outside the perimeter fencing and barriers.

(i) Road patterns to enable vehicle queuing, and turnaround of unauthorized vehicles outside of the final vehicle barrier system in such a way as to prevent them from gaining access.

(j) Vehicle by-pass control.

(k) IACP area lighting.

(l) Location of Visitor Control Center, per Army Standard Design.

(18) Use of temporary traffic lanes outside the installation perimeter for traffic congestion resulting from business rush hours and increased security measures implemented during heightened threat conditions.

(19) Conduct annual exercises of entry control contingency plans, including—

(a) Response to gate runners.

(b) Procedures for alerting emergency dispatch and command personnel.

(c) Transition to heightened Force Protection Condition System levels.

(d) Implementation of RAM.

(20) Response to natural and manmade disasters that include—

(a) Commuting procedures and entry requirements for critical personnel.

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

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

(21) Conduct random vehicle inspections (frequency to be determined by the garrison commander or director) of all privately owned vehicles, and commercial vehicles, that enter onto the installation. Inspect for prohibited items by using explosives-detecting devices and equipment such as hand-held vapor tracers, vehicle and cargo inspection systems, or military working dog teams.

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

e. Maintenance and testing of access control point equipment and systems will be conducted per appendix G.

8–18. Installation access control point security forces

a. Minimum manning for IACPs is two guards, one as an ID checker and one in over watch. At least one armed DASG, DA civilian police (DACP), or military police (MP) will be included in the security force at each IACP in the United States. Unit mission tasking (UMT) Soldiers performing the access control mission will be armed, unless the senior commander determines otherwise, and be issued—

(1) Adequate means of communications.

(2) Assigned weapons and ammunition and trained in their care and use per AR 190–14 and AR 190–56, as applicable.

(3) Personal protective equipment.

(4) For installations with fielded AIE systems, allocations must allow for one DASG per ACP, per shift, for IT system administration, equipment accountability, and leadership oversight.

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

c. Security personnel, to include DASGs, DACPs, MPs, and contract security guards (where authorized) will be trained to control entry at an access control point to prevent unauthorized personnel, packages, and vehicles from entering the installation in accordance with AR 190–56 and special text ST 19-LESM: DA Civilian Security Guard Field Training Manual, sub task 191–389–0045, control entry at an access control point. AR 190–56 outlines active-shooter response, weapons familiarization and qualification, and mandatory annual training requirements. Training and weapons qualification of security force personnel will be per applicable directives: AR 190–56 for all assigned DACPs and DASGs, the statement of work for contract security guards, and ACOM-issued instructions for UMT Soldiers. Training will also include—

(1) Assessing potential threat behavior for suspicious or threatening activity, per Training Support Package (TSP) 191-5323.

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

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

(4) Authorized forms of ID for access to the installation.

d. Manning requirements determination.

(1) Planners will use the factors in appendix G to determine staffing requirements at installation control points.

(2) Planners OCONUS will include allowances for tariff considerations in Europe and reduced stand-off distances in Europe and Korea.

8–19. Provisions to operate outside the continental United States

The OCONUS commanders and directors may continue to use current forms of ID and continue background checks to allow installation access to foreign nationals, contractors, and vendors per status of forces agreement and other theater regulations.

8–20. Controlling entry and exit and reporting of privately owned firearms and weapons

a. Privately owned arms and ammunition on Army property is prohibited unless authorized by the SC, or civilian (senior manager), in accordance with AR 600–20.

b. Signs will be posted at IACPs stating the prohibition of unauthorized firearms.

c. Personnel authorized to access the installation while carrying firearms will adhere to this policy and procedures in AR 190–11.

Chapter 9
Physical Security Equipment Planning

9–1. General

a. ESSs are essential for protection of Army resources in those instances and locations for which dedicated security guards are unavailable, unaffordable, and/or impractical. In virtually every case, ESS can be used as an effective technology substitute. ESS are comprised of major sub-systems such as ACS, IDS, video surveillance systems, and intercom systems.

b. A physical security system may use shared networks in lieu of point-to-point closed communication transmission media, if most practical.

c. Every reasonable effort will be made to physically and logically separate a physical security system, on a shared network, from other devices and systems to best ensure continuous reliability.

d. Physical security systems must be authorized to operate, per the DOD Risk Management Framework. This requirement applies to all systems whether local area network-based, stand-alone, or closed restricted.

e. All information technology-based systems must be registered in the Army Portfolio Management Solution (APMS). System owners should consult with the command's chief information officer. See AR 25–1 and DA Pam 25–1–1 for more information. APMS is available at https://cprobe.army.mil/login.htm?target=/enterprise-portal/web/apms.

9–2. Intrusion detection systems

a. General.

(1) An IDS is a technology substitute for continuous armed guard surveillance required for certain resources, such as AA&E stored in certain configurations, or for constant manning. Examples of constant manning could include an information-processing facility or a facility where controlled medical substances are stored.

(2) HQDA centrally plans IDS replacement, with the exception of USACE civil works and like projects, which are not eligible for Direct Army funding, based on asset criticality and system age. IDS, including those at USACE civil works and like projects, will be replaced on a 10-year life cycle, subject to availability of funds.

(3) ICIDS is the standardized DOD system that will be used by Army organizations not located on Joint bases supported by another Military Department, or at USACE civil works and like projects. Commercial IDS, however, may be used if ICIDS does not satisfy a specific technology requirement. The IDS design and installation of IDS will be per Unified Facilities Guide Specification 28 20 01.00 10.

(4) For specific IDS or electronic security system capabilities and system configuration, refer to the governing policy for the resources under consideration such as arms, ammunition, explosives, nuclear materials, chemical agents and biological agents and toxins assets for design, installation, monitoring and sustainment criteria.

(a) Each of the RCs' ESS program managers maintain standardized engineering baselines (hardware, software, and firmware) for COTS ESS, including IDS. These baselines are centrally managed by the respective program manager and comply with all applicable United Facilities Criteria (UFC), Army Regulations, and cyber security requirements (such as, Risk Management Framework). Acquisition and installation of ESS at ARNG and USAR SAF will not deviate from these baselines without prior approval from the respective RC ESS program manager.

(b) Deployment and installation of all IDS within the RC will be in accordance with each component's ESS program standards and criteria.

(c) Any major end items that will be, or have the potential of being, placed on the network must be certified through the RMF process.

(5) Keys and locks for IDS components will be safeguarded and accounted for per AR 190–51. Keys to IDS components used to protect AA&E will be safeguarded and accounted for per AR 190–11.

(6) Responsible USACE commanders and directors of USACE laboratories, centers, FOAs, divisions, and districts (including civil works and like projects) will ensure any new ESS (such as IDS), CCTV systems, and ACS design must include and be coordinated with the USACE Electronic Security Systems Mandatory Center of Expertise. This is per USACE Engineering Regulation 1110-1-8162.

(7) Additional IDS requirements for USACE civil works and like projects will be per AR 190–51.

b. IDS operational testing.

(1) Users will conduct monthly operational tests to ensure sensor activation, unless otherwise stated in specific regulatory documents. The checks will be conducted in coordination with personnel at the IDS monitoring station.

(2) Monthly operational test data at USACE facilities (including civil works and like projects) will be included as an annex in, or supplement to, the site-specific physical security plan.

(3) Sensors equipped with remote-test features that activate the same as would an actual intruder do not require an operational check.

(4) The DA Form 4930 (Alarm/Intrusion Detection Record) will be used to record test results.

(5) Alarms will be tested during the course of each physical security inspection and annotated on the inspection report and DA Form 4930.

c. IDS maintenance and inspections.

(1) The organizational security manager will perform user test of IDS components for areas containing classified information.

(2) Procedures for, and systems and maintenance checks at, USACE facilities (including civil works and like projects) will be included as an annex in, or supplement to, the site-specific physical security plan.

(3) At 6-month intervals, each zone component will be checked and tested by qualified alarm maintenance personnel during routine preventive maintenance schedules.

(4) The inspection will occur on a 3-month basis for IDS located in OCONUS-based, risk level III facilities, per AR 190–51. The inspection will also occur at facilities determined by the commander or director to be at high risk.

(5) Maintenance will only be performed by qualified personnel. Maintenance will be performed consistent with operational requirements of each system design, to ensure continuous operation and reliability. (See appendix H for testing information.)

(6) The DA Form 4930 will be used to record inspection results.

(7) An inspection will be conducted by qualified technical personnel, to ensure the system meets all minimum acceptable standards, before a new IDS is accepted for operation.

(8) IDS alarm records. The DA Form 4930 will be used to record alarm activations if the IDS does not provide an automated report with sufficient information. A record of all alarms received will be maintained for at least 1 year.

d. IDS signs.

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

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

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

(4) For resources requiring a perimeter IDS (see asset and/or resource specific regulations), warning signs will not be affixed to sensored fences to avoid false and nuisance alarms.

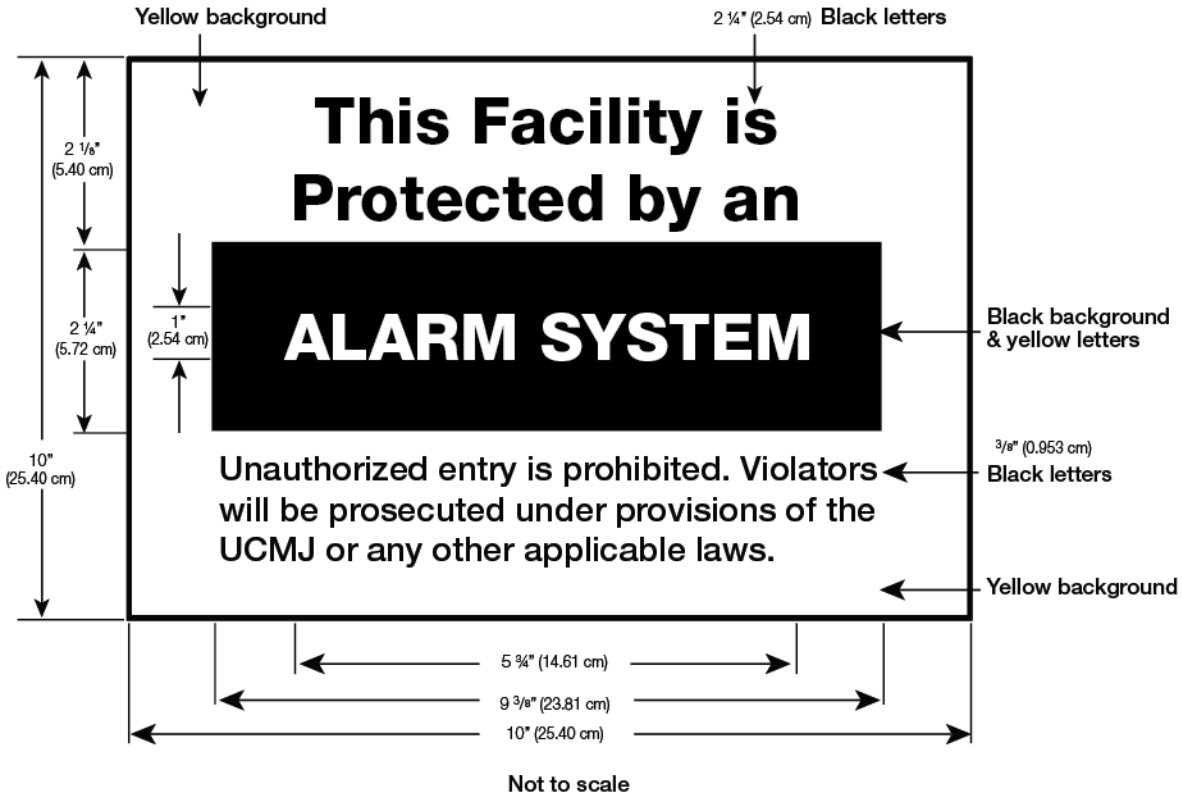

Figure 9–1. Intrusion detection system warning sign

Chapter 10
Security Forces

10–1. General

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

b. Security checks will be conducted on an irregular basis during non-duty hours to avoid establishing a pattern. Security checks will ensure unauthorized personnel are not in the area, and that structures are intact and have not been broken into.

c. Security patrols will physically inspect doors and locks on all storage structures in their area of responsibility during periods of increased vigilance.

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

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

f. DA controlled security forces will be provided with adequate means of communication.

g. Security forces may be armed with appropriate weapons and ammunition at the discretion of the commander or director, as permitted by applicable Federal, State, and territorial statutes, and status of forces agreement. Provisions in AR 190–14 apply if personnel are armed.

h. Armed guards will be immediately required at those MEVAs with IDS when the IDS fails. Commanders and directors will ensure the physical security plan addresses the procedures to arm the guards when needed, in accordance with the applicable regulations governing their MEVA.

10–2. Personnel selection and training
Provisions for selection, hiring, and minimum training requirements for DA civilian guards (GS-0085) will be per AR 190–56. Commanders and directors will adhere to the applicable provisions of AR 190–56, local status of forces agreement, and applicable theater requirements when contracting for security guards.

10–3. Procedures
Guard procedures will be reviewed at least annually, and revised as needed, to provide greater application of security measures. Special emphasis will be placed on guard post locations and guard orientation concerning required duties.

10–4. Inspections and guard checks
Inspections and checks for guards will be increased during nights, weekends, and holidays, based on local threat and as determined by the commander or director to deter violations and to detect asset loss early. Checks will be recorded using the Standard Form 702 (Security Container Check sheet) and will consist of an inspection of the building, facility, or area, including all doors and windows. Records of checks will be maintained for a minimum of 90 days.

10–5. Patrol plans
Security patrol plans will be coordinated and integrated with the guard plan or other security plans and programs to the maximum extent. When facilities are located in civilian communities, liaison will be established with local civil police for periodic surveillance and to coordinate a security plan.

Chapter 11
Management and Use of Unmanned Aircraft Systems on or near Installations

11–1. General
a. This section implements Army policy for the management and use of non-official unmanned aircraft systems (UAS) on Army installations. An unmanned aircraft (UA) is defined as an aircraft operated without the possibility of direct human intervention from within, or on, the aircraft. An UAS is defined as a UA with associated elements, to include communication links and components that control the UA. UAS include remote controlled aircraft capable of sustained flight in the atmosphere, including multirotor, drones, helicopters, fixed-wing aircraft, and other model aircraft.

b. Army installations worldwide include standard installations, non-standard installations and SAFs. Increasing UAS activity on, or near, Army installations raises safety and security concerns. These include overflights of military installations, flight safety hazards to military aircraft, and possible illicit use by criminals and adversaries. Meanwhile, counter-UAS capabilities for base perimeter detection, ID, tracking, point defense, and defeat of UAS are still limited. These factors underscore the need for installation commanders to develop and implement guidelines for regulating Army personnel hobby and recreational UAS use on Army installations and for responding to suspicious UAS activity.

c. The Federal Aviation Agency (FAA) provides policy for regulating the flight of UAS in the U.S. air space to include UAS flight over Army property. By request of the DOD, the FAA has established UAS-specific flight restrictions over specific DOD installations and sites which are particularly national-security sensitive and vulnerable to potential UAS-based threats. These UAS-specific flight restrictions are known formally as special security instructions (SSI). Though the initial number of Army installations protected by SSI is very small, the FAA and the Army will implement SSI for more qualifying Army locations in the future.

d. Self-defense of personnel and assets.

(1) For installations not protected by SSI, no Federal laws or regulations prohibit model aircraft from flying over DOD property in class G (uncontrolled) airspace below 400 feet. By itself, UAS incursion into class G airspace over most installations cannot be the basis for use of force, prosecution, fines, or seizure of aircraft.

(2) Army commanders and directors are authorized to take reasonably necessary and lawful self-defense measures to protect installation personnel and property, including the defense of other DOD forces in the vicinity, in response to a hostile act. Commanders and directors should review the standing rules for the use of force (SRUF) as defined in Chairman of the Joint Chiefs of Staff Instruction 3121.01B, including Notice 1. Interpret the SRUF with consideration of the local operating environment, the resources being protected, and policies related to protecting those resources.

e. Programs and procedures.

(1) Army commands, Army service component commands, direct reporting units, Army National Guard, and Army Reserve will establish programs and procedures to reduce UAS physical security risk for their specific location. Policy drafted by higher-level commands for installations should contain more generalized guidance to help installations develop their own local policies. These programs and procedures will include:

(a) A policy for operating drones on Army Installations.

(b) Coordination procedures with local law enforcement officials to respond to non-official UAS activity on or near installations.

(c) Reporting procedures for any non-official UAS activity that poses a risk to the installation or military aircraft operations. See section 11-4.

(2) Installation UAS policies should be codified in the Installation Defense Plan, appropriate base instructions, and other documents such as housing lease agreements or community standards guidelines.

(3) Public affairs should be leveraged to ensure community awareness of local policies.

(4) OCONUS installations should socialize UAS concerns with host nation law enforcement and legal advisors, and discuss relevant laws and restrictions before establishing policy and negotiating joint response procedures. Policies and procedures related to UAS response must be consistent with host nation laws and the status of forces agreement.

f. This chapter does not pertain to military or official use of UAS. Military or official use of UAS is governed by AR 95-2 and AR 95–23. AR 95–23 addresses the official procurement and operation of non-standard UAS by Army organizations. Personally procured UAS are not authorized for military or official use. For questions pertaining to military or official use, refer to Deputy Chief of Staff, G-3/5/7 Aviation Directorate and the U.S. Army Aeronautical Services Agency.

g. This chapter does not pertain to commercial services using UAS.

(1) Commercial services using UAS originating from within an Army installation are prohibited without prior approval from the senior commander, director, or their designee. Senior commanders or directors may authorize using UAS for commercial purposes, within their installation, on a case-by-case basis. Operators must comply with all requirements for commercial UAS use, found in part 107 of the Federal Aviation Regulations.

(2) Senior commanders and directors should also seek to limit, and monitor, commercial services using any UAS originating from outside an Army installation. Accordingly, residents and organizations within an Army installation are prohibited from receiving commercial services originating outside an installation by means of UAS.

11–2. Non-official, hobbyist and recreational unmanned aircraft system use by personnel affiliated with the installation

a. Recreational use of UAS within an Army installation is prohibited without prior approval from the senior commander, director, or their designee. Senior commanders and directors may authorize use of UAS for recreational purposes, on a recurring, or case-by-case basis. Each authorization will specify the scope of the recreational use, to include designated locations and times approved for flying.

b. When aviation operations are being conducted on Army-owned or Army-leased land, the Army installation rules must be more restrictive to deconflict privately owned UAS with Army aircraft. Additional restrictions also should be considered for active drop zones, ranges, forward arming, refueling points, and ammunition storage areas.

c. Installation commanders and directors are responsible to regulate UAS use and will establish a local policy, program, base orders, or procedures to inform military, dependent, and civilian employee UAS hobbyists. These instructions should address or contain the following items:

(1) UAS must not be operated when the installation is in FPCON Charlie or Delta.

(2) Designation of suitable installation locations and times for UAS activity.

(3) Not to interfere with other military or commercial aircraft operations or endanger personnel or resources.

(a) No manned aircraft, or Army, or commercial UAS operations in progress.

(b) UAS flight must not enter any air space within 2 miles of the active end of a runway.

(c) Other aircraft have the right of way in airspace use. UAS must give way to, and not interfere with, manned aircraft.

(d) UAS operations must terminate at the first indication of conflict with other aircraft.

(e) If within 5 miles of an airfield control tower, the UAS operator must contact the tower watch supervisor before flight. This may include providing contact information and require the UAS operator to call the tower when UAS flying is complete.

(4) Require recreational UAS operators to comply with:

(a) Section 336 of Public Law 112-95 (14 Feb 2012).

(b) Local UAS laws and regulations.

(c) FAA registration and operation requirements found on:

1. http://www.faa.gov/uas/.
2. https://www.faa.gov/uas/recreational_fliers/
3. https://www.faa.gov/uas/getting_started/register_drone/

(5) All UAS greater than 0.55 lbs. must have registration and markings.

(6) Do not fly an aircraft weighing more than 55 lbs.

(7) If UAS is equipped with a camera, operator must comply with installation photography guidelines.

(8) Describe the process for registration at the appropriate installation office.

(9) Describe the processes to check-in and/or notify installation authorities, operations center, military police, or duty staff, as appropriate, before flying the UAS.

(10) Describe the processes to obtain approval from the controlling air traffic services, where applicable.

(11) Restrict UAS operations to the following conditions for flight:

(a) Flight must be restricted to altitudes below 400' and remain clear of surrounding obstacles.

(b) Visual-line-of-sight operations only; keep the UA within visual line of sight at all times.

1. Clear weather.
2. Minimum visibility of 1 mile.
3. Flight limited to daylight hours and civil twilight.

(c) Must not endanger persons or property on the ground.

(d) Careless or reckless operation is subject to legal enforcement.

d. The installation's rules and regulations governing hobbyist UAS use will be disseminated and/or posted as appropriate, such as on-base locations where UAS activity is expected (to advise the public of any restrictions on UAS activities), and at additional locations per senior commander discretion.

e. Procedures for reporting suspicious UAS activity by DOD personnel and their Family members to installation operations center, military police, and/or local law enforcement.

f. The "No Drone Zone" in the Washington, DC area.

(1) Rules written after the 9/11 attacks designate the National Capital Region as a National Defense Airspace and prohibit any aircraft from operating in this region without specific FAA and Transportation Security Administration approval.

(2) The area within a 30-mile radius of Ronald Reagan-Washington National Airport is governed by a special flight rules area (SFRA), which restricts all flights in the greater DC area. Violators face stiff fines and criminal penalties. For more information, see http://www.faa.gov/uas/no_drone_zone.

(3) The SFRA has been divided into a 15-mile radius inner ring and a 30-mile radius outer ring. Flying an unmanned aircraft within the 15-mile radius inner ring remains prohibited without specific FAA authorization.

(4) Flying a UAS for recreational or nonrecreational use between 15 and 30 miles from Washington, DC is allowed under these operating conditions:

(a) Aircraft must weigh less than 55 lbs. (including any attachments such as a camera).

(b) Aircraft must be registered and marked.

(c) Fly below 400 ft.

(d) Fly within visual line-of-sight.

(e) Fly in clear weather conditions.

(f) Never fly near other aircraft.

11–3. Non-official unmanned aircraft system use by personnel not affiliated with the installation

a. Commanders and directors should collaborate with the Provost Marshal's Office, the Staff Judge Advocate, airspace managers, and Airfield Operations to analyze the threat, discuss local policies, laws, jurisdiction, and airspace regulations, and to establish appropriate response procedures.

(1) Installation policies will adhere to physical security requirements and the SRUF outlined in CJCSI 3121.01B.

(2) Prepare plans for rapid cessation, or masking of critical or sensitive activities vulnerable to suspected aerial observation.

(3) Procedures must include a method to immediately inform air traffic personnel of a UAS hazard that poses a risk to military aircraft operations, so appropriate separation procedures can be executed.

(4) Commercial and recreational UAS will suspend operations if the FPCON level rises to FPCON Charlie or Delta.

(5) Special considerations should be made to coordinate with other Services and agencies at Joint use facilities.

(6) Installations will display "No-Drone" signs at all installation entry points and any additional locations, per senior commander discretion.

(7) Conduct UAS awareness campaigns, including information about installation UAS regulations and policies, on the installation and in the local community.

b. Unauthorized use of UAS from within an installation subjects the operator to possible punishment under either the UCMJ, or Federal or State law as well as potential forfeiture of any unauthorized recordings, photographs, or videos. Pursuant to 50 USC 797, violations of a defense installation property security regulation, or an installation UAS policy may be punished as a Federal criminal offense.

c. Liaise with local law enforcement (LE) personnel and civilian prosecutors to identify Federal, State, and local laws and regulations related to privacy, photography, reckless endangerment, and so forth, that may be used to pursue prosecutions and/or civil penalties against UAS operators who fly aircraft over or near Army installations.

d. Establish agreements with local law enforcement (LE) officials to coordinate procedures for local LE response to non-official UAS activity on or near installations, such as assistance in locating operators and enforcing any violations committed beyond installation boundaries.

e. Installation law enforcement personnel are authorized defense of self and the defense of others against any UAS exhibiting hostile intentions. Hostile intentions include any UA behavior which unabated, would inflict physical harm to a person. UAS carrying or delivering weapons, explosives, or other hazardous materials may also be considered a threat to persons.

f. Installation security forces will:

(1) Respond to reports of unauthorized, suspicious, harassing, unsafe, or dangerous use of UAS.

(2) If applicable, immediately notify the Air Traffic Control Tower.

(3) If the UAS poses a physical threat to personnel or resources, respond with measures consistent with the SRUF.

(4) Notify local LE in accordance with the procedures previously established with local LE officials.

(5) Notify installation authorities, operations center, duty staff, and/or Criminal Investigative Division.

(6) Execute appropriate police action: at a minimum, stop, identify, and interview the operator(s).

(a) Locate the operator. Direct attention outward and upward to attempt to locate individuals who are holding a controller or device that appears to be operating an UAS. Look at parked or moving vehicles, windows, balconies or roof tops.

(b) Interview operator and collect the following information:

1. Name, address, and positive ID of operator.

2. Ask UAS operator for the type of operation and to present appropriate documentation. The operator must provide the registration certificate (paper or electronic) upon request.

3. Record registration number, and verify markings on the UAS.

4. Detailed description of the UAS.

5. Document time, place, and details of flight. Take pictures and interview witnesses, and so forth.

(7) After the incident, coordinate with CID, FBI, and FAA investigators as appropriate.

11–4. Reporting requirements

a. Reporting is an essential element for assessing the potential risk and guiding the Force Protection effort. Report all suspicious unmanned aircraft activity that pose a risk to the installation or to military aviation operations.

b. Suspicious UAS activity should be reported in accordance with DODI 2000.26 and recorded on the FBI's eGuardian system. Flight violations by UAS should be reported in accordance with AR 95–1.

c. Contact the FAA Regional Operations Center for safety concerns or serious UAS incidents.

d. Contact an FAA Law Enforcement Assistance Program special agent for investigation support, during business hours.

Appendix A

References

Section I

Required Publications

AD 2014–05
Policy and Implementation for Common Access Card Credentialing and Installations Access for Uncleared Contractors (Cited in the title page.)

AR 12–15
Joint Security Cooperation Education and Training (Cited in para 8–4*c*(8)(*b*).)

AR 25–1
Army Information Technology (Cited in para 9–1*e*.)

AR 95-1
Flight Regulations (Cited in para 11–1*f*.)

AR 95–2
Air Traffic Control, Airfield/Heliport and Airspace Operations (Cited in para 11–1*f*.)

AR 190–11
Physical Security of Arms, Ammunition, and Explosives (Cited in para 2–21*a*(1).)

AR 190–51
Security of Unclassified Army Property (Sensitive and Nonsensitive) (Cited in para 2–11*c*.)

AR 215–8
Army and Air Force Exchange Service Operations (Cited in para 4–3*f*(1).)

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives (Cited in para 8–4*c*(8)(*a*).)

AR 600–20
Army Command Policy (Cited in para 1–24.)

AR 608–10
Child Development Services (Cited in para 4–3*f*(6).)

CJCSI 3121.01B
Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces (Cited in para 11–3*a*(1).)

DA Pam 190–51
Risk Analysis for Army Property (Cited in para 1–26*o*.) (Available at http://www.apd.army.mil/.)

DOD 3305.13
DOD Security Accreditation and Certification (Cited in para 3–8*g*(3)(a).)

DOD 7000.14–R
Department of Defense Financial Management Regulations (Cited in para 4–3*f*(4).)

DODD 5105.55
Defense Commissary Agency (DeCA) (Cited in para 4–3*f*(2).) (Available at http://www.dtic.mil/whs/directives/.)

DODI 1000.25
DOD Personnel Identity Protection (PIP) Program (Cited in para 8–15*a*.)

DODI 3224.03
Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E) (Cited in the title page.)

DODI 3305.13
DOD Security Education, Training, and Certification, 13 February 2014 (Cited in para 3–8*a*.)

DODI 5200.08
Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)

DODI 8520.02
Public Key Infrastructure (PKI) and Public Key (PK) Enabling

DODM 4525.6–M
Department of Defense Postal Manual (Cited in para 4–3*f*(5).)

Executive Order 13434
National Security Professional Development, 22 May 2007 (Cited in para 1–10*p*.)

OPM Technical Manual (TM) 82 (TS-82)
Position Classification Standard for Security Administration Series GS-0080, December 1987 (Cited in para 3–1*c*(3).) https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/standards/0000/gs0080.pdf

PL 81–831, 64 Stat. 987
The Internal Security Act of 1950 (Cited in para 1–27*b*.)

PL 109–13, Division B, 119 Stat. 302
The Real ID Act of 2005 (Cited in para 8–2*c*(3)(*e*).)

Section II

Related Publications

AD 2011–08
Army Implementation of Homeland Security Presidential Directive 12

AFI 36–3026
Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel, dated August 2017

AR 1–1
Planning, Programming, Budgeting, and Execution System

AR 10–87
Army Commands, Army Service Component Commands, and Direct Reporting Units

AR 11–2
Managers' Internal Control Program

AR 25–2
Information Assurance

AR 25–22
The Army Privacy Program

AR 25–30
Army Publishing Program

AR 25–55
The Department of the Army Freedom of Information Act Program

AR 70–1
Army Acquisition Policy

AR 71–9
Warfighting Capabilities Determination

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

AR 190–17
Biological Select Agents and Toxins Security Program

AR 190–30
Military Police Investigations

AR 190–54
Security of Nuclear Reactors and Special Nuclear Materials

AR 190–56
The Army Civilian Police and Security Guard Program

AR 190–59
Chemical Agent Security Program

AR 380–5
Department of the Army Information Security Program

AR 380–13
Acquisition and Storage of Information Concerning Non–Affiliated Persons and Organizations

AR 380–40
Safeguarding and Controlling Communications Security Material (U)

AR 380–86
Classification of Former Chemical Warfare, Chemical and Biological Defense, And Nuclear, Biological Chemical Contamination Survivability Information

AR 381–10
U.S. Army Intelligence Activities

AR 381–12
Threat Awareness and Reporting Program

AR 420–1
Army Facilities Management

AR 525–2
The Army Protection Program

AR 525–13
Antiterrorism

AR 525–26
Infrastructure Risk Management (Army)

AR 530–1
Operations Security (OPSEC)

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

AR 600–8–22
Military Awards

AR 690–950
Career Program Management

AR 700–127
Integrated Product Support

ATP 3–39.12
Law Enforcement Investigations

ATP 5–19
Risk Management

DA General Order 2003–09
Establishment of the Office of the Provost Marshal General

DA Pamphlet 25–1–1
Army Information Technology Implementation Instructions

DeCA Directive 30–18 (C5)
Defense Commissary Agency Security Programs (Available at https://www.us.army.mil/suite/doc/13937758.)

DFAS–IN Manual 37–100
Financial Management

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

DODD 5200.43
Management of the Defense Security Enterprise, 1 October 2012

DODI 5210.65
Security Standards for Safeguarding Chemical Agents

DODI 5210.88
Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT)

DODI O-2000.16 Volume 1
DOD Antiterrorism (AT) Program Implementation: DOD AT Standards

DODI O-5210.63
DOD Procedures for Security of Nuclear Reactors and Special Nuclear Materials (SNM)

DODI 5525.15
Law Enforcement (LE) Standards and Training in the DOD

DODI 5525.19
DOD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information and TSDBs

DODM 5200.01 Volume 1
DOD Information Security Program: Overview, Classification and Declassification

EOP 16–1
Exchange operating procedures: AAFES Security (Available at https://www.us.army.mil/suite/doc/13783119.)

FAR 22.1803
Federal Acquisition Regulation section concerning exceptions to FAR 52.222-54 (Available at https://www.acquisition.gov.)

FAR 52.222–54
Federal Acquisition Regulation section for employment eligibility verification (Available at https://www.acquisition.gov.)

FED–STD–809B
Federal Standard: Neutralization and repair of GSA approved containers (Available at www.gsa.gov/cdnstatic/FED-STD-809BFinal.doc/.)

FIPS 201
Federal Information Processing Standards 201 (Available at http:// https://www.nist.gov/publications/personal-identity-verification-piv-federal-employees-and-contractors-federal/.)

HSPD–12
Homeland Security Presidential Directive 12 (Available at https://www.dhs.gov/homeland-security-presidential-directive-12.)

II PEG Program Guidance Memorandum, fiscal years 2017–2021, 28NOV14
VCSA Capability Portfolio Review Guidance

Installation Access, 07 NOV 14
Directed Actions: Countering Air and Missile Threats

Joint Pub 3–01
Countering Air and Missile Threats

MIL–STD–3007F
Department of Defense Standard Practice For Unified Facilities Criteria And Unified Facilities Guide Specifications (Available at https://www.wbdg.org/ffc/dod/federal-military-specifications-standards/mil-std-3007.)

SDDCTEA Pam 55–15
Traffic and Safety Engineering for Better Entry Control Facilities (Available at http://www.tea.army.mil/pubs/dod.asp.)

ST 19–LESM
DA Civilian Security Guard Field Training Manual, sub task 191-389-0045 (Available at https://atiam.train.army.mil/.)

STD 872–90–03
Standard Drawing: FE6 Chain-Link Security Fence Details for Non-Sensored Fence (Available at https://pdc.usace.army.mil/library/drawings/fence/.)
Signage

TSP 191–5323
Training Support Package (Available at https://atiam.train.army.mil/.)

UFC 3–120–01 with Change 3
Unified Facilities Criteria: Design: Sign Standards
(Available at https://pdc.usace.army.mil/library/sign.)

UFC 4–010–01 with Change 1
Unified Facilities Criteria: DoD Minimum Antiterrorism Standards for Buildings (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–010–02
Unified Facilities Criteria: DoD Minimum Antiterrorism Standoff Distances for Buildings (FOUO) (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–020–01
Unified Facilities Criteria: DoD Security Engineering Facilities Planning Manual (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–020–02FA
Unified Facilities Criteria: Security Engineering Concept Design (FOUO) (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–020–03FA
Unified Facilities Criteria: Security Engineering Final Design (FOUO) (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–020–03FA, with change 2
Unified Facilities Criteria: Electronic Security Systems: Security Engineering, with Change 2 (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–020–04FA / TM 5–853–4
Security Engineering: Electronic Security Systems

UFC 4–022–01
Unified Facilities Criteria: Security Engineering: Entry Control Facilities/Access Control Points (Available at http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/.)

UFC 4–022–03
Security Fences and Gates

UFGS 28 20 01.00 10
Unified facilities guide specification: Electronic Security System (Available at http://www.wbdg.org/ccb/browse_org.php?o=70/.)

18 USC 32
Destruction of aircraft or aircraft facilities

18 USC 795
Photographing and sketching defense installations (Available at http://uscode.house.gov/search/criteria.shtml/.)

18 USC 797
Publication and sale of photographs of defense installations (Available at http://uscode.house.gov/search/criteria.shtml/.)

18 USC 1382
Entering military, naval, or Coast Guard property (Available at http://uscode.house.gov/search/criteria.shtml/.)

18 USC 3041
Penalty for violation of security regulations and orders (Available at http://uscode.house.gov/search/criteria.shtml/.)

50 USC 797
War And National Defense (Available at http://uscode.house.gov/search/criteria.shtml/.)

50 USC Chapter 23
Internal Security Act of 1950 (Available at http://uscode.house.gov/search/criteria.shtml.)

Section III

Prescribed Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website

(https://armypubs.army.mil).

DA Form 2806
Physical Security Survey Report (Prescribed in para 2–14*d*.)

DA Form 2806–1
Physical Security Inspection Report (Prescribed in para 2–15*a*.)

DA Form 4261 and DA Form 4261–1
Physical Security Inspector Identification Card (Prescribed in para 2–15*a*.)

DA Form 7708
Personnel Reliability Screening & Evaluation Form (Prescribed in para 2–21*e*.)

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the APD website (www.armypubs.army.mil); DD forms are available on the Office of the Secretary of Defense (OSD) website http://www.esd.whs.mil/directives/form/; and standard forms (SF) are available on the U.S. General Services Administration (GSA) website (www.gsa.gov).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 1602
Civilian Identification Card

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 4930
Alarm/Intrusion Detection Record

DA Form 7278
Risk Level Worksheet

DD Form 2S (RES)
Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green) (Available through normal forms supply channels.)

DD Form 2S (RES RET)
United States Uniformed Services Identification Card (Reserve Retired) (Red) (Available through normal forms supply channels.)

DD Form 2S (RET)
United States Uniformed Services Identification Card (Retired) (Blue) (Available through normal forms supply channels.)

DD Form 369
Police Records Check

DD Form 1173
Uniform Services Identification and Privilege Card

DD Form 1173–1
Department of Defense Guard and Reserve Family Member Identification Card

DD Form 1173–1S (PRIV)
United States Uniformed Services Identification and Privilege Card (Reserve Dependent) (Red))

DD Form 1173S (PRIV)
United States Uniformed Services Identification and Privilege Card (Dependent) (Tan)

DD Form 1391
Military Construction Project Data

DD Form 2765
Department of Defense/Uniformed Services Identification and Privilege Card (Tan)

DD Form 2870
Authorization for Disclosure of Medical or Dental Information

SF Form 50
Notification of Personnel Action

SF Form 702
Security Container Check Sheet

Appendix B

Physical Security Plan Format for Army Commands, Army Service Component Commands, Direct Reporting Units, and the Army National Guard

B–1. Minimum requirements

The following format will be used to prepare a physical security plan appropriate for these command levels. Portions may not be applicable to a specific command, and other requirements may require inclusion of additional material. Care will be taken to mark pertinent portions for classification per applicable policy.

a. Standards for—

(1) Physical security inspections and reporting.
(2) Physical security surveys and reporting.
(3) Security engineering surveys to include team composition and reporting.
(4) Military construction reviews and reporting.
(5) Security criteria deviations and reporting.
(6) Installation access control.
(7) Facility access control.
(8) Visitor suitability.
(9) Bomb threats.
(10) Natural disaster.
(11) Active shooter.

b. Development of criminal and terrorist threat statements.

c. Management of physical security inspector credentials, physical security personnel and security guards.

d. Integration with—

(1) Other security programs such as information security and antiterrorism.
(2) Supporting programs such as intelligence and resource management.

e. The use of SMS(CM) for information synthesis to support informed decision making.

f. Execution of installation physical security plans and unit standard operating procedures.

g. Resource programming, planning, and execution.

h. Relationships with supporting and supported Military Departments and agencies.

i. Assessment processes to ensure compliance with requirements in paragraphs 1–24 and 1–25.

j. Minimum requirements and planning considerations of physical security measures during elevated FPCON.

B–2. Review and certification of currency

The plan will be reviewed annually and revise as required. If no revision is required, a brief statement affirming currency will be placed on the front page in this format: certified current by (principal official) (date).

Appendix C

Physical Security Plan Format for Installations, Stand-Alone Facilities, and Units

C–1. General

a. These organizations will use the following format for preparing physical security plan appropriate for the command level. These requirements pertain equally to USACE civil works and like projects. The plan may be a stand-alone document, but should instead be considered for inclusion as an annex to an overarching protection plan. Portions of the requirements below may not be applicable to a specific location or organization, and local requirements may require inclusion of additional material. Care will be taken to mark pertinent portions for classification per applicable policy.

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

c. The plan will be reviewed annually, and revised as needed to remain current. A brief statement affirming currency will be placed on the front page in this format: Certified current by (commander or director of designated representative) (date).

d. For installations, the plan will include the area access control plan per paragraph 8–14.

e. Physical security plans will include protection measures for sensitive compartmental information facilities (SCIFs) and open storage areas, where applicable. Physical security measures will be applied to the maximum extent possible in accordance with AR 380–5 and Director of Central Intelligence Directive (DCID) 6/9.

C–2. Classification and authority

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

C–3. Name and location of the installation, facility, or unit

Self-explanatory.

C–4. Mission of the installation, facility, or unit

Self-explanatory.

C–5. General

Cite a brief purpose of the plan. The physical security plan should identify key responsibilities, critical activities and resources being protected as well as integrate all physical security measures, forces, devices, and equipment into an effective and holistic security system. The plan should include physical security threat, criticality, vulnerability assessments, and risk -decisions that are updated regularly. The commander or director should approve the plan and recertify it.

C–6. Objectives

Cite the objectives of the plan, such as protection of chemical resources from sabotage or unauthorized access.

C–7. Analysis of external and internal threat

The PSO will work with the antiterrorism and intelligence offices to determine the current external and internal threats.

a. Analyze threats against resources.
b. Review and consider the postulated threat.
c. Consider the tactics and associated weapons, tools, and explosives that aggressors are likely to use.
d. Review the antiterrorism threat assessment.
e. Evaluate local threat information obtained from intelligence, counterintelligence, and law enforcement sources.
f. Consider recent security incidents that may bear on the overall threat analysis.
g. Review a single threat assessment for each installation and stand-alone facility.

C–8. Vulnerabilities

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

C–9. Priorities

Establish priorities for protecting all MEVA and other asset areas and required by the commander or director.

C–10. Controlled, limited, and exclusion areas
Delineate these areas.

C–11. Equipment and devices to detect or delay intrusion Identify equipment and devices to detect or delay intrusion
a. Perimeter boundary.
(1) Type.
(2) Construction.
b. Clear zones.
(1) Widths.
(2) Surface undulations and ditches.
(3) Obstacles such as poles, trees, boulders, structures that could not be relocated or removed.
(4) Culverts, utility tunnels, and other structures.
c. Gates.
(1) Type and construction of personnel and vehicle gates.
(2) Locations.
(3) Hours of operation.
(4) Locking means and procedures.
d. Signs.
(1) Types such as no trespassing, persons and vehicles subject to search, use of deadly force, and bilingual when appropriate.
(2) Location.
e. Identify types of inspection or maintenance.

C–12. Security lighting
Identify types of lighting used and current procedures.
a. Types such as area, glare projection, controlled, and portable.
b. Type of light source such as low or high-pressure sodium vapor, mercury vapor, or incandescent.
c. Use, control, and standards in foot candles or lumens.
(1) Perimeter.
(2) Gates.
(3) Interior areas and structures.
d. Inspections and maintenance.
e. Emergency actions for power failure.
f. Emergency generator type, location, fuel supply, operating instructions, testing procedures, and maintenance requirements.
g. Emergency backup lighting operating instructions.

C–13. Intrusion detection system
Identify the system to be used and required procedures.
a. Types.
b. Locations.
c. Procedures for operation, monitoring, and activation or deactivation.
d. Tests and anti-tamper procedures.
e. Inspections and maintenance.
f. Record logs.
g. Actions by security force when alarms occur or when the alarm system, or any part of the system, becomes inoperative.
h. Procedures to arm security force while alarm system in inoperative.
i. Duress system.
j. Warnings and alarms.
k. Emergency or back-up power sources.

C–14. Communications
Identify communication system procedures.

a. Types.
b. Locations.
c. Use.
d. Tests.
e. Inspections and maintenance.
f. Record logs.
g. Emergency or back-up power sources.

C–15. Locks and keys

Identify locks, keys, procedures.
a. Types.
b. Use.
c. Locations.
d. Maintenance and rotation.
e. Controls, logs, accountability.
f. Two-person control keys.
g. Identify key custodian.

C–16. Delay systems

Identify delay systems and procedures.
a. Types.
b. Locations.
c. Total delay time, provided in terms of aggressor time needed to gain access to protected resources.
d. Inspections and maintenance.

C–17. Security procedures during construction, renovation, or extensive maintenance

Provide instruction when applicable.

C–18. Measures to control access for personnel vehicles and material

Determine what personnel and vehicle movement restrictions are required for each critical area or structure (such as, limited area, exclusion area, material access area).
a. Personnel access controls.
b. Assigned personnel.
c. Visitors.
d. Maintenance personnel, both government and contractor.
e. Escort requirements.
f. Search and seizure procedures.
g. Duress system.
h. Nonoperational hours access procedures.
i. Emergency entrance procedures for fire, security, asset disposal, and medical personnel.

C–19. Personnel identification system

Personnel recognition and ID cards or badges for assigned personnel, visitors, and maintenance personnel.
a. ID cards.
b. Badges.
c. Entry control rosters.

C–20. Vehicle control

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

C–21. Material control

Identify requirements for controlling material.

a. Incoming.

(1) Requirements for admission, to include restrictions.

(2) Inspection, search, and seizure.

(3) Sealed packages and containers.

b. Outgoing.

(1) Documentation required.

(2) Inspection, search, and seizure.

(3) Classified documents or materials, controls, and procedures for incoming and outgoing, to include emergency destruction.

C–22. Security forces

Identify procedures for the security force.

a. Type—military, civilian and contractor, both U.S. and foreign.

b. Composition and organization.

c. Authority and jurisdiction.

d. Weapons, ammunition, and equipment.

e. Rules of engagement and use of deadly force to include fixed-wing aircraft and helicopter assault.

f. Training.

g. Actions to be taken under adverse weather and limited visibility conditions.

h. Posts.

(1) Locations.

(2) Areas of responsibility.

(3) Hours.

(4) Duties and functions including general patrol routes. Vary patrol routes and rotate stationary posts to combat boredom.

(5) Reporting procedures.

(6) Employment of military working dogs, if applicable.

i. Response force.

(1) Purpose and mission.

(2) Size, composition, and organization.

(3) Weapons, ammunition, and equipment.

(4) Location and call-out procedures.

(5) Reaction times.

(6) Protection of response vehicles from sabotage.

(7) Protected response means and alternate routes.

(8) Actions for multiple site intrusions.

(9) Training, including frequency of testing.

j. Augmentation force.

(1) Purpose and mission.

(2) Size, composition, and organization.

(3) Weapons, ammunition, and equipment.

(4) Location and call-out procedures.

(5) Response time.

(6) Tactical plan as an appendix.

(7) Other supporting security forces. Identify procedures.

C–23. Emergency actions of general nature

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

C–24. Coordination

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

a. Integration of the plan with installation supporting agencies.

b. Liaison and coordination with nearby military units, police, and intelligence agencies, and with civil agencies including civil police and FBI, as appropriate.

C–25. Appendixes

a. Criminal and terrorist threat statements.
b. Threat analysis.
c. Restricted areas list.
d. MEVA list.
e. Bomb threat plan including—
(1) Control of operations.
(2) Evacuation.
(3) Search.
(4) Finding the device.
(5) Disposal.
(6) Detonation and damage control.
(7) Control of publicity.
(8) After-action report.
f. Site closure plan.
g. Installation area access control plan.
h. Natural disaster plan per the National Incident Management System.
i. Civil disturbance plan based on local threats.
j. Resource plan for minimum essential physical security needs.
k. Communications plan.
l. Guard orders.
m. Rules of engagement and use of deadly force.
n. Site vulnerability assessment documentation.
o. Contingency defense plan.
p. Disaster control plan.
q. Demonstration control plan.
r. Memorandums of agreement or understanding with external first responders.
s. Alternate storage locations for AA&E and other sensitive items.
t. Minimum requirements and planning considerations of physical security measures during elevated FPCON.
u. Physical security plan format for barracks (see app D below).
v. Small unmanned aircraft systems response plan.
w. Active shooter plan.

Appendix D

Physical Security Plan Format for Barracks

D–1. General

a. The following format for a barracks physical security plan is provided for a minimum set of physical protective measures and security procedural measures. The term barracks can be used interchangeably with unaccompanied housing.

b. The format purposely lacks specific standards, because barracks environments differ across the Army; the most prominent difference being trainee barracks in comparison to permanent party barracks. Paragraph 1–23*c*, above, directs commanders and directors to develop a barracks physical security plan appropriate for the command, and to implement consistent use across the command.

c. The plan will be reviewed annually and revised, as needed, to remain current. A brief statement affirming currency will be placed on the front page in this format: Certified current by (commander or director) (date).

d. The plan is an inspectable item. The plan will be included in command operations inspections, installation inspections, and similar inspections and assessments.

e. The plan does not have to be a separate document. It can be an annex to a barracks management plan, a protection plan or similar encompassing plan, but will address each planning element below at a minimum.

D–2. Name and location of the barracks

Self-explanatory.

D–3. Purpose

The purpose of this plan is to provide a safe and secure environment for Soldiers' residences by preventing unauthorized access into, and activity in, the unaccompanied housing and gender-specific areas. The plan is intended to integrate personnel, processes, procedures, devices, and equipment into an effective security system.

D–4. Objective

The objective of this plan is to effect a safe and secure lodging environment for Soldiers by preventing unauthorized access into the quarters and into gender-specific areas. At no time will security measures be established that conflict with safety standards. The command will consult with engineers, safety personnel and housing to determine the best solution if a conflict exists.

D–5. Distribution

a. Soldiers will be provided a copy of the barracks physical security plan when in-processing.

b. A copy of the barracks physical security plan will be posted in a prominent location in each barracks.

D–6. Entry and circulation control

a. Describe how entry to the barracks and circulation in the facility is positively controlled.

b. Describe duties for personnel such as a charge-of-quarters.

c. Describe entry control measures.

d. Describe any electronic monitoring devices used, legal constraints, operating procedures, and privacy procedures.

e. Describe procedures for recording the presence of visitors.

f. Describe procedures for escorting visitors.

g. Describe procedures for escorting vendors.

h. List age restrictions for visitors without an accompanying parent or legal guardian.

i. List visiting hours.

j. List any off-limits or limited access areas.

k. Describe procedures for reporting violations.

l. List all other factors directed by the command.

D–7. Security of Soldiers in mixed-gender sleeping and personal hygiene facilities

Describe procedures for the physical security of Soldiers in--

a. Mixed-gender sleeping facilities.

b. Mixed-gender personal hygiene facilities.

c. Describe visitation procedures for all visitors.

D–8. Key control and accountability

a. Primary and alternate key custodians will be appointed on written orders.

b. Describe the duties of the primary and alternate key custodians.

c. Describe procedures for controlling and accounting for keys.

d. All types of keys will be address regardless if keys are for mechanical locks, code-activated locks, or electronic locks.

e. All keys will be controlled and accounted for in the same manner regardless if keys are mechanical (metal), access codes, or electronic lock access devices such as a card or fob.

f. Master keys are authorized. Describe how master keys, combinations to locks, and master lock cards or fobs are strictly controlled at the command level.

g. Describe procedures with emergency services personnel for emergency ingress.

h. Describe procedures for lock-outs and issuance of temporary keys.

i. Describe procedures for key turn-in.

D–9. Security of lodging rooms

a. Describe the standards and procedures for securing sleeping rooms.

b. What are the standards when the room is occupied?

c. What are the standards when the room is briefly unoccupied such as when the occupant momentarily steps away?

d. List the standards and procedures for the security of common use rooms.

e. Describe the lock-out resolution procedures.

D–10. Security of personal property

a. Describe the standards and procedures for securing personnel property in sleeping rooms and common-use rooms.

b. Describe the standards and procedures for securing personally owned bicycles and motor vehicles.

c. Describe requirements for marking, identifying, and recording high-value personal property items for ID in the event of loss or theft.

D–11. Prohibitions

a. List prohibited items. Note that privately owned weapons must be stored in a unit arms room, per AR 190–11.

b. List prohibited substances.

c. List prohibited behaviors.

d. Describe the administrative and legal processes if prohibited items and substances are discovered, or prohibited behaviors occur.

D–12. Emergency communications

Provide the emergency numbers for the supporting law enforcement, fire, and emergency medical responders.

D–13. Hazards plans

Coordinate and exercise these plans with the supporting garrison.

a. Bomb threat plan.

b. Natural disaster plan.

c. Active shooter plan.

d. Other plans directed by the command.

Appendix E

Instructions for Completing the DA Form 7708

E–1. Purpose

This regulation provides instruction to use the DA Form 7708 (Personnel Reliability Screening and Evaluation). The purpose of the form is to help review records to determine the suitability of a person to perform a certain duty assignment or gain access to certain materials. Examples of duty assignments include, but are not limited to physical security inspectors and DA civilian police and security guards. Examples of access to certain materials include, but are not limited to, unaccompanied access to arms, ammunition, explosives, and controlled medical substances. The DA Form 7708 is available for any Army policy proponent having duty assignments that warrant a greater degree of suitability determination than provided for civilian employees upon entry and Soldiers upon accession to the U.S. Army.

E–2. General

a. The DA Form 7708 is designed for electronic signatures, and is also intended to be transmitted and stored as an electronic document.

b. Emails that electronically transmit the DA Form 7708 will include an electronic signature to verify the sender, and also digital encryption to protect personally identifiable information.

c. The Social Security number is used to retrieve correct medical and law enforcement records.

d. A paper copy of the DA Form 7708 is authorized, if necessary. The form will be protected at all times while in use or being hand-carried to protect personally identifiable information.

e. The DA Form 7708 provides for eight personnel roles.

(1) The individual.
(2) The supervisor of the individual.
(3) The certifying official.
(4) The reviewing official.
(5) A supporting personnel official.
(6) A supporting security officer.
(7) A supporting competent medical authority.
(8) A supporting law enforcement authority.

f. The DA Form 7708 will be retained for record until such time the individual is no longer associated with the command.

E–3. Potentially disqualifying information

Information that is adverse to the individual may be revealed during checks of required records. Information that could potentially disqualify a person from a specific duty will vary. An example is medical information that could indicate a condition that poses a safety risk for one duty but is suitable for another duty. Records reviewing officials will consider the nature and elements of the duty for which the individual is being considered, and provide a professional assessment to the interviewer. The interviewer will consider all information as a whole and make an informed decision. The DA Form 7708 is marked For Official Use Only, due to the presence of personally identifiable information.

E–4. Completing the DA Form 7708

The DA Form 7708 will be used to screen and evaluate personnel reliability of physical security inspectors, per paragraph 2–21. The interview must complete part I prior to parts II through VI. Part VII will only be completed once parts II through VI are completed as required.

a. Part I: Immediate supervisor, commander, or director interview.

(1) Block 1. Enter the name of the interviewed individual.
(2) Block 2. Enter the organization.
(3) Block 3. Enter position title.
(4) Block 4. Enter the person's Social Security number.
(5) Block 5. The person will check one of the two blocks. The interview process will be terminated if the person indicates objection to the screening requirements. The certifying official will record the objection in blocks 49 and 50.
(6) Block 6. Check the applicable block for the pending duty. If the duty is not listed, use the "other" block and specify the duty.
(7) Block 7. The person will electronically sign the form in this block.

(8) Block 8. The date is automatically applied when Block 7 is signed.
(9) Block 9. Enter the name of the interviewer.
(10) Block 10. The interviewer will electronically sign the form in this block.
(11) Block 11. The date is automatically applied when Block 10 is signed.

b. Part II: Check of personnel records.

(1) Block 12. The reviewing personnel official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.
(2) Block 13. The reviewing personnel official will enter their name.
(3) Block 14. The reviewing personnel official will electronically sign the form in this block.
(4) Block 15. The date is automatically applied when Block 14 is signed.

c. Part III: Check of security records.

(1) Block 16. The reviewing security official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.
(2) Block 17. The reviewing security official will enter the date of the personnel security adjudication, the type of investigation, if the adjudication was favorable, or if the dossier requires a review.
(3) Block 18. The reviewing security official will enter the date and type of investigation, if a personnel security investigation or reinvestigation was requested.
(4) Block 19. The reviewing security official will indicate the level of security clearance.
(5) Block 20. The reviewing security official will enter their name in this block.
(6) Block 21. The reviewing security official will electronically sign the form in this block.
(7) Block 22. The date is automatically applied when Block 21 is signed.

d. Part IV: Check of medical records.

(1) Block 23. The reviewing medical official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.
(2) Block 24. The reviewing medical official will enter their name.
(3) Block 25. The reviewing medical official will electronically sign the form in this block.
(4) Block 26. The date is automatically applied when Block 25 is signed.

e. Part V: Check of law enforcement records.

(1) Block 27. The reviewing law enforcement official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.
(2) Block 28. The reviewing law enforcement official will enter their name.
(3) Block 29. The reviewing law enforcement official will electronically sign the form in this block.
(4) Block 30. The date is automatically applied when Block 29 is signed.

f. Part VI: Results of random or directed drug testing.

(1) Block 31. The reviewing drug-testing official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.
(2) Block 32. The reviewing drug-testing official will enter their name.
(3) Block 33. The reviewing drug-testing official will electronically sign the form in this block.
(4) Block 34. The date is automatically applied when Block 33 is signed.

g. Part VII: Immediate supervisor, commander, or director's evaluation or briefing.

(1) Block 35. After reviewing all provided records, the certifying official making the informed decision that the individual is suitable for the duty will check one of the two blocks. The certifying official will brief the individual on the duties and standards.
(2) Block 36. The person will read this statement.
(3) Block 37. The person will affirm an understanding of the duties and standards by electronically signing the form in this block.
(4) Block 38. The date is automatically applied when Block 37 is signed.
(5) Block 39. Enter the name of the certifying official (interviewer).
(6) Block 40. The certifying officer will electronically sign in this block.
(7) Block 41. The date is automatically applied when Block 40 is signed.

h. Part VIII: Continuing periodic evaluation.

(1) Block 42. The person will electronically sign the form in this block.
(2) Block 43. The certifying official will electronically sign the form in this block.
(3) Block 44. The certifying official will enter relevant comments in this block.

i. Part IX: Suspension or temporary disqualification. Block 45. The certifying official will enter the date in this block. The certifying official will annotate information about the suspension or disqualification in Part VIII.

j. Part X: Administrative termination. Block 46. The certifying official will enter the date in this block. The certifying official will annotate information about the administrative termination in Part VIII.

k. Part XI: Disqualification.

(1) Block 47. The certifying official will annotate the status of the individual at the time of the disqualification in this block.

(2) Block 48. The certifying official will annotate the reason for the disqualification in this block, and use Block 50 as the reason, if other than the listed reasons.

(3) Block 49. The certifying official will check this block to indicate the individual is disqualified.

(4) Block 50. The certifying official will annotate the rationale for disqualifying the individual in this block.

(5) Block 51. The certifying official will annotate the date the person was notified of the disqualification and the means of notification in this block.

(6) Block 52. Enter the name of the certifying official.

(7) Block 53. The certifying official will electronically sign the form in this block.

(8) Block 54. The date is automatically applied when Block 53 is signed.

(9) Block 55. Enter the name of the reviewing official.

(10) Block 56. The reviewing official electronically signs the form in this block.

(11) Block 57. The date is automatically applied when Block 56 is signed.

Appendix F

Manning Factors for Installation Access Control Points

F–1. General

This appendix provides standards to determine the number of guards necessary to operate installation access control points. General standards are provided, followed by standards specific to CONUS, Europe, and Korea.

a. Traffic studies. Traffic studies for Army installations will be conducted by Government personnel or by contractor personnel not affiliated with any contract security guard contract.

(1) Conduct traffic studies for at least 14 consecutive days.

(2) Count the volume per hour and per lane of automobiles, motorcycles, trucks, buses, bicycles, and pedestrians entering the installation.

(3) Count each bus as 10 vehicles for traffic volume.

(4) If available, use automated traffic recordings devices to continuously record traffic over a 24-hour period.

(5) Do not factor more than three guards per lane regardless of traffic volume.

b. Department of the Army civilian guards.

(1) The standard availability factor for a DA civilian is 1,740 hours per year, which equates to five personnel for a 24/7/365 duty position. Installations are provided one chief of guards and one supervisor per shift.

(2) The standard availability factor for a DA civilian will be used when using military police Soldiers or unit mission tasking Soldiers for the IACP mission.

c. Contract security guards.

(1) The standard factor for a contractor manpower equivalent (CME) is 2,087 hours per year in the United States and Korea, which equates to 4.2 CME per 24/7/365 duty position. The staffing factor in Europe is 1,817 hours due to U.S./Europe tariff agreements and equates to 4.82 contract security guards per 24/7/365 duty position.

(2) Limited, temporary increases in contract security guards to meet surge requirements in Europe and Korea are authorized if HQ IMCOM and OPMG are notified and the increase is within the scope of existing contract requirements.

d. Random vehicle inspection team.

(1) Each installation will have one random vehicle inspection team, consisting of five guards. The commander or director will determine the operational hours. The team will randomly inspect vehicles at IACPs other than the IACP designated for vehicle inspections, and will move between IACPs on an irregular basis to best avoid establishing a detectable pattern.

e. Overwatch position.

(1) Provide one overwatch position manned by one armed person to each IACP during hours of operation.

(2) Provide an additional overwatch position with one guard to cover the vehicle search area if a single overwatch position cannot cover both the IACP and the vehicle search area.

f. Vehicle inspection IACP.

(1) Designate at least one IACP for inspecting vehicles.

(2) Use no more than one guard per lane to inspect vehicles.

(3) Use no more than one over watch position for every three inspection lanes as long as the lanes are adjacent and within view and control of the over watch. A random vehicle inspection team will conduct the vehicle inspection used to inspect vehicles at other IACP.

g. OCONUS pedestrian gates. The following standards apply for pedestrian gates not equipped with an automated entry system.

(1) Use one guard for the lane and one guard for the overwatch position at isolated pedestrian gates.

(2) Use one guard for the lane, unless the hourly volume is less than 100 pedestrians at pedestrian gates that are collocated with vehicle gates. Pedestrians will use the vehicle gate if the volume is less than 100 per hour.

(3) Only man pedestrian gates during peak traffic periods (normal business hours on installations that do not contain essential life-support functions), unless conditions directly affecting Soldier safety or access to essential life-support functions warrant additional operating hours.

F–2. CONUS staffing factors

a. Use 1 guard per access lane, if the average per-lane volume is between 115 and 375.

b. Use 2 guards per access lane, if the average per-lane volume is between 375 and 675.

c. Use 3 guards per access lane, if the average per-lane volume exceeds 675.

d. Close half of the processing lanes, and use one guard per-lane for each open lane, if the average per lane volume is between 115 and 175.

e. Close two thirds of the processing lanes, and use one guard per lane for each open lane, if the average per-lane volume is less than 115.

f. Use one supervisor for each installation.

F–3. Europe staffing factors

a. IACPs with the installation access control system.

(1) Use 1 guard per access lane, if the traffic volume is 300 vehicles per hour or less.

(2) Use 2 guards per access lane, if the volume is greater than 300 vehicles per hour, but less than 400 vehicles, for as long as the traffic volume remains above 300.

(3) Use 3 guards per access lane, if the volume is greater than 400 vehicles per hour, for as long as the traffic volume remains about 400 vehicles.

b. IACPs without the installation access control system.

(1) Use 1 guard per access lane, if the traffic volume is 400 vehicles per hour or less.

(2) Use an additional guard per access lane, if the volume is greater than 400 vehicles per hour, but less than 500 vehicles, for as long as the traffic volume remains above 400 vehicles per hour.

(3) Use a third guard for the access lane, if the volume is more than 500 per hour, for as long as the volume remains above 500.

c. Vehicle and cargo inspection systems.

(1) Use three guards for each system.

(2) Operating hours for the system will be no more than 12 hours per day, 5 days per week.

d. Department of Defense Dependent Schools. One guard and one overwatch position will control vehicle and pedestrian access for each DOD Dependent School located on unsecured, off-post installations during school hours only.

e. Additional factors for contract security guards.

(1) One chief-of-the-guard for each installation.

(2) One lead supervisor for each U.S. Army garrison.

(3) One supervisor per shift for each U.S. Army garrison.

(4) One additional shift supervisor for each additional 15 contractor manpower equivalents.

F–4. Korea staffing factors

a. IACPs with the installation access control system.

(1) Use one guard per access lane if the traffic volume is 300 vehicles per hour or less.

(2) Use an additional guard per access lane, if the volume is between 300 and 600 vehicles, for as long as the traffic volume remains above 300 vehicles per hour.

(3) Use a third guard for the access lane, if the volume is more than 600 per hour, for as long as the volume remains above 600.

b. Additional factors for contract security guards.

(1) Use one chief-of-the-guard for each installation.

(2) Use one captain-of-the-guard for each installation with 60 or more contractor manpower equivalents.

(3) Use one supervisor per shift.

(4) Use one sergeant-of-the-guard for every 15 contractor manpower equivalents.

Appendix G

Maintenance and Testing of Installation Access Control Point Systems and Equipment

G–1. General

a. Commanders and directors will have written processes to routinely test, evaluate, and maintain IACP systems and equipment, in accordance with the manufacturers' recommendations and/or prescribed maintenance requirements.

b. Test results will be recorded in the Military Police Journal and made available for compliance reporting.

c. System and equipment deficiencies and nonmission-capable equipment or components will be specifically noted.

G–2. Active vehicle barrier systems

a. Exercise barriers in accordance with manufacturer's recommendations.

b. At a minimum, barriers will be tested on a weekly basis.

c. Barriers at IACPs must comply with the Surface Deployment and Distribution Command Transportation Engineering Agency (SDDCTEA) safety scheme current at the time of design and construction.

d. No requirement existed for use of an SDDCTEA safety scheme prior to December 2004. Barriers installed prior to this date should be considered as possible candidates for SDDCTEA-compliant safety scheme upgrades.

e. Barrier systems should be evaluated for conformance with either the SDDCTEA safety scheme current at the time of construction or a more current version of an SDDCTEA safety scheme, if upgrades have occurred.

f. The barrier safety scheme should not be modified after successful commissioning, unless the intent of such modifications is to bring the system into compliance with a more current version of an SDDCTEA safety scheme.

g. Commissioning of barrier systems will be performed on new or replacement systems prior to use.

h. Commissioning of existing barriers systems should be performed on a 5-year cycle.

i. Test barrier control systems on a monthly basis at a minimum.

j. A barrier control system test will include, as a minimum, barrier deployment from each Emergency Fast Operate control location.

k. A barrier control system test should be performed during climatological extremes to account for hot and/or cold extremes for the local climate.

l. If the barrier control system includes sensors for wrong-way or over-speed detection, the functionality of those systems will also be tested.

G–3. Other systems and equipment

a. Test CCTV systems and lighting on a weekly basis.

b. Test and exercise generators, uninterruptible power supply systems, and automatic transfer switches on a monthly basis.

c. Test generator systems under load with all, or nearly all, of the systems activated that are supported by the generator. The test under load should last 30 minutes, but no less than 15 minutes.

G–4. Representatives and responsibilities

a. Commanders and directors will ensure that all IACP improvements—except for USACE civil works and like projects' ACPs, which are not eligible for Direct Army funding—are either in compliance with the U.S. Army Standard for Access Control Points or an exception has been acquired through the process identified in AR 420–1.

b. IACP equipment that was provided by the OPMG is centrally sustained by the U.S. Army Engineering and Support Center, Huntsville, AL. Technical assistance is available by telephone at commercial 256-895-1348, DSN 760–1348, or by email at acpinquiries@usace.army.mil.

c. IACP projects that include military construction programming or other significant renovations (for example, changes to the footprint of the IACP) will include coordination with the Center of Standardization for Access Control Points, except for USACE civil works and like projects' ACPs, which are not eligible for Direct Army funding.

d. Commissioning of active vehicle barriers is performed by the USACE Protective Design Center or its designated representative. Additional information is available at 402–995–2359 or pdc.web@usace.army.mil.

Appendix H

Procedures for Intrusion Detection Monthly Operational Testing

The testing procedures in this appendix are general guidelines, to be adapted for local use based upon the type and configuration of the local system.

H–1. General

a. IDS users will test the system sensors on a monthly basis to ensure proper functioning, except for self-testing sensors.

b. Prior to conducting a monthly operational test, setup the test criteria by checking with the supporting IDS monitoring station to determine what types of sensors are in your protected area, the numbers of sensors, and which ones are self-testing. Ensure that you have the key to your duress switch (if necessary) and the cabinet key to ensure a full test of your IDS.

c. Basic test procedures—

(1) Contact the supporting IDS monitoring station and identify yourself, your location (for example, building name or number and room number), and the purpose of the test. Inform them that multiple alarms will be generated during the test.

(2) Before conducting the operational tests, it will be necessary to close all doors and openings equipped with balanced magnetic switches.

(3) It may also be necessary to mask ultrasonic motion sensors, passive infrared motion sensors, and passive ultrasonic sensors, so the tester can test each individual sensor, without generating unintentional alarms from the other sensors in the protected area.

(4) Close doors and drawers, or otherwise secure protected objects equipped with a capacitance proximity sensor. Allow one minute for the system to stabilize.

(5) Set the control unit mode switch to the test/reset position.

(6) Conduct the applicable operational tests below.

d. Test and inspection guide—

(1) This protected room passed.

(2) This protected room failed (contact maintainer for service).

(3) Tester name.

(4) Signature.

e. After all test of the system is complete annotate the results on a DA Form 4930. All sections of the form will be completed.

H–2. Operational test—balanced magnetic switch

The balanced magnetic switch (BMS) consists of a magnet assembly and a reed switch assembly enclosed in individual housings. The switch assembly is mounted to the moveable door or window. With the door or window closed, the magnet assembly acts on the switch assembly, holding it closed to complete a circuit. When the door or window is opened, the magnet moves away from the switch, releasing it. As the switch is released, it opens the circuit causing an alarm. The BMS is used to detect the opening and closing of doors, windows, skylights, and other similar moveable entryways.

a. Test procedure—

(1) Verify the control unit mode switch is in the test/reset position.

(2) With the door or window closed and locked, attempt to rattle or move the door or window. The alarm should not activate. If an audible signal initiates from the control unit, contact the maintainer for adjustment.

(3) Slowly open the door, gate, or window. An audible alarm should initiate immediately from the control unit when the latching edge of the opening has moved not more than 1-1/4 inches from the closed position.

(4) Close the door, gate, or window. After 10 seconds, the audible alarm will stop at the control unit.

(5) Repeat steps 2, 3, and 4 for each BMS installed in the protected area.

b. Test and inspection guide—

(1) Number of BMSs in this room.

(2) Number of BMSs in this room passed.

(3) Number of BMSs in this room failed (contact maintainer for service).

(4) Tester name.

(5) Signature.

H–3. Operational test—capacitance proximity sensor

The capacitance proximity sensor (CPS) establishes an electrical field around the protected objects, which must be metallic and insulated from the ground. A person approaching or touching the protected object disturbs the field causing a change in system capacitance, resulting in an alarm.

a. Test procedure—

(1) Verify the control unit mode switch is in the test/reset position.

(2) Slowly approach the protected area. An audible alarm should sound at the control unit immediately either just prior, or as you touch the object.

(3) After the audible signal initiates, move away from the object. The control unit audible signal will stop within 1 minute.

(4) Repeat steps 2 and 3 for each protected object.

b. Test and inspection guide—

(1) Number of objects protected by CPSs in this room.

(2) Number of objects protected by CPSs in this room passed.

(3) Number of objects protected by CPSs in this room failed (contact maintainer for service).

(4) Tester name.

(5) Signature.

H–4. Operational test—passive infrared motion sensor

All objects radiate infrared energy to some degree. The intensity of infrared energy emitted is dependent on the temperature, color, and surface texture of the object. Infrared energy is always present, and its intensity changes as the temperature of the object changes. The passive infrared motion detector is able to detect an intrusion, because the entry of a person into the detection field abruptly changes the background level of infrared energy being sensed by the detector. This triggers an alarm.

a. Test procedure—

(1) Verify the control unit mode switch is in the test/reset position.

(2) Unmask the passive infrared motion sensor (PIMS) being tested.

(3) Allow 1 minute for system to stabilize.

(4) Conduct a walk test by beginning at a point outside the protected area, or at the doorway to the protected area, moving along likely intruder paths, until audible alarm is activated at the control unit.

(5) Re-mask the sensor.

(6) Repeat steps 2, 3, 4, and 5 for each PIMS in the protected area.

b. Test and inspection guide—

(1) Number of PIMSs in this room.

(2) Number of PIMSs in this room passed.

(3) Number of PIMSs in this room failed (contact maintainer for service).

(4) Tester name.

(5) Signature.

H–5. Operational test—vibration signal detector

The vibration signal detector (VSD) is typically mounted directly on expanded metal cages, walls, and ceilings. Attempts to penetrate structural materials generate shock waves, which are transmitted through the structural material to the sensor. Different structural materials transmit different specific frequencies, so the range, detection characteristics, and effectiveness are variable from surface to surface.

a. Test procedure—

(1) Verify the control unit mode switch is in the test/reset position.

(2) Allow 1 minute for system to stabilize.

(3) Tap the protected surface with a solid object several times in succession. An audible signal should initiate from the control unit, when the required number of taps or pulses have been received within the proper time interval. The audible signal will stop at the control unit 10 seconds after the detector is out of alarm.

(4) Repeat steps 2 and 3 for each VSD in the protected area.

b. Test and inspection guide—

(1) Number of VSDs in this room.

(2) Number of VSDs in this room passed.

(3) Number of VSDs in this room failed (contact maintainer for service).

(4) Tester name.
(5) Signature.

H–6. Operational test—ultrasonic motion sensor

The ultrasonic motion sensor (UMS) detection operates on the Doppler frequency shift principle. A pattern of inaudible sound waves, generally in the 20-to-45kHz range are transmitted into the room and monitored by the system receiver(s). Motion within the room disturbs the sound wave pattern, altering its frequency. The change in frequency or Doppler shift is detected, resulting in an alarm.

a. Test procedure—

(1) Verify the control unit mode switch is in the test/reset position.
(2) Unmask the ultrasonic motion sensor to be tested.
(3) Allow 1 minute for system to stabilize.
(4) Conduct a walk test by beginning from a point outside the protected area or at the protected area boundary and moving along likely intruder paths until an audible signal is initiated at the control unit. The audible alarm will stop at the control unit 10 seconds after the sensor is out of alarm.
(5) Re-mask the sensor.
(6) Repeat steps 2, 3, 4, and 5 for each UMS installed in the protected area.

b. Test/inspection guide—

(1) Number of UMS in this room.
(2) Number of UMS in this room passed.
(3) Number of UMS in this room failed (contact maintainer for service).
(4) Tester name.
(5) Signature.

H–7. Operational test—alarm latching switch (duress)

The alarm latching switch (ALS) provides individuals with a means to covertly signal that they are under duress or threat. Is intended to be easily reached and covertly operated. For the protection of the user, the ALS must never annunciate in the area where they are located.

a. Test procedure—

(1) Activate the ALSs to be tested. Test should be accomplished with the control unit in the access position.
(2) Verify that an alarm was received from the zone under test. If no alarm was received, contact the maintainer for service.
(3) Reset the sensor by removing the switch cover and depressing the red reset switch. Install the cover. NOTE: Different styles of duress switches require a different type of reset. If the device requires a key, ensure that you have the key to reset. Momentary duress switches can only be reset at the IDS monitoring station, and another switch is reset by removing the switch cover and depressing the red reset switch then replacing the cover.
(4) Reset the control unit by placing the control unit mode switch to the secure position momentarily and then setting the mode switch to the access position.
(5) Verify that the zone status is access.
(6) Repeat steps 1 through 5 for each ALS to be tested.

b. Test and inspection guide—

(1) Number of ALSs in this room.
(2) Number of ALSs in this room passed.
(3) Number of ALSs in this room failed (contact maintainer for service).
(4) Tester name.
(5) Signature.

Appendix I

Installation Access Control Data Reporting – Spreadsheet Instructions

I–1. General

Commanders and civilian directors of installations and SAFs will submit NCIC-III and continuous vetting denial results pertaining to Installation Access Control, quarterly, through the portal at https://army.deps.mil/army/sites/pmg/team/ps/pages/installationdata.aspx, using the format specified in this appendix. Submitted data must be approved by the DES, deputy DES, PM, or other individual authorized by the commander or director.

I–2. Identifying information

Enter the installation or facility name, month or months included in the reporting period, year being reported, and the total number of visitors or NCIC-III checks conducted during the period reported.

I–3. National Crime Information Center-III results summary

Enter the total number of NCIC-III hits, denials, active warrants, and KST notifications in each category listed. For each active warrant, indicate the type (specific crime, reasons) and the action taken. Enter the total number of waivers submitted and approved in each category listed.

I–4. Continuous vetting results

Enter the total number of active warrants, confiscated ID cards, barments, and TSDB hits in each category listed, identified by continuous vetting.

I–5. Felony crimes

Enter the total number of felony convictions or plea within the last 10 years by each crime listed identified by NCIC-III checks. For individuals identified as having a history of multiple felonies record each one appropriately. For felony crimes not specifically listed record as OTHER.

I–6. Any conviction for the following crimes

Record felony convictions for the crimes listed that occurred longer than 10 years ago, as identified by NCIC-III checks and misdemeanor convictions, for the identified crimes that occurred at any time.

I–7. Other disqualifiers

List the total number of individuals identified as having been convicted as identified by NCIC-III checks for the other disqualifiers listed.

I–8. Active warrant details

Record the details for each active warrant identified by NCIC-III check or continuous vetting.

I–9. Unit mission tasking

Record the average number of unit mission tasking personnel conducting installation access control on a daily basis during the reporting period.

I–10. Completing the spreadsheet

Definitions and instructions are explained in table I–1, below:

Table I-1
Spreadsheet definitions

Part I - Identifying information:	1. Installation: Enter installation name.
	2. Month: Enter the month (or months) being reported.
	3. Year: Enter the current year.
	4. All visitors: Enter the total of NCIC-III checks conducted during the reporting period.

Table I-1
Spreadsheet definitions—Continued

Part II - Summary: Indicate the results from NCIC-III checks and continuous vetting (if available at installation) by personnel category as defined below:	5. CTR (contractor): Non CAC-holding contractors including but not limited to cleaning personnel, vendors (delivery personnel), and repair people. 6. U.S. visitors: Member of the general public (other than contractors or Family) who are U.S. citizens. 7. Foreign visitors: Member of the general public (other than contractors or Family) who are citizens of a foreign country. 8. Family: Family member (NOT dependent ID card holders) of a uniformed Service member or DOD Civilian. 9. Hits: Enter the total number of NCIC-III responses returned with any response, other than No Record Found, by each personnel category. A response requires further examination of record to determine adjudication. 10. Active warrants: Enter the total number of active warrants identified by NCIC-III checks by personnel category. Provide complete details as stated in Part VI. 11. Denials: Enter the total number of installation access denials by personnel category. 12. KST hit: Enter the total number of known or appropriated suspected terrorist hits by personnel category. 13. Waivers submitted: Enter the total number of waivers submitted by personnel category. 14. Waivers approved: Enter the total number of waivers approved by personnel category. 15. DOD: Uniformed or civilian DOD personnel. 16. CTR (contractor): CAC-holding contractors. 17. U.S. visitors: Members of the general public (other than contractors or Family) who are U.S. citizens. 18. Foreign visitors: Member of the general public (other than contractors or Family) who are citizens of a foreign country. 19. Family: Family member (including dependent ID card holders) of a uniformed Service member or DOD Civilian. 20. Confiscated ID cards: Enter the total number of ID cards confiscated from continuous vetting results by personnel category. 21. Barments: Enter the total number of barments by personnel category. 22. TSDB hits: Enter the total number of TSDB hits by personnel category.
Part III - Felony conviction within the last 10 years:	23. Crime: Enter the total number of felony crimes committed within the last 10 years, identified by NCIC-III checks, by each crime listed. If an individual has multiple felonies, record each one appropriately.
Part IV - Conviction for the following crimes:	24. Crime: Record felony convictions for the crimes listed that occurred more than 10 years ago and misdemeanor convictions for the identified crimes that occurred at any time, as identified by NCIC-III checks. Do not include felony convictions recorded in Part III.
Part V - Other disqualifiers:	25. Engaged in acts or activities to overthrow the U.S. Government by force: Enter the total number of individuals identified by NCIC-III results as having engaged in acts or activities to overthrow the U.S. Government by force. 26. Registered sex offender: Enter the total number of sex offenders identified by NCIC-III results.
Part VI - Active warrant details:	27. Active warrant type: Specify the charge or reason for the warrant (murder, failure to appear, fugitive from justice, and so forth). 28. Action taken: Indicate what action was taken (arrested and transferred to local police department, issuing jurisdiction declined extradition – individual released and denied installation access, and so forth). 29. Source: Indicate if the active warrant was identified by NCIC-III check or continuous vetting (AIE). 30. Personnel type: Indicate if the individual with the active warrant was a contractor, visitor, DOD, as defined above.

Appendix J

Internal Control Evaluation Checklist

J–1. Function

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

J–2. Purpose

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

J–3. Instructions

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

J–4. Test questions

a. Do commanders and directors of ACOMs, ASCCs, DRUs, and the ARNG—

(1) Maintain a physical security program, to plan and coordinate physical security matters and to ensure practical, effective, and common sense measures are used?

(2) Does the command have a current physical security plan?

(3) Does the plan's implementation of Army policies provide sufficient clarity and detail for personnel to understand roles, responsibilities, and required actions?

(4) Appoint a command PSO on orders?

(5) Review, approve, and maintain copies of subordinate organization PS plans?

(6) Identify and forward resource requirements to DAPM–MPO–PS?

(7) Coordinate new PSE performance requirements with TRADOC?

(8) Use SMS(CM) for inspections, surveys, cost analysis, trend analysis and loss expectancy analysis?

(9) Ensure physical security, antiterrorism and engineering personnel coordinate design criteria for new construction projects?

(10) Ensure physical security personnel track construction projects at every milestone of the planning, design, and construction process, and also document the tracking process?

(11) Ensure forces deploying to overseas areas designate personnel to carry out physical security responsibilities to safeguard personnel, facilities, equipment, operations, and materiel against hostile intelligence, terrorists, and criminal, dissident, or other disruptive activity?

(12) Ensure deployed inspectors are provided credentials for the duration of their deployment tour, and to ensure issued credentials are recovered and accounted for after deployment?

(13) Record, track, and resolve deficiencies found during inspections and surveys?

(14) Ensure the contract structure that supports PSE sustainment promotes competition?

(15) Issue, control, account for, and properly destroy inspector credentials?

(16) Ensure inspections and surveys are conducted per this regulation and against the minimum standards of asset specific regulations?

(17) Appoint a voting member or nonvoting adviser and APSEAG?

(18) Publish and maintain a barracks physical security plan, per appendix D of this regulation, to include additional requirements directed by the command?

(19) Is the barracks physical security plan—

(a) Reviewed at least annually?

(b) Displaying a statement of currency on the front page?

(c) Containing the required information?

(d) Appointing a command credential custodian on orders?

(e) Appointing a command key control custodian (KCC) on orders?

(20) Identifying requirements through the planning, programming, budgeting, and execution system?

(21) Validating requirements by the chain of command, and recording them in Schedule 75 of the automated schedule and reporting system?

b. Do commanders and directors of posts, camps, stations, and installations (including Army-managed Armed Forces Reserve Centers, Army Reserve Centers, Army National Guard Armories, and other Army facilities subject to DA jurisdiction or administration, or in DA custody) by formal process—

(1) Publish and maintain a physical security plan?

(2) Ensure it is certified as current?

(3) Appoint a command PSO on orders?

(4) Use SMS(CM)?

(5) Conduct inspections and surveys per this regulation and against the minimum standards of asset- specific regulations?

(6) Designate restricted areas in writing?

(7) Post warning signs at restricted areas?

(8) Designate MEVAs in writing?

(9) Ensure engineers and physical security personnel coordinate in the construction process?

(10) Issue written appointment orders establishing a PSC, chaired by the senior installation law enforcement officer?

(11) Review threat information for organizational military activities on and off the installation?

(12) Include physical security as an annex to all applicable orders and plans?

(13) Ensure supporting military intelligence elements are given all the information relating to the organization and its activities needed to support the force protection mission?

(14) Provide physical security support when requested by tenant activities?

(15) Appoint a command KCC on orders?

(16) Is the barracks physical security plan—

(a) Reviewed at least annually?

(b) Displaying a statement of currency on the front page?

(c) Containing the required information?

J–5. Supersession

This is the initial internal control evaluation for AR 190–13, dated 27 June 2019.

J–6. Comments

Help make this a better tool for evaluating management controls. Submit comments to Headquarters, Department of the Army (DAPM–MPO–PS), 2800 Army Pentagon, Washington, DC 20310–2800

Glossary

Section I

Abbreviations

AA&E
arms, ammunition and explosives

AAFES
Army and Air Force Exchange Service

ACOM
Army command

ACP
access control points

ACS
access control systems

ACSIM
Assistant Chief of Staff for Installation Management

ACTEDS
Army Civilian Training Education Development System

AIE
automated installation entry

ALS
alarm latching switch

APMS
Army Portfolio Management System

APSEAG
Army Physical Security Equipment Action Group

AR
Army regulation

ARNG
Army National Guard

ASA (ALT)
Assistant Secretary of the Army for Acquisitions, Logistics and Technology

ASA (CW)
Assistant Secretary of the Army for Civil Works

ASA (IE&E)
Assistant Secretary of the Army for Installations, Energy and Environment

ASA (M&RA)
Assistant Secretary of the Army for Manpower and Reserve Affairs

ASCC
Army service component command

ASI
additional skill identifier

ASI H3
additional skill identifier, physical security inspector

AVB
active vehicle barrier

BMS
balanced magnetic switch

CAC
common access card

CAR
Chief, Army Reserve

CCTV
closed circuit television

CDSE
Center for Development of Security Excellence

CE
civilian equivalent

CG
commanding general

CIO/G–6
Chief Information Officer/G–6

CJIS
Criminal Justice Information Service

CME
contractor manpower equivalent

COE
Chief of Engineers

CONUS
continental United States

COS
Center of Standardization

COTS
commercial off-the-shelf

CP
Program

CPM
Career Program manager

CUI
controlled unclassified information

DA
Department of the Army

DACP
Department of the Army civilian police

DAGO
Department of the Army general order

DASG
DA security guard

DBIDS
Defense Biometric Identification System

DCS, G–1
Deputy Chief of Staff, G–1

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3/5/7
Deputy Chief of Staff, G–3/5/7

DCS, G–4
Deputy Chief of Staff, G–4

DD
Defense directive

DeCA
Defense Commissary Agency

DEERS
Defense Enrollment Eligibility Reporting System

DES
director of emergency services

DMDC
Defense Manpower Data Center

DOD
Department of Defense

DOD RMF
Department of Defense Risk Management Framework

DODD
Department of Defense directive

DODI
Department of Defense instruction

DODM
Department of Defense memorandum

DRU
direct reporting unit

DSS
Defense Security Services

EC
Engineering circular

ESC
Electronic Security Center

ESS
electronic security system

FAA
Federal Aviation Agency

FAR
Federal Acquisition Regulation

FBI
Federal Bureau of Investigation

FCR
functional chief representative

FIPS
Federal Information Processing Standards

FOAs
field operating activities

FPCON
Force Protection Condition System

GIG
global information grid

GSA
General Services Administration

HQDA
Headquarters, Department of the Army

HRP
high risk personnel

IACP
installation access control point

IACS
installation access control system

ICIDS
Integrated Commercial Intrusion Detection System

ID
identification card

IDS
intrusion detection system

IDSWG
Intrusion Detection Systems Working Group

III
Interstate Identification Index

IMCOM
U.S. Army Installation Management Command

IMESA
Identity Matching Engine for Security and Analysis

ISOC
Industrial Security Oversight Certification

IT
information technology

KCC
key control custodian

KST
known or appropriately suspected terrorist

LE
law enforcement

MCAR
military construction, Army Reserve

MDEP
management decision package

MEVA
mission essential vulnerable area

MILCON
military construction

MP
military police

MWR
Morale, Welfare and Recreation

NCIC
National Crime Information Center

Nlets
National Law Enforcement Telecommunication Systems

O–4
major

O–5
lieutenant colonel

OACSIM
Office of the Assistant Chief of Staff for Installation Management

OCONUS
outside the continental United States

OPM
Office of Personnel Management

OPMG
Office of the Provost Marshal General

PDC
Protective Design Center

PdM–FPS
Product Manager, Force Protection Systems

PDU
professional development unit

PIMS
passive infrared motion sensor

PIN
personal identification number

PIV
personal identity verification

PM
provost marshal

PMG
Provost Marshal General

PSC
Physical Security Council

PSE
physical security equipment

PSEWG
Physical Security Equipment Working Group

PSI
physical security inspector

PSO
physical security officer

QPSM
the management decision package for physical security matters

QWI
A combination of keyboard keys used for the National Law Enforcement Telecommunications System

RAM
random antiterrorism measures

RC
Reserve Component

RDECOM
U.S. Army Research, Development and Engineering Command

RMF
Risk Management Framework

SAFs
standalone facilities

SC
senior commanders

SDDCTEA
Surface Deployment and Distribution Command Traffic Engineering Agency

SFPC
Security Fundamentals Professional Certification

SFRA
special flight rules area

SME
subject matter expert

SMS(CM)
Security Management System (CounterMeasures)

SO
security officer

SOS
Survivor Outreach Services

SPIPC
Security Program Integration Professional Certification

SRUF
standing rules for the use of force

SSI
special security instructions

STEPP
Security Training, Education and Professionalization Portal

sUAS
small unmanned aircraft systems

TRADOC
U.S. Army Training and Doctrine Command

TSC
Terrorist Screening Center

U.S.
United States

UA
unmanned aircraft

UAS
unmanned aircraft systems

UCMJ
Uniform Code of Military Justice

UFC
unified facilities criteria

UFGS
unified facilities guide specification

UMS
ultrasonic motion sensor

UMT
unit mission tasking

USACE
U.S. Army Corps of Engineers

USAR
U.S. Army Reserve

USARC
U.S. Army Reserve Command

USC
United States Code

USG
United States Government

VCC
Visitor Control Center

VHIC
veteran's health identification card

Section II

Terms

access (relating to a restricted area)
Personnel movement within a restricted area that allows the chance for visual observation of, or physical proximity to, either classified or protected materiel. It is also the ability and opportunity to obtain detailed knowledge of a controlled cryptographic item through uncontrolled physical possession. External viewing or escorted proximity to a controlled cryptographic item does not constitute access.

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

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

Army access control points standards
Provides standards to meet access control functions on Regular Army installations and RC prime installations (https://www.us.army.mil/suite/page/441649).

Army standard for access control points
Provides standards for Army access control points (ACPs) (https://www.us.army.mil/suite/doc/8912967).
Army Standard (Part I) and System Specifications (Part II) for Automated Installation Entry
Provides standards for Army AIE (https://www.us.army.mil/suite/doc/9647105).

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

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

common access card
The CAC is an ID card displaying the cardholder's name, photo, and organization. The CAC is the DOD implementation of Homeland Security Presidential Directive 12 that requires Federal executive departments and agencies to implement a government-wide standard for secure and reliable forms of ID for employees and contractors, for access to Federal facilities and information systems.

compensatory measure
An action or condition that mitigates or compensates for vulnerabilities created by the inability to achieve a minimum physical security standard. Examples of compensatory measures include, but are not limited to, such physical security measures as additional security forces, security procedures, and physical security equipment or devices such as locks, intrusion detection systems, lighting, barricades, alarms, and anti-intrusion devices.

concern
An existing condition that is exploitable and can directly or indirectly lead to the injury or death of DOD personnel or damage or compromise of DOD resources or resources.

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

contractor verification system
A web-based system established by the Defense Manpower Data Center to automate the application, validation, and approval process for issuing a CAC to eligible DoD contractors.

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

crime prevention
The anticipation, recognition, and appraisal of a crime risk, and initiation of some action to remove or reduce the risk. Crime prevention is a direct crime control method that applies to before-the-fact efforts to reduce criminal opportunity, protect potential human victims, and prevent property loss.

dedicated guard force
A force that is specifically dedicated to guarding the identified facility, capable of performing required measures at a higher FPCON. Individually armed Soldiers (such as armed recruiters or Army reservists), or local law enforcement officers executing their daily duties, are not a dedicated guard force.

deviation
Inability to achieve compliance with a minimum physical security standard for facilities, equipment, and procedures either combined or individually.

electronic security system
The collection of electronic systems hardware, components, software, and interconnecting communication media that together provide the functions of intrusion detection, alarm assessment, surveillance, and access control.

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

exception
An approved waiver, 3-year permanent, or permanent continuation of a deviation from this regulation in which the requirements are not being met and the approving authority determines it is inappropriate to meet the requirements. Compensatory security measures are required to provide adequate security for the deviation.

exclusion area
A type of restricted area that contains a security interest or other material of such vital importance that proximity resulting from entry into the area constitutes access to such security interest or material.
Therefore entry into an exclusion area is more restrictive than into a limited area. An exclusion area is usually located within a limited area.

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

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

installation
See the definition provided in AR 420–1.

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

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

intrusion detection system
The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system and reporting directly to an alarm-monitoring station.

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

limited exception
Approval of a long-term deviation from minimum physical security standards, due to a security condition that can be corrected within 3 years.

line supervision
Line supervision is defined as the various techniques designed to detect or inhibit manipulation of communication networks, detect and annunciate communication interruptions, or compromised communications between field devices and the central station.

locks
A mechanical or electro-mechanical fastening device intended to control access. Locks are devices designed to delay intruders, rather than means to fully stop unauthorized entry since any lock can eventually be defeated by expert manipulation or by force. Refer questions to the DOD Lock Program technical manager, Naval Facilities Engineering Service Center, Code C66, 560 Center Drive, Port Hueneme, CA 93043–4328. Phone: DSN 551–1567 or –1212. (https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).

management decision package
An MDEP is a funding source that describes a particular organization, program, or function, and records the resources associated with the intended output. An individual MDEP applies uniquely to management areas for the Regular Army, Guard, and Reserve. During programming for resource requirements, MDEPs provide useful visibility to assist Army managers, decision makers, and leaders to assess program worth, confirm compliance, and rank resource claimants. During budgeting, MDEPs help convey approved programs and priorities into budget estimates and assist in recording program changes caused by budget decisions and approved funding. During execution, MDEPs help track program and financial performance, and help determine future requirements. See DFAS-IN 37-100 for more information.

mission essential vulnerable areas
Mission essential vulnerable areas (MEVAs) are facilities or activities on or off the installation that, by virtue of their function, are evaluated by the commander as vital to meet the mission of an installation, State National Guard, or major U.S. Army Reserve command. The intent of the MEVA designation is to help the commander or director focus attention and resources. This includes areas nonessential to the operational mission of the installation or facility, but which, by the nature of the activity, are considered vulnerable to theft, trespass, damage, terrorism, or other criminal activity.

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

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

permanent exception
Approval of a permanent deviation from minimum physical security standards that cannot be corrected in 3 years or more.

personal identity verification
A process to verify a person's identity.

physical protective measures
Physical security measures are physical systems, devices, personnel, animals, and procedures employed to protect security interests from possible threats and include, but are not limited to, security guards; military working dogs; lights and physical barriers; explosives and bomb detection equipment; protective vests and similar equipment; badging systems; electronic entry control systems and access control devices; security containers; locking devices; electronic intrusion detection systems; standardized command, control, and display subsystems; radio frequency data links used for physical security; security lighting; delay devices; artificial intelligence (robotics); and assessment and/or surveillance systems to include

closed-circuit television. Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans.

physical security
That part of the Army security system using risk analysis as a decision basis, physical security is a combination of physical protective measures and security procedural measures employed to safeguard personnel, property, operations, equipment, facilities, materiel, and information against loss, misuse, theft, damage, or destruction by disaffected persons (insiders), vandals, activists, extremist protesters, criminals (individuals and organized groups), terrorists (domestic, state-sponsored, and transnational), saboteurs and spies.

physical security deficiency
Not meeting a minimum physical protective measure, or security procedural measure, specified in policy, which can create a protection vulnerability

physical security equipment
A generic term for any item, device, or system that is used primarily to protect Government property, including nuclear, chemical, and other munitions, personnel, and installations, and to safeguard national security information and material, including the destruction of such information and material both by routine means and by emergency destruct measures.
a. Interior physical security equipment. Physical security equipment used, internal to a structure, to make that structure a secure area. Within DOD, the SECARMY is the proponent for those functions associated with development of interior physical security systems, which include—but are not limited to—interior physical security equipment, tactical security equipment, barriers, lighting systems, personnel alerting systems, command and control systems, and interior and exterior robotics.
b. Exterior physical security equipment. Physical security equipment used, external to a structure, to make the structure a secure area. Within DOD, the Department of the Air Force is the proponent for developing external physical security systems; however, the Army will develop lights, barriers, and robotics.

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

physical security plan
A comprehensive written plan that describes the critical components of a command, unit, or installation physical security program to protect personnel, activities, and critical resources from loss, damage, or destruction by espionage, sabotage, terrorism, criminal, and other threats. The physical security plan should identify key responsibilities, the critical activities and resources being protected as well as integrate all physical security measures, forces, devices, and equipment into an effective and holistic security system. The plan should include physical security threat, criticality, and vulnerability assessments, as well as risk management decisions that are updated regularly. See appendixes C and D. The commander or director should approve the plan and recertify it, at least annually but optimally more often.

physical security program
The interrelationship of various components that complement each other to produce a comprehensive approach to security matters. These components include, as a minimum, the physical security plan; physical security inspections and surveys; participation in combating terrorism committees and fusion cells; and a continuing assessment of the installation's physical security posture.

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

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

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

risk
The degree or likelihood of losing a resource. Factors that determine risk are the value of the resource to its user in terms of mission criticality, replaceability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the resource to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the resource.

risk analysis
Method of examining various risk factors to determine the risk value of likelihood of losing a resource. This analysis will be used to decide the level of security warranted for protecting resources.

risk factors
Elements that make up the total degree of resource loss liability. Factors to be considered in a risk analysis include the importance of the resource to mission accomplishment; the cost, volume, criticality, and vulnerabilities of the resources; and the severity of threats to the resources.

security (force)
An armed, trained, dedicated guard force. That dedicated guard force may be DOD-controlled (for example, military police, security forces, DOD police) or non-DOD controlled (Department of Homeland Security Federal Protective Service, contracted guard force), but must be armed with lethal force capability in order to be classified in a group with security.

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

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

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

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

tenant activity
A unit or activity of an agency, Military Department, or commercial entity that occupies facilities on an installation and that receives supplies or other support services from that installation.

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

threat statement
The product of the threat analysis for a particular unit, installation, or activity.

transportation worker identification credential
A common ID credential for all personnel requiring unescorted access to secure areas of regulated facilities and vessels. The U.S. Transportation Security Administration manages the credential. Personnel meeting eligibility requirements will be issued a tamper-resistant credential containing the person's biometric (fingerprint template), to allow for a positive link between the card and the person.

Trusted traveler
A person enrolled in the Trusted Traveler Program.

Trusted Traveler Program
A process by which a uniformed Service member or Government employee with a valid CAC, driver's license, and clear NCIC check, presents their ID token for automated authentication at an IACP, and simultaneously vouches for other vehicle occupants.

U.S. person
Any person that is a U.S. citizen or national of the United States, and any person that is a lawful permanent resident.

Unified Facilities Criteria (UFC) 4–010–01
Provides minimum construction standards for all DOD buildings, to mitigate mass casualties from the terrorist threat.

Unified Facilities Criteria (UFC) 4–010–02
Provides minimum standoff distances for all DOD buildings, to mitigate mass casualties from the terrorist threat.

Unified Facilities Criteria (UFC) 4–020–01
Supports the planning of DOD facilities that include requirements for security and antiterrorism.

Unified Facilities Criteria (UFC) 4–022–01
Provides construction standards for entry control facilities and access control points.

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

vulnerability
A situation or circumstance, which left unchanged, may result in the degradation of physical security, injury or death of DOD personnel, or damage or compromise of DOD resources.

waiver
Approval of a short-term deviation from minimum physical security standards due to a security condition that cannot be corrected within 90 days, but can be corrected within 1 year. Compensatory measures are required during the waiver period.

Section III

Special Abbreviations and Terms

This section contains no entries.