Army Regulation 190–51

Military Police

Security of Unclassified Army Resources (Sensitive and Nonsensitive)

Headquarters
Department of the Army
Washington, DC
27 June 2019

UNCLASSIFIED

SUMMARY of CHANGE

AR 190–51
Security of Unclassified Army Resources (Sensitive and Nonsensitive)

This major revision, dated 27 June 2019—

- Adds responsibilities for the Provost Marshal General and the Commanding General, U.S. Army Corps of Engineers (paras 1–4*a* and 1–4*d*, respectively).

- Realigns the responsibility to conduct physical security inspections from facility commanders to commanders and directors of Army commands, Army service component commands, direct reporting units, the Chief, National Guard Bureau, and commanders and directors of U.S. Army Corps of Engineers Divisions, districts, centers, laboratories, and field operating activities (para 1–4*b*).

- Provides standards for other Department of Defense component aircraft transiting Army installations (para 3–9*l*).

- Provides standards for high-value optical devices and launched electrode stun devices (para 3–12).

- Revises the security requirements for petroleum, oils, and lubricants at bulk storage facilities and ties the assets to the Defense Critical Infrastructure Program (para 3–19).

- Provides standards for on-post public and privatized utilities (para 3–24).

- Provides standards for air items and airdrop systems, and personnel and cargo parachute systems including associated ancillary items (para 3–25).

- Provides standards for critical communication facilities (para 3–26).

- Provides additional standards for medical resources, to include infectious agents and toxins (chap 4).

- Revises policy for the security of Army museums (chap 5).

- Provides standards for U.S. Army Corps of Engineers civil works and like project resources (chap 6).

- Revises structural standards for secure storage structures and vaults (app B).

- Revises policy for locks and keys (app D).

- Provides information for the high-value asset security cage (app E).

- Provides for control of bolt cutters (app F).

- Incorporates aircraft, petroleum, and critical communications facilities security previously prescribed in AR 190–16 (hereby superseded) (throughout).

Headquarters
Department of the Army
Washington, DC
27 June 2019

*Army Regulation 190–51

Effective 27 July 2019

Military Police

Security of Unclassified Army Resources (Sensitive and Nonsensitive)

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 DODI 5200.08 by establishing physical security policies, procedures, and standards for the safeguarding of U.S. Army resources. It provides guidance for protection of both sensitive and nonsensitive resources, controlled medical resources and other medical resources, historically significant items in the care of the U.S. Army museum system, and U.S. Army Corps of Engineers civil works and like project resources. It gives commanders the flexibility to enhance physical security by adapting invested resources to meet local needs based on risk analysis results. Actual physical security posture will be based on local conditions; however, it must not be less than the minimum standards for the categories of U.S. Army resources specified in this regulation.

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. This publication applies during partial and full mobilization, normal operations, and during contingency operations.

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

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see app G).

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

Distribution. This regulation is available in electronic media only and is intended 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 190–51, dated 30 September 1993 and AR 190–16, dated 31 May 1991.

UNCLASSIFIED

Contents—Continued

Appendixes

Glossary

Chapter 1
Introduction

1–1. Purpose
This regulation prescribes policies, requirements, and responsibilities for safeguarding unclassified named U.S. Army resources, both sensitive and nonsensitive.

1–2. References and forms
See appendix A.

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

1–4. Responsibilities
a. Provost Marshal General. The Provost Marshal General has overall Army Staff responsibility for the security of unclassified sensitive and nonsensitive Army resources and will—

(1) Develop policies, goals, and objectives for the program.

(2) Direct the Chief, Military Police Operations Division (DAPM–MPO) to coordinate with the Army Staff; Army commands; Army service component commands; direct reporting units; the Chief, National Guard Bureau; and the Chief, Army Reserve; and other organizations as appropriate to establish policy, requirements, and standards pertaining to security of Army resources.

(3) Establish standards, criteria, and metrics for the electronic security systems (ESS) programs, based on Army policy, Unified Facilities Guide Specifications (UFGS), manufacturer and engineering specifications, and security industry best-practices.

(4) Plan, program, budget, and execute ESS requirements consistent with this regulation and in accordance with the standards, criteria, and metrics for their respective programs.

b. Commanders of Army commands; Army service component commands; direct reporting units; the Chief, National Guard Bureau; Chief, Army Reserve; senior commanders; garrison commanders; and commanders and directors of U.S. Army Corps of Engineers divisions, districts, centers, laboratories, and field operating activities. These commanders and directors will—

(1) Direct the conduct of physical security inspections per AR 190–13.

(2) Direct the conduct of risk analysis for the resources of assigned and tenant units and activities maintaining specified facilities for particular categories of Army resources under this regulation and for other resources which have been designated mission essential and vulnerable per AR 190–13.

(3) Direct the conduct of risk analysis for the resources of units and activities that are to occupy new or renovated facilities or facility additions. Risk analyses for resources to be located in such facilities will be performed during the planning stages of the facility construction or renovation so that security measures can be incorporated at the project's inception.

(4) Determine security requirements for museum activities in their commands and comply with this and other related regulations and directives.

c. Senior commanders. Senior commanders will—

(1) Ensure a risk analysis is conducted for the assets of all assigned and tenant units and activities maintaining specified facilities for particular categories of Army property under this regulation and for any other assets which have been designated mission essential or vulnerable as indicated in AR 190–13.

(2) Ensure a security risk analysis is conducted for the resources of all activities which are to occupy new or renovated facilities or facility additions. Risk analysis for resources to be located in such facilities will be performed during the planning stages of the construction or renovation so that security measures can be incorporated at the project’s inception.

(3) Determine security requirements for Army asset and activities in their commands and comply with this and other related regulations and directives.

d. Commanding General, U.S. Army Corps of Engineers. The CG, USACE will—

(1) Ensure a security analysis is conducted for the resources of all assigned and tenant units and activities maintaining specified facilities and property for USACE, to include, but not limited to, all stand-alone facilities (SAFs) and real property owned or leased by USACE elements, civil works and like project sites, formerly utilized defense sites, and formerly utilized sites remedial action program sites mandated by congress.

(2) Ensure a security risk analysis is conducted for the resources of all activities which are to occupy new or renovated facilities or facility additions. Risk analysis for resources to be located in such facilities will be performed during the planning stages of the construction or renovation so that security measures can be incorporated at the project's inception.

e. Unit commanders and director and activity chiefs. These commanders, directors, and activity chiefs will—

(1) Implement and enforce physical protective measures and security procedural measures to protect resources within their command or activity.

(2) Promptly report incidents involving loss, theft, misuse, or damage of Army resources required by AR 190–11 or AR 735–5. The reporting requirements are—

(a) Persons responsible for Government property will immediately report, in writing, all losses or damages to their immediate supervisor or commander. The report will state the circumstances of the loss or damage and a listing and description of the property involved.

(b) When reporting personal arms and equipment (PA&E) according to AR 190–11, or whenever the loss appears to involve unlawful conduct, report incident to military law enforcement authorities for investigation. Personal arms and personal equipment are the weapons and equipment assigned to Soldiers for their use. This includes a Soldier's organizational clothing and individual equipment (OCIE) issued to them. A preliminary investigation by the military or security police will assist the commander when taking action according to this regulation.

(3) Establish end-of-day security checks using Standard Form (SF) 701 (Activity Security Checklist).

(4) Based on the results of a risk analysis, the unit commander, director, or activity chief will implement the physical protective measures and security requirements measures described in chapters 3, 4, 5, and 6.

(5) Appoint a physical security officer in writing to perform the duties outlined in AR 190–13.

(6) Establish physical security standard operating requirements outlining responsibilities and requirements for the proper control and accountability of resources.

(7) Direct that resources will be secured with approved locks and locking systems per appendix D.

(8) Establish and record all security checks using SF 702 (Security Container Check Sheet).

(9) Protect property in accordance with its controlled inventory item code (CIIC).

(10) May request the U.S. Army Criminal Investigation Command conduct a crime prevention survey for the purpose of detecting crime, evaluating the possibilities of easy criminal activity, and identifying requirements beneficial to criminal activity.

f. Commanders, directors, and activity chiefs involved in supply operations. These leaders will protect their own supplies and equipment per this regulation.

g. Those assigned custody of controlled medical substances. Commanders and individuals who are assigned custody of controlled medical substances cited in this regulation are responsible for implementing the measures to safeguard them required by this regulation. These responsibilities include—

(1) Ensuring physical security responsibilities are fixed in the receipt, storage, issue, transportation, use, disposal, turn–in, and accounting for all controlled medical substances and sensitive items.

(2) Providing specific security instructions to individuals who are in the possession and control of, or who are responsible for, controlled medical substances and sensitive items.

(3) Ensuring the careful selection of personnel, including volunteer workers, who are assigned duties that require access to controlled medical substances and sensitive items storage areas or who have custodianship or possession of keys and combinations to locks securing these areas.

(4) Taking action to deny access to controlled substances by individuals undergoing investigation, treatment, rehabilitation, judicial or nonjudicial processes, or administrative action as a result of actual or suspected drug abuse or as a result of suspected illegal activity involving controlled drugs (for example, theft, wrongfully prescribing, inventory manipulation, and so forth).

(5) Establishing appropriate escort procedures and designating escort personnel, by name or duty position, to escort unauthorized people into storage areas.

(6) Ensuring a physical security officer is appointed, in writing, by the medical facility commander to assure that appropriate protection is provided for all controlled medical substances and sensitive items.

h. Museum curator. The museum curator is the authority who decides if a weapon is antique or unique and if it should be made inoperable for display purposes.

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 Army 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.

1–6. Objective

The policy objectives are to establish standardized, cost effective, and minimally acceptable security requirements for specified categories of U.S. Army resources, including those of Reserve Component (RC) and Army National Guard (ARNG) units and activities in off-installation SAF when guards and/or agreements with local law enforcement are not available, to provide a risk analysis method that allows commanders the flexibility to tailor physical security posture and resources to meet local need, and to reduce loss, theft, misuse, and damage of Army resources.

1–7. Unified Facilities Criteria and Unified Facilities Guide Specifications

The Unified Facilities Criteria (UFC) and UFGS cited throughout this policy are engineering documents that provide consistent construction standards for Department of Defense (DOD) military departments and defense agencies. The UFCs and UFGSs are collaborative and maintained by the U.S. Army Corps of Engineers, the Naval Facilities Engineering Command, and the U.S. Air Force Civil Engineer Center and are available at the Whole Building Design Guide (http://www.wbdg.org/).

1–8. Security measures and standards

a. Physical security measures and standards more stringent than those contained in this regulation, as appropriate, will be developed jointly by the senior commander in coordination with the tenant activity commander and the installation physical security officer. This also applies to unit commanders, directors, and activity directors in charge of RC (U.S. Army Reserve (USAR) and ARNG) stand-alone (off-installation) facilities. Such measures will be based on a design criteria development requirements developed per UFC 4–020–01. These measures will be incorporated into the installation physical security plan as an annex.

b. Provisions for security and necessary funding will be included in budget documents. Tenant activities must identify their security requirements to the host installation. USACE civil works and like projects will pursue funding to plan, design, construct, and maintain the minimum standard security measures for the resources defined in this regulation through the USACE civil works direct program budget process.

c. Installation of an Intrusion Detection System (IDS) will be per applicable UFGS and with applicable Army regulations depending on the resources to be protected. Examples of regulations that prescribe the use of IDS include, but are not limited to, chapter 6 of this regulation, AR 190–11, AR 190–17, AR 190–54, and AR 190–59. UFGS specifications are available at the Whole Building Design Guide (http://www.wbdg.org/). USAR and ARNG commanders s will incorporate established policy and specifications into ARNG and USAR standards, criteria, metrics, and typical designs for electronic security systems to protect resources. When guard forces are not available, every effort will be made to secure agreements with local law enforcement to conduct checks and patrols as required by this regulation. Where agreements cannot be made with local law enforcement or if the security checks and patrols are not being conducted in accordance with the agreement, this regulation specifies the measures that will be taken in order to protect the specific asset.

1–9. Security criteria deviation process

Use the process provided in AR 190–13 to request a waiver or exception to this policy.

Chapter 2
Risk Analysis

2–1. General

a. Commanders, directors, and activity chiefs will identify resources to be protected and analyze the risks to those resources from espionage, sabotage, terrorism, damage, misuse, and theft to provide the most practical protection. Risk analysis will assist in determining the type and minimum level of protection needed to adequately and economically safeguard resources.

b. The objectives of risk analysis are to—

(1) Provide commanders and directors a tool to design a physical security system based on local needs.

(2) Allow commanders and directors the flexibility to adapt the use of physical security resources to local risk conditions.

(3) Obtain the maximum security return from invested fiscal and manpower resources.

(4) Serve as a basis for a resource–specific threat analysis.

(5) Serve as a basis for physical security inspections utilizing the U.S. Army Security Management System (Countermeasures) (SMS(CM)).

2–2. Use of risk analysis

a. The background and explanation of the requirements for determining security requirements and conducting a risk analysis for categories of Army resources are in DA Pam 190–51. A risk analysis will be conducted for mission essential and vulnerable areas (MEVAs) in accordance with AR 190–13 and the resource categories in chapter 3 and chapter 6, section III—

(1) When a unit or activity is activated.

(2) When a unit permanently relocates to a new site or facility.

(3) When no formal record exists of a prior risk analysis.

(4) At least every 3 years or more frequently at the discretion of the unit commander, director, or activity chief .

(5) During the planning stages of new facilities, additions to facilities, and facility renovations.

(6) When an incident occurs in which resources are compromised.

b. The installation physical security office will conduct a risk analysis for MEVA assets not owned by a command or activity, when directed by the senior commander and conduct a review of all risk analysis submitted by commands or activities.

c. Command or activity physical security officers will conduct risk analyses of all command level MEVAs listed in AR 190–13. Command or activity physical security officers will submit risk analyses with their command MEVA list to the installation/garrison or Directorate of Emergency Services (DES) physical security office annually for review.

2–3. Implementation of risk analysis

a. Based on risk analysis results, the unit commander/director or activity chief will implement the physical protective measures and security requirements prescribed in chapter 3, section II and chapter 6, section III. The resources listed in section III of chapter 3, chapter 4, chapter 5, and section IV of chapter 6 do not require risk analysis.

b. Results of the risk analysis and physical protective measures and security procedural measures to be implemented will be recorded in the SMS(CM). The DA Form 7278 (Risk Level Worksheet) will be used if a SMS(CM) is not readily available. Instructions for the risk analysis process are in DA Pam 190–51. Copies of these records will be kept by the supporting provost marshal, DES, or equivalent Army or agency designated security officer for the unit or activity concerned. The results will be used in planning and assessing physical security programs under AR 190–13.

c. Results from the risk analysis may be reviewed and portions of the results revised at the discretion of the unit or senior commander, director, or activity chief/director, senior USAR site commander, or State Adjutant General. Revisions will be based on a significant change in risk factors to a specific category of Army resources, to a particular unit or activity, or installation. Revisions will be coordinated with the supporting provost marshal, DES, or equivalent Army or agency designated security officer. The rational or reasons for any revisions to the risk analysis incorporated as a result of the unit, activity, or senior commander, director, or chief exercising their discretion to change results will be documented in the form of a memo attached to the risk analysis report.

d. In addition to the risk analysis for resources outlined above, antiterrorism (AT) risk assessments are conducted in accordance with AR 525–13 to assess and control terrorism risks associated with missions, functions, or operations.

Chapter 3
Physical Security Standards by Category of Army Resources

Section I

Overview

3–1. General

a. Common types of U.S. Army resources are categorized in this chapter for quick reference. Guidance for each category includes references to the primary directives for management and accountability and required minimum security standards.

b. Section II of this chapter outlines physical protective measures and security procedural measures for particular resource categories. The measures are categorized by risk levels established using the risk analysis procedure in DA Pam 190–51. Risk level I measures will be the minimum.

c. Section III of this chapter outlines measures for resource categories that do not require risk analysis.

d. All facilities will incorporate a key and lock control program.

e. See appendix D for the use of master-keyed and keyed-alike lock systems.

f. Other types of U.S. Army resources have unique requirements. As such, any resource categorized in DA Pam 190–51 as "M. U.S. Army Corps of Engineers Civil Works and Like Projects," or "O. Medical and Medical Research Resources" will follow the guidelines of chapters 6 and 4 respectively.

3–2. Guidance and requirements for fencing

a. General.

(1) Use UFC 4–022–03 to design security fences and gates.

(2) Variations can be made to allow for different materials and to allow for the esthetics of a community, provided the physical protective value of the variation is not less than the value afforded by the above fence type.

(3) Fencing specifications are available at https://wbdg.org and fence drawings are available at https://pdc.usace.army.mil.

b. Perimeter fencing.

(1) The minimum fence fabric height of 7 feet, excluding the top guard. Fence height including outriggers must be a minimum of 8 feet.

(2) When perimeter fencing is required as a protective measure, the type and quantity of fencing, including heights in excess of 7 feet and whether a top guard or other features are required will be based on the appropriate security publication and the judgment of the responsible senior commander/director or chief.

(3) A nonsensored perimeter fence will meet the requirements of UFGS 32 31 13 and USACE drawing number Standard (STD) 872–90–03, unless otherwise specified.

3–3. Guidance and requirements for security lighting

Use UFC 3–530–01 as a guide for lighting patterns and minimum protective lighting intensities and requirements.

3–4. Guidance and requirements for electronic security systems

a. Use of ESS will meet requirements of UFGS 28 10 05 (for example, IDS, Closed Circuit Television (CCTV) systems, and Access Control System (ACS)). ESS should be used with fencing or barriers to provide delay to which will enhance the security and allow time for greater response time before access is gained.

b. IDS will meet the minimum requirements of UFGS 28 10 05. IDS will be used to ensure aggressors are detect before they reach a resource from any path that might be used to approach it.

c. Central monitoring services for ESS will meet requirements of UFGS 28 20 02.

d. CCTV systems will meet requirements of UFGS 28 10 05.

e. The RCs use commercial off-the-shelf (COTS) systems which are compliant with the above specifications and which also comply with the RC standards and criteria.

f. Where systems are required to comply with cybersecurity requirements, such as risk management framework, the Regular Army, ARNG, and USAR are responsible for ensuring that any ESS deployed will comply with these requirements.

g. ESS not specifically identified as a regulatory requirement by AR 190–17, AR 190–54, or AR 190–59 may be purchased and maintained by commands if the command opts to use these systems. CCTV systems, components, and supporting equipment and well as video telecom systems not required will be funded by commands, not Management Decision Package (MDEP) Physical Security Matters (program QPSM) funds.

3–5. Guidance for locks, electronic locks and locking systems, keys, locking devices, hasps and chains, and protective seals

Follow standards in appendix D.

3–6. Guidance for antiterrorism measures

Apply AT standards in AR 525–13.

3–7. Guidance for safety

Any conflicts between security and safety requirements will be identified in writing. Waiver or exception requests must list compensatory measures.

3–8. Guidance for resources that do not fit the listed categories

This publication cannot list all Army resources so some resources will not correspond exactly to the categories in this publication, or some may relate to multiple categories. If no category seems appropriate, the commander responsible for the resource will develop and implement physical protective measures and security procedural measures necessary to safeguard the resource. The measures will be reviewed by the supporting physical security officer and approved by the senior commander.

Section II

Minimum Security Standards for Resources Requiring Risk Analysis

3–9. Aircraft and components at Army aviation facilities

a. Property management and accountability directives.

(1) AR 95–1.

(2) AR 710–2.

(3) AR 735–5.

(4) DA Pam 710–2–1.

b. Aircraft with arms, ammunition, and explosives aboard. Army aircraft with arms, ammunition, and explosives (AA&E) aboard will be secured per AR 190–11 and this regulation.

(1) When not in use, aircraft containing weapons will be parked inside an aircraft parking area. The parking area will be lighted and will have either continuous surveillance or an IDS on the perimeters to detect aggressor before they access the aircraft.

(2) When operational readiness permits, weapons mounted on aircraft that are accessible and easily removable will be removed and stored in a secure location. Weapons that remain installed on the aircraft will be made inoperable by removing barrels or firing mechanisms when practical in accordance with AR 190–11.

(3) Removed components will be stored in a secured location. A secured location is an arms room, an ammunition supply point, an area under continuous armed surveillance, or any structure meeting the requirements for storage of category I or II AA&E in AR 190–11.

c. Accessible and easily removable components. Additional security for accessible and easily removable components will be by storage in a secure structure per appendix B.

d. Aircraft with classified material. U.S. Army aircraft with classified materials aboard will be secured per AR 380–5. Classified materials which can be readily removed will be placed in secure storage per AR 380–5.

e. Unmanned aerial systems. The requirements in this paragraph apply to unmanned aircraft systems over 20 pounds (for example, RQ–4 Global Hawk, MQ–1 Predator, and Sky Warrior) and maintained in aircraft parking areas/hangars. Unmanned aircraft systems under 20 pounds (for example, RQ–11 Raven, RQ–14 Dragon Eye) will be secured per paragraph 3–27*c*.

f. Physical protective measures (risk level I).

(1) Army aircraft at Army aviation facilities will be secured with manufacturer-installed or approved modification work order ignition and door–locking security devices when not in use. Aircraft undergoing maintenance with duty personnel present and aircraft employed in tactical exercises are exempt.

(2) Keys to locking devices and ignitions will be controlled and accounted for per appendix D. Aircraft keys will not be issued for personal retention. Duplicate keys will not serve as operational keys at maintenance facilities.

(3) When not in use, aircraft and aircraft components, to include crew member equipment at Army aviation facilities, will be placed in the most secure hangars or structures available. If adequate hangar space is not available, this equipment may be stored on the ramp nearest the facility.

(4) When aircraft are not stored in storage structures and when operational requirements permit, keep them in proximity to each other for ease of monitoring and away from the perimeter of the parking area unless operational considerations dictate otherwise.

g. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Aviation facility aircraft parking areas will be protected by a perimeter fence. Parking areas already located within perimeter fences, such as provided by an adjacent civil airport, do not require a separate perimeter fence.

h. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Aviation facility aircraft parking areas will be lighted at night sufficiently to allow security personnel to detect intruders. Airfield lighting will be coordinated with the aviation facility commander for consideration of safety and training issues.

(3) IDS should be added to hangars and, where practical, around aircraft parking areas.

i. Security procedural measures (risk level I).

(1) Each Army aviation facility will have a physical security officer appointed in writing. Responsibilities of the physical security officer are defined in AR 190–13.

(2) Each Army aviation facility will develop a physical security plan and will—

(a) Be prepared by the physical security officer in accordance with AR 190–13.

(b) Aviation facilities located on or close to an Army installation will include the physical security plan as an annex to the installation physical security plan.

(c) Aviation facilities located on other than Army property will coordinate the physical security plan with the appropriate host authorities.

(d) A copy of the ARNG and USAR physical security plan will be maintained by the State Adjutant General or major U.S. Army Reserve Command provost marshal for RC aviation facilities.

(3) Screening of arriving and departing aircraft at U.S. Army airfields and heliports. Senior/garrison commanders will develop and implement access control requirements to screen arriving and departing aircraft. All aircraft, passengers, and cargo arriving at or departing from Army airfields or heliports will be screened per access control requirements that will address the following situations, at a minimum:

(a) U.S. Government aircraft, if directed by the senior/garrison commander.

(b) Civilian and foreign aircraft on approved Army aircraft landing authorization numbers or civil aircraft landing permit (see AR 95–2).

(c) Aircraft executing an emergency landing.

(d) Any aircraft not scheduled or authorized to land at an Army airfield or heliport.

(e) Aircraft will be checked at least every 4 hours by roving guard and recorded using the SF 702.

(4) For aircraft parked at Regular Army aviation facilities and for USAR and ARNG activities where guards or roving patrols are available, aircraft will be checked at least every 4 hours by a roving guard and recorded using the SF 702. At USAR and ARNG activities where guards or roving patrols are not available, local law enforcement agencies will be requested, in writing, to include the aviation facilities in their patrol areas and to check aircraft parking areas at intervals not exceeding once every 4 hours during nonoperational hours.

(5) Access to aviation facility aircraft and aircraft components will be controlled at all times through the use of access rosters at a minimum. The access roster will be approved by the aviation facility or airfield commander. The airfield will be designated as a restricted area per AR 190–13. Measures such as badges, passes, or similar identification credentials are encouraged.

(6) Privately owned vehicles will be prohibited from the flight line or other areas where aircraft are parked, except when individually authorized in writing by the aviation facility or airfield commander. Blanket authorizations will not be used.

(7) Aviation facility auxiliary power units for starting aircraft, vehicle tugs, forklifts, aircraft boarding ladders, and other items that might be used to circumvent existing security measures will be secured during non-duty hours to prevent unauthorized use.

(8) Conduct end-of-day security checks and record the checks on the SF 701.

j. Security procedural measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Entry to and exit from all buildings associated with the aviation facility, aircraft parking areas, and support equipment storage areas will be controlled at all times. Entry and exit can be controlled through manpower and procedural means, mechanical means, or electronic means.

(3) Aircraft parked at Regular Army aviation facilities will be checked at least once every hour by a roving guard after duty hours and recorded using the SF 702.

k. Security procedural measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Guards will provide continuous surveillance of aircraft parked at Regular Army aviation facilities. Aviation unit personnel working on or near aircraft may be considered to be equivalent to continuous surveillance.

(3) IDS may be installed as an alternative to providing continuous surveillance.

(4) At USAR and ARNG facilities where guards or roving patrols are available, aircraft will be checked at least every 4 hours and recorded using the SF 702. Where guards or roving patrols are not available, local law enforcement agencies will be requested, in writing, to include USAR and ARNG aviation facilities in their patrol areas, and to check the parking

areas at least once every 4 hours during nonoperational hours. Commands who cannot meet the requirements of this paragraph will complete a deviation request in accordance with AR 190–13.

l. Other Department of Defense component aircraft transiting Army installations.

(1) Plans will be developed to protect aircraft from other military departments and defense agencies that transit Army installations. The transiting department or agency is expected to provide a request for special security support as far in advance as possible. The host commander will provide security without resorting to external support to the extent feasible.

(2) The transiting department or agency cognizant DOD component is responsible for requirements beyond those provided by the Army host commander and should provide materiel and personnel especially those that cause a heavy expenditure of funds, equipment, or manpower, or unique or unusual technology.

3–10. Aircraft and components not at Army aviation facilities

a. Follow the accountability requirements in paragraph 3–9*a*, and the security requirements in paragraphs 3–9*b*, 3–9*c*, 3–9*d*, and 3–9*e*.

b. Physical protective measures for risk level I in paragraph 3–9 will also be implemented along with the following security physical protective measures:

(1) The aircraft will be parked, whenever practical, at a Government airfield or civilian airport with an active security program. If a location has no security program and a crew member cannot remain with the aircraft, the aircraft commander will advise local aviation facility and local law enforcement authorities of the aircraft location, identification, length of stay, and ways to contact crew members.

(2) The aircraft will be checked at least once daily by a crew member for tampering, sabotage, and loss or damage.

3–11. Vehicles and carriage-mounted or towed weapons systems

a. Property management and accountability directives.

(1) AR 58–1.

(2) AR 710–2.

(3) AR 735–5.

(4) DA Pam 710–2–1.

(5) DA Pam 750–8.

b. Army vehicles with weapons or ammunition aboard. These vehicles will be secured per AR 190–11. When operational readiness permits, weapons mounted on vehicles that are accessible and easily removable will be removed and stored in a secure location. Unless there is an operational necessity determined by battalion or higher level commanders, firing mechanisms on weapons that are not easily removable will be removed from combat vehicle weapon systems and stored in the unit arms room or be under continuous surveillance.

c. Army vehicles with classified equipment. These vehicles will be secured per AR 380–5. Classified components that can be readily removed without damage will be placed in secure storage per AR 380–5.

d. Army vehicles when not in use. These vehicles will be parked in motor pools to the maximum extent practicable. The motor pool will be protected by a perimeter fence or dedicated guards. UFGS 32 31 13 will be used as a guide for determining fencing requirements.

e. Army vehicle dispatch. All vehicles will be dispatched in accordance with DA Pam 750–8 prior to leaving the motor pools.

f. Physical protective measures (risk level I).

(1) Vehicle parking areas, except those for empty trailers, will be lighted during the hours of darkness. Vehicles parked in noncombat areas will be secured with an approved locking mechanism as follows:

(a) Commercial-design vehicles. Activate manufacturer-installed door and ignition-locking device(s).

(b) Tactical vehicles with steering wheels. Steering wheels will be immobilized with an installed and approved locking mechanism or cable/approved chain wrapped around the spoke of the steering wheel and low security padlock. Those tactical armored vehicles, such as Abram Tanks, M113 family of vehicles, Bradley infantry fighting vehicles, uparmored high-mobility multipurpose wheeled vehicles, Mine Resistant Ambush Protected vehicles will be secured as per their technical manuals (TMs). Hatches and other openings into the vehicles will be secured with an approved low security padlock or their integrated combat locking systems. Hood, spare tires, and fuel tank should also be secured with vehicle installed locking devices if the local environment warrants this action. Brass padlocks supplied with vehicles may be used to secure vehicle compartments, except those uploaded with AA&E or other sensitive items and as long as other security measures required by applicable regulations and directives are followed.

(c) Other Army vehicles. M1008, 1009, and 1010 series vehicles and commercial utility and cargo vehicles will be secured by activating installed door and ignition locks and immobilizing the steering wheel with a low security padlock. As an alternative, such vehicles may be stored in a secure structure.

(d) Material handling equipment. Material handling equipment and other Army vehicles which cannot be secured as indicated in paragraphs 3–11*f*(a) through 3–11*f*(c) will have the steering mechanism immobilized or transmission lever locked in the neutral position. Alternatively, these vehicles may be stored in secure structures.

(e) Signs. Signs will be posted at activity entrances stating "Restricted Area."

(2) Exceptions to this policy are as follows:

(a) Vehicles actively employed in tactical exercises and field operations, undergoing test and evaluation, or pending turn-in through property disposal channels.

(b) Dispatched emergency, military or security police, courtesy patrol, and interior guard vehicles for brief periods when response time is critical for the successful performance of the operator's or crew's duties. Ignition keys will be removed from unaccompanied vehicles.

(c) Trailers, semitrailers, towed weapons systems, and other non-self-propelled vehicles.

(d) Inoperable, unserviceable vehicles. Requirements will be implemented to protect these vehicles from cannibalization.

(e) Vehicles, without installed locking mechanisms, under the continuous surveillance of a guard.

(f) Vehicles of specific units outside the United States when so designated by the equipment owning commander. Basis for a unit exemption will be an impact on readiness. The equipment owning commander will decide whether locking the unit's vehicles would adversely affect readiness to the extent of jeopardizing the unit's contingency mission.

(g) Fuel tanker vehicles when, in the judgment of the equipment owning commander, locking would create a potential unacceptable hazard to life or property. In this case, continuous surveillance through guards or roving patrols will be provided.

(h) Administrative use vehicles, as defined in AR 58–1, when dictated by safety requirements within an ammunition or explosives production or storage area.

(3) Accessible and easily removable components. These components, vulnerable to theft because of value or utility, will be removed and secured separately. Additional security for components will be provided by one of the following methods:

(a) Storing in a secure storage structure per appendix B.

(b) Storing in a locked, totally enclosed armored vehicle or truck van.

(c) Storing in a locked equipment box or similar container secured to an open bed vehicle; for example, in a locked ammunition or tool box chained to the bed of a 2–1/2 ton truck.

(d) Securing the item directly to the vehicle by a locally fabricated method.

(e) Keys and locks will be controlled in accordance with appendix D.

(f) Items that can be used to defeat security measures, such as bolt cutters, hacksaws, oxyacetylene torches, axes, or steel rods or bars will be secured in respective tool kits or other secure locations when not in use.

g. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Vehicles, trailers, storage containers, and equipment will be kept at least 20 feet away to the extent feasible from the perimeter to avoid their use by intruders as a means to climb the fence and to provide clear observation of the boundary by unit members and security forces.

h. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Ground anchors will be constructed for trailers, semitrailers, and other towed equipment or a cable will be run through all items of such equipment and a lock will be affixed to one end.

(3) Vehicles particularly vulnerable to theft, misappropriation, or damage will be placed in secured garages and motor sheds to the maximum extent practicable.

i. Security procedural measures (risk level I).

(1) For Regular Army installations and for USAR and ARNG units and activities at locations where guards or roving patrols are available, motor pools will be checked for tampering, sabotage, loss, and damage not less than once every 4 hours after duty hours and recorded using the SF 702.

(2) USAR and ARNG units and activities commanders at locations where guards are not available will request, in writing, that the local law enforcement agency check the security of the motor pool at intervals not exceeding 4 hours during nonoperational hours and recorded using the SF 702.

(3) Privately owned vehicles will not be permitted in motor pools except that units engaged in deployment exercises may store privately owned vehicles in the motor pool at the discretion of the installation or USAR commander, or State Adjutant General provided security measures are taken to safeguard Army vehicles and components remaining in the mot or pool.

(4) Those privately owned vehicles owned by contractors and required for the performance of their jobs will be allowed access after the contract officer representative provides an access roster listing all vehicles and personnel, as well as the reason for access, to the battalion commander or the highest level commander responsible for the motor pool. This access roster will be used to match against the vehicle and the personnel prior to allowing access. Unit personnel or guards will escort all privately owned vehicles allowed access to and from the job site while within the motor pool. Requirement will be required language within any contracts that allow access to controlled access areas.

(5) Conduct end–of–day security checks using SF 701.

j. Security procedural measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Entry to and exit from motor pools will be controlled. Control of entry and exit may be by guards or locks on gates. Unit personnel working in the motor pool are an alternative to guards if they are capable of controlling entry and exit.

(3) Multi-unit motor pools—

(a) A commander will be designated as the host having responsibility for the overall security of the motor pool. The host commander will establish a signed memorandum of agreement with tenant commanders.

(b) At a minimum, requirements will be established to fix responsibility for issue, receipt, and accountability for vehicles; for controlling vehicular and pedestrian entry control points; for building, vehicle, and storage building security requirements; and assigning responsibility for key control per appendix D.

(4) Types of vehicles particularly vulnerable to theft, misappropriation, or damage in the motor pool will be segregated. These vehicles will be placed where guards or unit personnel can see them during operating hours and where roving guards can see them during non-operating hours.

(5) The motor pool will be designated a restricted area.

k. Security procedural measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Drivers will be checked for possession of a valid dispatch and operator's permit by unit personnel or guards before they depart the motor pool.

(3) Continuous surveillance will be made of the motor pool by guards on Regular Army installations.

(4) IDS may be installed in accordance with regulatory guidance as an alternative to providing surveillance during the operational hours of the aviation facility.

(5) At USAR and ARNG activities where guards or roving patrols are available, motor pools will be checked for tampering, sabotage, loss, or damage no less than once every 4 hours. Where guards or roving patrols are not available, local law enforcement agencies will be requested, in writing, to include USAR and ARNG motor pools in their patrol areas, and to check the parking areas at least once every 4 hours during nonoperational hours and recorded on an SF 702.

(6) Keyed-alike locksets.

(a) Keyed-alike locksets are authorized to secure various storage compartments within one vehicle to include the lock used to secure the steering wheel.

(b) Keyed-alike locksets may be used to secure the manifold access doors and hatches of petroleum, oil, and lubricants (POL) trucks (one set per truck).

(7) Low security padlocks with hardened steel shackles may be used for the storage compartments of wreckers, heavy equipment, and so forth (one set per vehicle). The same set will not be used on more than one vehicle.

(8) Master-keyed locksets. (See appendix D for the use of master-keyed and keyed-alike lock systems.)

3–12. Communications and electronics equipment, forward repair systems, standard automotive tool sets, night vision devices, other high-value optical devices, high-value precision equipment, and launched electrode stun devices

a. Property management and accountability directives.

(1) AR 710–2.

(2) AR 735–5.

(3) DA Pam 710–2–1.

b. Store and maintain all property in accordance with the requirements of its Controlled Inventory Item Code. When no code exist the following security requirements will be used:

(1) *Physical protective measures (risk level I).*

(a) Portable items will be provided double barrier protection when not in use, to include training environments and while in transit. Examples of double barrier protection include—

1. A locked or guarded separate building or an enclosed van, trailer, or armored vehicle protected by a perimeter fence identified in paragraph 3–2.

2. A locked steel cage located in a secure storage structure (see app B).

3. A locked high-value asset security cage (HVASC) located in a locked room that is not constructed per appendix B.

4. A locked, built-in container (bin, drawer, cabinet) or a free-standing locked container located in a secure storage structure (see app B).

5. Securely affixing the item to an internal structure of a secure storage structure (see apps B and D).

6. Securely affixing the item to a locked vehicle which is under continuous surveillance or in a motor pool (see app D).

(b) Nonportable items will be secured in a building with doors and windows locked during the hours the facility is nonoperational. Particularly bulky or heavy items stored outside will be protected by a perimeter fence.

1. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

2. Equipment will be located in the interior of the facility as far from the exterior as possible.

3. Tactical communications equipment remaining on vehicles will be secured to the vehicle with an approved low security padlock. Vehicles will be secured per paragraph 3–11.

4. Tool kits will be secured as specified in paragraph 3–27.

(2) *Physical protective measures (risk level II).*

(a) Measures required for risk level I will be implemented.

(b) Portable, pilferage-coded items will be separated from other equipment and stored in a separate, locked, secure room, area, or container with controlled access. Secure rooms will be constructed per secure structure guidance in appendix B.

(3) *Physical protective measures (risk level III).*

(a) All measures required for risk levels I and II will be implemented.

(b) The activity will be lighted during the hours of darkness.

(c) Landscaping features greater than 1-foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

(d) IDS will be installed around or on the storage room, area, or container.

(4) *Security procedural measures (risk level I).*

(a) Access to the equipment storage area will be controlled.

(b) Access to keys, padlocks, and protective seals will be controlled per appendix D. Portable, pilferage–coded items temporarily assigned to a user will be issued on a hand receipt.

(c) Command-directed inventories will be made as indicated in AR 710–2. A copy of the inventory will be kept until the next inventory is conducted.

(5) *Security procedural measures (risk level II).*

(a) Measures required for risk level I will be implemented.

(b) Privately owned vehicles will not be permitted to park within 50 feet of the storage facility.

(6) *Security procedural measures (risk level III).*

(a) Measures required for risk levels I and II will be implemented.

(b) Stock accounting records for portable pilferage–coded items will be reviewed at least monthly by an officer, non-commissioned officer (sergeant or above), or civilian employee of equivalent grade. A record of such review will be maintained until completion of the next monthly review.

(c) The activity will be checked at least every 4 hours after duty hours by guards on Regular Army installations and recorded using the SF 702.

(d) Local law enforcement agencies will be requested, in writing, to include USAR and ARNG facilities storing communications and electronics equipment in their patrol areas and to check the facilities at least every 4 hours during nonoperational hours.

(7) *Launched electrode stun devices.*

(a) A launched electrode stun device (LESD) without an attached cartridge will be secured per appendix B. Issued LESDs will not be left unattended at any time.

(b) All LESDs will be strictly accounted for as CIIC of controlled inventory items.

(c) Cartridges for LESDs are category IV ammunition. Non-issued cartridges will be secured in an arms room or ammunition supply point per category IV requirements in AR 190–11.

3–13. Organizational clothing and individual equipment stored at central issue facilities

a. Property management and accountability directives.

(1) AR 710–2.

(2) AR 735–5.

(3) DA Pam 710–2–1.

b. Physical protective measures (risk level I).

(1) Stocks will be secured in a separate building or room meeting the security standards per paragraph B–1.

(2) The facility exterior will be lighted during the hours of darkness.

(3) Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

c. Physical protective measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) High-value or small, easily pilferable items will be separated from other OCIE and stored in a secure, separate container, room, or building with controlled access.

d. Physical protective measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) IDS will be installed in the facility.

(3) Rooms or buildings will be constructed per secure storage structure guidance for at least risk level II in appendix B.

(4) Landscaping features greater than 1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

e. Security procedural measures (risk level I).

(1) Access to the facility and to keys, padlocks, and protective seals will be controlled in accordance with appendix D.

(2) Command-directed inventories will be conducted per AR 710–2.

(3) Conduct end-of-day security checks using SF 701.

f. Security procedural measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) The joint inventory check–out point will be placed next to the facility exit to preclude personnel from remaining in the facility once the OCIE has been inventoried. A copy of the inventory will be retained until the next inventory is conducted.

g. Security procedural measures (risk level III).

(1) Measures for risk levels I and II will be implemented.

(2) The facility will be checked at least once every 4 hours by roving guards and recorded using the SF 702.

3–14. Organizational clothing and individual equipment not at central issue facilities

a. Risk level I physical protective measures and the security requirements in paragraph 3–13 will be implemented for OCIE stored centrally in units.

b. OCIE will not be stored in privately owned vehicles.

c. Individual clothing and equipment of personnel living in troop billets and RC personnel will be secured by one of the following means to be determined by the unit commander.

(1) In a locked wall locker or footlocker.

(2) In a locked duffel bag, further secured to the building structure, or a separate locked room.

d. Access to RC OCIE will be controlled by designated personnel. Locked duffel bags, wall lockers, or footlockers will be placed in a separate locked room or cage. In lieu of a separate room, access to wall lockers may be controlled by modifying the lockers to accept a locking bar or by adding a second hasp and securing the locker with a second lock. Keys to access RC OCIE will be placed in the unit key depository and access will be controlled by the unit key custodian.

3–15. Subsistence items stored at commissaries, commissary warehouses, and troop issue subsistence activities

a. Property management accountability directives.

(1) AR 30–22.

(2) AR 735–5.

b. Physical protective measures (risk level I).

(1) Commissaries, commissary and subsistence warehouses, and troop issue subsistence activities will meet the construction requirements for secure storage structures in appendix B.

(2) "Off Limits to Unauthorized Personnel "signs will be posted at entrances to subsistence storage facilities signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

(3) Refrigeration units will be secured with approved locking devices or kept in a room or building meeting the standards for secure storage structures in appendix B.

(4) Subsistence items temporarily stored outside the facility, such as in secured vans and reefer trucks, will have protective lighting. Use UFC 3–530–01 as a guide to determine the type of protective lighting.

(5) Break areas will be located away from the storage areas.

(6) Personal lockers will be in a designated area away from loose or broken containers of subsistence items.

c. Physical protective measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Highly pilferable items such as cigarettes, coffee, and health and beauty aids will be placed in a separate locked room, cage, or container under the control of a designated property custodian.

(3) Protective seals will be placed on doors and other operable openings into secured vans and reefer trucks in which subsistence items are stored outside the facility.

d. Physical protective measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) The facility will be lighted during the hours of darkness.

(3) IDS will be installed in the facility.

(4) Landscaping features greater than 1-foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

e. Security procedural measures (risk level I).

(1) Access to subsistence storage facilities, the facility and to keys, and padlocks, and protective seals protecting assets will be controlled in according to appendix D.

(2) Subsistence storage facilities will always be secured when entrances or exits are not under the surveillance of personnel assigned to the facility.

(3) Personal packages and hand-carried items will be prohibited in ration breakdown and subsistence storage areas.

(4) Shipping containers and cases will be inspected to ensure that they are empty prior to being disposed of and cardboard boxes will be flattened before disposal.

(5) Conduct end–of–day security checks using SF 701.

f. Security procedural measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Personnel entering the storage facility who are not assigned to the activity will be logged in and out or, when practical, escorted. When using the log system, designate the destination of the unassigned person.

(3) Accuracy of scales will be tested monthly with known weights or by using a second set of calibrated scales. A written record of the monthly tests will be maintained for a period of 3 months.

(4) Highly pilferable items will be spot-checked daily by supervisors to ensure that all items are accounted for. These items will also be inventoried each quarter and a copy of the inventory kept until the next inventory.

(5) Trash receptacles will not be located within 50 feet of the facility.

(6) Privately owned vehicles will not be parked within 50 feet of the storage facility.

g. Security procedural measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) Highly pilferable items will be inventoried once each month. A copy of the inventory will be kept until the next inventory.

(3) The facility will be checked at least every 4 hours after normal duty operating hours by roving guards and recorded using the SF 702.

3–16. Subsistence items not stored at commissaries, commissary warehouses, and troop issue subsistence activities

Risk level I physical protective measures and the security requirements in paragraph 3–9 will be implemented.

3–17. Repair parts at installation level supply support activities and direct support units with an authorized stockage list

a. Property management and accountability directives.

(1) AR 708–1.

(2) AR 710–2.

(3) AR 735–5.

(4) DA Pam 710–2–1.

b. Classified repair parts. Secure these items per the AR 380 series of requirements. Store all property in accordance with its CIIC, but at the minimum, property will be stored in the following manner:

(1) *Physical protective measures (risk level I).*

(a) Portable repair parts will be secured in the following manner:

1. In a locked building or room, meeting the secure storage structure standards in appendix B.

2. In a locked, steel cage.

3. In a locked, built-in container (bin, drawer, cabinet) or a free-standing container (desk, wall locker, container express (CONEX)) large and heavy enough to be non-portable with stored parts.

(b) Attached to the building in which located or other permanent structure.

(c) Non-portable repair parts will be secured in a building with doors and windows locked during those hours the facility is nonoperational. When bulky or heavy items are stored outside, they will be protected by a perimeter fence addressed in paragraph 3–12.

(d) Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

(2) *Physical protective measures (risk level II).*

(a) Measures required for risk level I will be implemented.

(b) Pilferage-coded items will be separated from other stock and stored in a separate room, building, or container with controlled access.

(c) Rooms or buildings will be constructed per secure storage structure standards in appendix B.

(3) *Physical protective measures (risk level III).*

(a) Measures required for risk levels I and II will be implemented.

(b) The storage facility will be lighted during the hours of darkness.

(c) IDS will be installed in the storage facility or continuous surveillance through the use of on-site guards.

(d) Landscaping features greater than1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

c. Security procedural measures (risk levels I and II).

(1) Access to storage areas, keys, padlocks, and protective seals protecting these items will be controlled.

(2) Command-directed inventories will be conducted per AR 710–2.

(3) Used parts will be processed as indicated in DODM 4160.21 to recover parts when prescribed, to protect and dispose of non-recoverable parts, and to preclude recycling.

(4) Conduct end-of-day security checks using SF 701.

d. Security procedural measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) The facility will be checked at least every 4 hours after duty hours by guards and recorded using the SF 702.

(3) Access for pilferage-coded items will be separately controlled.

3–18. Repair parts not at installation level support activities and direct support units

a. Risk level I physical protective measures and the security requirements in paragraph 3–17 will be implemented.

b. Unit and activity repair parts will be stored in a single area, readily accessible to designated maintenance or supply personnel only.

3–19. Petroleum, oils, and lubricants at bulk storage facilities

The following requirements apply to government-owned/government-operated, and government-owned/contractor-operated fuel support points, pipeline pumping stations, piers, and other similar bulk storage sites. Conduct security planning and protection per DODD 3020.40 if the facility is designated as part of the Defense Critical Infrastructure Program.

a. Property management and accountability directives.

(1) AR 710–2.

(2) AR 735–5.

(3) DA Pam 710–2–1.

b. Physical protective measures (risk level I).

(1) Construction of storage facilities will be per UFC 3–460–01.

(2) When not under the surveillance of personnel authorized to dispense the products, POL pumps will be locked and electrical power turned off. The electrical power shutoff will be secured. Hoses to pumps will be secured to prevent loss of POL through gravity feed. These measures are not required if pumps are activated by a credit card or a fuel key. Use of such devices will be approved by the unit commander concerned.

(3) Packaged POL will be stored in structures under secure storage structure standards in appendix B. Large POL packages (for example, 55-gallon drums) will be stored to preclude their use as hiding places for pilfered items.

(4) Keys to petroleum, oil, and lubricants storage areas, equipment, and buildings will be controlled per appendix D.

c. Physical protective measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Storage facilities will have a perimeter fence. Gates and openings will be closed and locked.

(3) Signs will be posted at the perimeter stating "Off Limits To Unauthorized Personnel."

d. Physical protective measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) Storage facilities will be lighted during the hours of darkness.

(3) Seals will be placed on all points of fuel storage that could allow extraction of fuel by any means. A broken seal may indicate tampering.

e. Security procedural measures (risk level I).

(1) Written instructions to POL dispensing personnel will include procedures for determining if patrons entering the facility are authorized and vehicles have valid dispatches.

(2) When unattended, the facility will be checked at least once every 4 hours and recorded using the SF 702.

(3) POL credit cards, fuel keys, identification plates, and aviation fuel plates will be centrally controlled by a custodian, preferably at the director of logistics level. Credit cards, identification plates, and aviation fuel plates will be secured in a locked container with controlled access. They will be controlled through a log book with the signature and rank of the person to whom issued, credit card and identaplate serial number, aircraft or vehicle number or U.S. Army registration number, and date and time signed out and returned.

(4) Privately owned vehicles will not be permitted in storage facilities unless it is approved based upon the judgment of the responsible commander.

(5) All incoming and outgoing issuances of fuel will be accounted for and supervised by authorized personnel.

(6) Hoses or other devices to siphon fuel will be secured. All containers that can be used to carry fuel also will be secured.

(7) Containers storing used POL will be marked and stored separately.

(8) Keys to POL storage areas, equipment, buildings, and protective seals will be controlled in accordance with appendix D.

(9) Conduct end-of-day security checks using SF 701.

f. Security procedural measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Facility personnel will verify all POL quantities issued by personally reading the meter.

(3) When unattended, the facility will be checked at least once every 4 hours and recorded using the SF 702.

g. Security procedural measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) The storage facility will be designated a restricted area per AR 190–13.

(3) Continuous surveillance will be made of the facility by guards.

(4) Intrusion detection systems may be installed as an alternative to continuous surveillance by guards.

(5) Unannounced audits of POL will be conducted at least quarterly.

(6) Security planning will be conducted per AR 525–26 and DODD 3020.40 when the facility is designated as part of the Defense Critical Infrastructure Program.

3–20. Petroleum, oils, and lubricant not at bulk storage facilities

Property management and accountability directives in paragraph 3–19 will be followed. Risk level I physical protective measures and security requirements in paragraph 3–19 will be implemented. In addition, the following security requirements will be implemented—

a. POL tank trucks containing fuel and that are not under the surveillance of the operator or a dedicated guard force will have—

(1) Locked hatch covers where possible.

(2) Locked manifold access doors.

(3) Each manifold valve secured with a transportation seal if a manifold access door cannot be locked.

(4) Low security padlocks.

b. Fuel pods on vehicles and fuel vehicle tanks will be secured with approved low security padlock or have the commercial locking devices engaged when the vehicles or tanks are carrying fuel and are not under the surveillance of the operator.

c. Fuel-carrying vehicles will be parked in lighted areas of airfields or in motor pools protected by locked perimeter barriers or guards.

d. Dome covers and manifold system shutoff valves of tanker rail cars with POL products aboard will be locked when they are located on an installation for unloading and when POL handling personnel do not have the equipment under surveillance. Rail cars with packaged POL products aboard will be secured by locking all doors.

e. Packaged POL not onboard a vehicle or rail car will be safeguarded in a structure meeting the standards in appendix B. To increase the security posture above minimum, the area may be protected by lighting, a perimeter fence, guards, or an IDS. The need for implementing these additional measures will be determined by vulnerability risk assessment prepared by the physical security officer.

f. Keys to POL storage areas, equipment, buildings, vehicles, and protective seals will be controlled per appendix D.

3–21. Facility engineering supply, construction material storage areas, and industrial and utility equipment

a. Property management and accountability directives.

(1) AR 420–1.

(2) AR 735–5.

b. Physical protective measures (risk level I).

(1) Storage buildings will meet the secure storage structure requirements in appendix B.

(2) Buildings storing supplies and portable construction material, and outside storage areas will be lighted during the hours of darkness.

(3) Outside storage areas will be enclosed by a perimeter fence.

(4) Points of issue will be kept to a minimum.

(5) Signs will be posted at facility entrances stating "Off Limits To Unauthorized Personnel."

c. Physical protective measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Easily pilferable items will be separated from other supplies and construction material and stored in a separate room, building, or container with controlled access.

d. Physical protective measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) An IDS will be installed if the storage building is fully enclosed.

(3) Landscaping features greater than 1 foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

e. Security procedural measures (risk level I).

(1) Access to the facility and to keys, padlocks, and protective seals protecting access will be controlled.

(2) Supplies will be issued only to authorized persons with a signed DA Form 1687 (Notice of Delegation of Authority-Receipt for Supplies) on file.

(3) Incoming shipments of supplies will be checked upon receipt.

(4) Work orders will be reviewed to determine if the recipient has requested excessive supplies for the job to be done.

(5) Entry of privately owned vehicles will not be permitted in storage areas unless it is approved based upon the judgment of the responsible commander.

(6) Annual inventories of all stocks will be made. A copy of the inventory will be kept until the next inventory.

(7) Conduct end-of-day security checks using SF 701.

f. Security procedural measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Small, easily pilferable items identified by the unit commander, will be inventoried once each month. A copy of this inventory will be kept, either until the following month or in accordance with the supply series of regulations, depending on which is more restrictive. .

(3) Bulk packaged items securely crated, banded, or sealed will remain in their original configuration and not broken until they are issued.

g. Security procedural measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) Access to storage areas will be limited to facility personnel authorized to issue the stockage.

(3) The storage building and outside storage areas will be checked at least every 4 hours by a roving guard during hours that the facility is not operational and recorded using the SF 702.

3–22. Audiovisual equipment, training devices and sub-caliber devices at training support centers

a. Property management and accountability directives.

(1) AR 190–11.

(2) AR 710–2.

(3) AR 735–5.

(4) DA Pam 710–2–1.

b. Training devices. Any training device that can be used to fire a projectile or explosive defined as an ammunition or explosives in AR 190–11 will be protected per the standards prescribed in AR 190–11.

c. Physical protective measures (risk level I). Equipment will be secured and maintained in accordance with the requirements required by its CIIC.

(1) Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

d. Physical protective measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) Audiovisual equipment and portable, high-value sub-caliber devices and training aids will be separated from other equipment and stored in a secure, separate container, room, or building with controlled access, Equipment will be secured and maintained in accordance with the requirements required by its CIIC.

(3) Equipment will be located in the interior of the facility as far from the exterior as possible.

e. Physical protective measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) The facility will be lighted during the hours of darkness.

(3) An IDS will be installed in the facility.

(4) Landscaping features greater than 1-foot in height and other features which may obstruct views around the facility and provide concealment for aggressors will be eliminated within 20 feet of the facility.

f. Security procedural measures (risk level I).

(1) Access to the facility and to keys, padlocks, and protective seals will be controlled.

(2) Audiovisual equipment and portable, high-value sub-caliber devices and training aids will be inventoried as indicated in AR 710–2. A copy of the inventory will be kept until the next inventory.

(3) Conduct end-of-day security checks using SF 701.

g. Security procedural measures (risk level II).

(1) Measures required for risk level I will be implemented.

(2) The inventory check-out point will be next to the training support center (TSC) exit to preclude personnel from remaining in the center when equipment has been checked out.

(3) Access to the equipment storage area will be limited to TSC personnel authorized to issue the equipment.

(4) The TSC will maintain separate property book accountability for all equipment.

h. Security procedural measures (risk level III).

(1) Measures required for risk levels I and II will be implemented.

(2) The TSC will be checked at least once every 4 hours by a roving guard after duty hours and recorded using the SF 702.

3–23. Audiovisual equipment, training devices and sub-caliber devices not at training and audiovisual support centers

Risk level I physical protective measures and the security requirements in paragraph 3–22 will be implemented.

3–24. Public and privatized utilities located on government-owned property

a. Utility systems that serve the Army are mission essential vulnerable areas per AR 190–13. The MEVA designation is applicable to all utility services, regardless of ownership or operation, to include Army-owned, privately owned, transferred by utilities privatization, and government-owned/contractor-operated resources. Utility systems include natural gas, water, wastewater, electricity, and communications services and infrastructure for distribution, generation, and treatment facilities.

b. At a minimum, MEVA designation is required for—

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

(2) Utility distribution systems to include tank farms, supply points and distribution hubs, and water sources, water treatment facilities.

(3) Communications facilities to include Network Enterprise Centers.

c. The resource owner will implement and sustain the following:

(1) *Protective measures (risk level I).*

(a) Provides fencing to the extent feasible.

(b) Provides locks to all structures and other resource items.

(c) Control access to the utility at all times.

(d) Control keys and locks.

(e) Designate as a restricted area per AR 190–13.

(2) *Protective measures (risk level II).*

(a) Implement all risk level I measures.

(b) Check unattended utilities at intervals not to exceed every 8 hours.

(c) Illuminate at night in accordance with restricted area lighting guidance in UFC 3–530–01 to allow detection of intruders.

(d) Establish a 20-foot wide clear zone on the inside and outside of the fence to the extent feasible, and keep it clear of obstacles, topographical features and vegetation greater than 1-foot in height.

(3) *Protective measures (risk level III).*

(a) Implement all risk level I and II measures.

(b) Check unattended utilities at intervals not to exceed every 4 hours and recorded using the SF 702.

(c) If the utility is located within a structure, the structure will meet the requirements of a secure storage structure for this risk level per appendix B. In cases where the utility requires ventilation, coordinate with engineers to ensure both ventilation and secure storage structure standards are maintained.

(d) Consider adding IDS if the utility is located within a structure.

d. The supporting garrison—

(1) Provides a risk analysis to the utility owner regardless if the utility is public or privatized.

(2) Conducts a physical security inspection per AR 190–13 regardless if the utility is public or privatized.

(3) For government-owned/contractor-operated or privatized utilities, coordinates with the supporting contracting officer to address physical security deficiencies or other issues, in coordination with the contracting officer's representative which is typically assigned to the Directorate of Public Works.

(4) For government-owned/contractor-operated or privatized utility operations, adherence to physical security requirements will be incorporated into contract quality assurance surveillance plans for periodic review.

3–25. Air items and airdrop systems, and personnel and cargo parachute systems including associated ancillary items

a. Airdrop systems are parachute systems for personnel and cargo airdrop. They include military type-classified and COTS parachute systems, intended for use in the premeditated airdrop of personnel, supplies, and equipment. These items and systems include associated ancillary air items such as aviator breathing oxygen equipment and electronic automatic opening devices. They are portable life-sustaining precision equipment by nature of their implementation.

b. Property management and accountability directives.

(1) AR 710–2.

(2) AR 735–5.

(3) DA Pam 710–2–1.

c. Physical protective measures (risk level I).

(1) Personnel items and systems. Provide double barrier (see glossary) protection for the items and systems at the custodial rigger facility when not in use and while in training in non-tactical environments as follows:

(a) Locked in a secure storage structure per appendix B.

(b) Lock items and systems in a steel cage, approved container, room, bin, drawers, or cabinets as the required second barrier while in a secure storage structure. Extend steel caging, if used, to the ceiling or enclose with a top of like material per appendix B.

(c) Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

(d) Locked in a secure storage structure per appendix B.

(e) Lock items and systems in a steel cage, approved container, room, bin, drawers, or cabinets as the required second barrier while in a secure storage structure. Extend steel caging, if used, to the ceiling or enclose with a top of like material per appendix B.

(f) Post signs at activity entrances announcing that the area is off limits to unauthorized personnel.

(g) Illuminate the exterior of secure storage structure buildings during the hours of darkness.

(2) Personnel items and systems in transit on/off installations. Secure items and systems while in transit away from the originating custodial rigger facility or off the military installation as follows:

(a) Post one guard for every three vehicles when stationary if use is within 24 hours after issue and use is on the originating installation.

(b) Post one guard for every three vehicles directly involved with transportation if use exceeds 24 hours after issue and the location of use is off the military installation utilizing military transportation.

(c) No guard is required if vehicles are parked within an area that meets the double barrier protection.

(d) Secure containers with security seals if use exceeds 24 hours after issue and the location of use is off the military installation utilizing commercial transportation.

(e) Lock systems in a secure storage structure or container per appendix B if use exceeds 24 hours after issue and the location of use is off the military installation and requires interim storage.

(f) Post one guard per aircraft when in transit by air and property is not locked in a steel cage or approved secured container within the aircraft.

(g) Post one guard per aircraft or off-loaded to a steel cage or approved secure container per appendix B when in transit by air and interim storage is required.

(h) Lock items and systems in a secure storage structure (building) and approved container(s) as outlined in appendix B at all interim storage locations.

(i) Secure items and systems in containers with security seals per appendix B when in transit by rail and or vessel.

(3) Cargo items and systems at the custodial rigger facility. Provide double barrier protection for items and systems such as cargo parachutes and select precision ancillary equipment (not including airdrop platforms) when not in use as follows:

(a) Locked within a secure storage structure (building) per appendix B.

(b) Lock items and systems in a steel cage, approved container, room, bin, drawers, or cabinets as the required second barrier while in a secure storage structure.

(c) Extend steel cages to the ceiling or enclose with a top of like material per appendix B.

(d) Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel." Post signs at structure or area entrances announcing that the area is off limits to unauthorized personnel.

(e) Illuminate the exterior of secure storage structure buildings or storage areas during the hours of darkness.

(4) Cargo items and systems not at the custodial rigger facility. Protect these items and systems such as airdrop platforms, not including cargo parachutes, as follows:

(a) Lock in secure storage structure (building) per appendix B.

(b) Provide a perimeter barrier such as fencing when stored outdoors and lock the barrier during nonoperational hours.

(c) Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel." Post signs at activity entrances announcing that the area is off limits to unauthorized personnel.

(5) Cargo parachutes and select precision ancillary equipment not including airdrop platforms. Protect these items while in transit or in use away from originating installation custodial rigger facility as follows:

(a) Lock in a container(s) with security seal(s) while in transit regardless of transit mode.

(b) Post one guard per aircraft when in transit by aircraft and the property is not locked in a steel cage or approved secured container within the aircraft.

(c) Lock items in a container(s) and place in a secure storage structure (building) at final or interim destinations.

(6) Airdrop platforms not including cargo parachutes. Physical protective measures are not required for these items while in transit regardless of transportation mode. If, however, these items are off-loaded at an in-transit interim stop or off-loaded at the final destination, they will be secured as follows:

(a) Lock in a container(s) and place in a secure storage structure (building).

(b) Provide a perimeter barrier such as fencing when stored outdoors and lock the barrier during non-operational hours.

(7) Rigged airdrop loads. Door bundles, container loads, ram-air cargo loads or anything rigged for premeditated airdrop will be considered a rigged airdrop load. The custodial rigger facility supervisor or facility supervisor will determine physical protective measures. The supervisor will consider the following factors at a minimum:

(a) The highest level of property sensitivity contained in the airdrop load.

(b) Physical protective measures of the property versus a fixed or austere staging/rigging environment.

(c) Volatility of load content such as ammunition and fuel.

(d) Load security classification.

(e) Inspections, storage, and shipments. Compliance to standards in relevant TM 10–1670 series publications is mandatory for all air items and airdrop systems.

d. Physical protective measures (risk level II).

(1) Implement all risk level I measures.

(2) Conduct periodic 100 percent inventories. Maintain the inventory record until completion of the next inventory.

(3) Safeguard aerial delivery items during shipment at all times to prevent illegal use and pilferage.

e. Physical protective measures (risk level III).

(1) Implement all risk level I and II measures.

(2) Eliminate landscaping features greater than 1-foot in height and other features that may obstruct views and provide concealment for aggressors within 20 feet of the originating installation custodial rigger facility.

f. Security procedural measures (risk level I).

(1) Control access to equipment storage areas.

(2) Control access to keys, padlocks, and protective seals per appendix D.

(3) Issue portable, pilferage–coded items temporarily assigned to a user on a hand receipt or a locally devised temporary receipt.

(4) Check unattended storage facilities at least every 4 hours when items are issued for more than 24 hours or when interim storage is required and recorded using the SF 702.

(5) Conduct routine serviceability inspections per relevant TM 10–1670 series publications, or applicable manufacturer, or relevant Federal Aviation Administration publication by a current and qualified Parachute Rigger (military occupational

specialty (MOS) 92R/921A) when air items including COTS items are issued from the custodial rigger facility for more than 72 hours.

(6) Conduct in-storage inspections per the relevant TM 10–1670 series publication by a qualified Parachute Rigger (MOS 92R/921A) when items are stored away from the originating installation custodial rigger facility.

(7) Provide IDS in all facilities constructed after 2014 for the purpose of storing air items and airdrop systems.

(8) Conduct end–of–day security checks using SF 701.

g. Security procedural measures (risk level II).

(1) Implement all risk level II measures.

(2) Prohibit privately owned vehicles from being parked within 50 feet of the storage facility. Post signs announcing this prohibition.

(3) Conduct periodic 100 percent inventories. Maintain the inventory record until the next inventory is completed.

(4) Escort personnel entering the facility that are not assigned to the activity.

h. Security procedural measures (risk level III).

(1) Implement all risk level I and II measures.

(2) Conduct monthly 100 percent inventories. Maintain the inventory record until the next monthly inventory is completed.

(3) Either garrison or unit personnel will check the originating installation facility at least every 2 hours after normal operating duty hours.

(4) Guards will continuously secure items and systems that are in transit or in use while away from the originating custodial rigger facility either on or off the installation.

Section III

Minimum Security Standards for Resources Not Requiring Risk Analysis

3–26. Critical communications facilities

These facilities process, transmit, and receive telecommunications traffic determined to be a defense critical infrastructure capability or crucial by the President of the United States. They include nuclear weapon delivery units and storage facilities, main operating bases for allied air forces, and primary command and control elements. These standards apply to facilities located on and off military installations and also mobile systems. Because of the difference in location, physical layout and equipment, security considerations must be thoroughly assessed for each communications system, and tailored to that particular facility or system. Protection will be sufficient to maintain continuity of operations of critical users and the facilities they support.

a. The senior commander is responsible for site security and will establish supporting relationships with the nearest DOD installation, host nation, and local law enforcement and intelligence agencies.

b. The supporting installation will provide a level of support common to all tenants.

c. Access to the facility will be controlled and only authorized personnel will be allowed entry.

d. Facilities will be designated and posted as a restricted area, as a minimum.

e. Depending on regional conditions, commanders should consider maintaining sufficient weapons and ammunition at a facility to arm designated personnel.

f. Essential structures should be hardened against attacks per UFC 4–010–01. This includes large antenna support legs, antenna horns, operations buildings and cable trays. Future construction programs for communications facilities should include appropriate hardening of essential structures.

g. Security planning will be conducted per AR 525–26 and DODD 3020.40 when the facility is designated as part of the Defense Critical Infrastructure Program.

3–27. Small unmanned aircraft systems, hand tools, tool sets and kits, and shop equipment

a. Property management and accountability directives.

(1) AR 710–2.

(2) AR 735–5.

(3) DA Pam 710–2–1.

b. Tool sets and kits with lockable tool boxes. These items, when not in use, will be secured with a key operated lock, consisting of either a low security padlock per appendix D factory-installed key operated tumbler-type lock. The person signing for the set or kit will retain the key. A duplicate key will be held by the supervisor or commander/director if it is stored in a locked container with controlled access.

c. Tier I small unmanned aircraft systems, portable hand tools, tool sets or kits, and shop equipment. These items, when not in use and not under the surveillance of a responsible person (for example, user, tool room keeper, or guard), will be stored in accordance with their CIIC. At a minimum non-portable items will be secured in the building or van in which they are located. Secure locations for portable items include—

(1) A locked building or room meeting the requirements for a secure storage structure in appendix B locked metal cage in a secured building.

(2) A locked built–in cabinet, bin, or drawer in a secure room or building.

(3) A locked drawer or compartment of a furniture item (for example, wall locker or desk) in a secure room or building.

(4) Attached to the building structure with a 5/16-inch chain or equivalent cable and a low security padlock or permanently fastened to a working surface.

(5) Locally fabricated, lockable racks that, when locked, prevent tool box lids from being opened or individually placed larger tools from being removed.

(6) A locked enclosed truck, van, armored vehicle, or vehicle trunk.

(7) A locked vehicle equipment box or secured, either directly, or in a locked container, to the vehicle itself.

(8) A locked CONEX container.

d. Common tools and portable shop equipment. These items, when not on hand receipt to a user, will be controlled in accordance with DA Pam 710–2–1. Tool checks (metal disks that can be stamped or etched with a mechanic's identification) are available in supply channels under national stock number (NSN) 9905–00–473–6336.

e. Access. Access to tools and shop equipment will be controlled in accordance with DA Pam 710–2–1. If possible, access will be limited to the user, the person designated as responsible for security items when not in use.

f. Keys and locks used to safeguard tools. Keys, locks, and protective seals used to safeguard hand tools, tool sets or kits, shop equipment, and the facilities on which they are stored or located will be controlled and accounted for per appendix D. Master–keyed or keyed–alike locksets will not be used to secure these items.

g. Special accountability. Hand tools with a nonmilitary application that are particularly subject to improper use will be placed under special accountability.

h. Marking. All hand tools will be marked with the unit or unit designation for accountability.

i. Resources. High-value hand tools, tool sets and kits, and shop equipment stored at USAR and ARNG facilities will be protected by IDS where it is feasible and logical to do so.

3–28. Unit supply rooms

a. A unit supply room will be a locked room which, as a minimum, meets the secure storage structure standards in appendix B or will be a locked metal cage in a secured building. Security lighting, fencing, or other protective measures may be warranted based on risk analysis.

b. Access to items stored in the supply room will be controlled at all times by the supply noncommissioned officer or other designated person using lock and key control security requirements in accordance with appendix D.

c. Signs will be posted that state, "Off Limits to Unauthorized Personnel."

d. Bolt cutters will be controlled and accounted for per appendix F.

3–29. Postal unique items

Minimum security standards will be per DOD 4525.6–C and/or DOD 4525.8–M.

3–30. Minimum security standards for office machines

a. Buildings, rooms, and offices in which office machines are located will be secured whenever an individual permanently assigned to the activity is not present. Security will consist of closing and locking appropriate doors and windows, as a minimum.

b. Automated systems, including word processing systems, will be secured per AR 25–1. Cable locks are recommended for laptop computers.

c. When size and weight allow, small office machines such as hand-held calculators and portable computers will be locked in a desk or cabinet.

3–31. Stand-alone facilities

For the purpose of this regulation, a SAF is a facility not located on a military installation, often located within a community or collocated in municipalities which lack sufficient security to protect personnel and assets.

3–32. Controlled cryptographic items

a. Property management and accountability directives.

(1) AR 710–2.

(2) AR 710–3.

(3) AR 725–50.

(4) AR 735–5.

(5) AR 740–26.

b. Controlled cryptographic items protective measures. Controlled cryptographic items (CCIs) are high-value, sensitive U.S. Army property which require protection against unauthorized access because they contain an embedded logic which performs cryptographic functions. Access in this instance means uncontrolled physical possession which gives the opportunity to obtain detailed knowledge of the CCI. The security protective measures and requirements addressed in paragraphs 3–32*c* and 3–32*d* establish minimum standards for controlling access to CCI (installed or uninstalled) to protect against tampering, loss, and unauthorized use and apply only to unkeyed CCIs which are unclassified. Installed CCIs, for the purposes of this regulation, means the equipment on hand that has been set up and is available for use to perform its design function for authorized users. Uninstalled means on hand but not set up for use. Keyed CCIs are classified and will be protected per AR 380–40. Commanders should provide the same or equal security protection for unclassified CCIs as is given to other high-value unclassified U.S. Army assets and should apply the risk analysis principles in DA Pam 190–51 to assist in determining appropriate acceptable risks and safeguards.

c. Physical protective measures for unattended controlled cryptographic items.

(1) CCI which is not under continuous surveillance by an individual permanently assigned to the activity will be provided protection consisting of—

(a) A building or room where the doors, windows, and other means of entry and exit can be locked or secured and physical access controlled.

(b) A locked, enclosed van, trailer, armored vehicle, or aircraft protected by a perimeter fence.

(c) Securing the items directly to tactical vehicles by a locally fabricated method and providing perimeter fencing when removal and storage in a secure room or building is impractical.

(2) Aircraft and vehicles containing CCIs will be parked and protected as indicated in paragraphs 3–9, 3–10, and 3–11.

(3) When commanders select double barrier protection for CCIs, the building or room being used as one barrier does not have to be a secure storage structure as indicated in appendix B.

(4) "Off Limits to Unauthorized Personnel" signs will be posted at the activity entrances.

(5) At risk level II, lighting will be provided for the exterior of the building or the site perimeter.

(6) At risk level III, IDS, or continuous surveillance is required.

d. Attended. CCI which is under continuous surveillance and control of an individual permanently assigned to the activity does not require any additional physical protective measures as safeguards.

e. Security procedural measures.

(1) Access to the facility or area will be controlled per this regulation. Physical access will be limited to authorized individuals.

(2) Access to keys and locks protecting CCIs will be controlled per appendix D.

(3) Periodic command–directed inventories will be conducted per AR 710–2.

(4) The facility or vehicle parking area will be checked by guards at least every 2 hours.

(5) A standing operating procedure (SOP) which includes instructions for safeguarding CCIs, controlling access to and use of CCIs, and reporting of incidents of loss or tampering, as a minimum, will be published.

Chapter 4
Security of Medical and Medical Research Resources

Section I

General

4–1. General
This chapter establishes policy, procedures, and minimum physical security standards for the safeguarding and storage of controlled medical substances and medically sensitive items.

4–2. Security checks
a. All isolated structures having controlled medical substances or medically sensitive items will be checked every 4 hours. Facilities within hospitals or other medical or research, development, test, and evaluation facilities, complexes, or structures may be checked by duty officers or other duty, medical, or unit personnel. When the medical or research, development, test, and evaluation facility is not occupied, security checks will be conducted at irregular intervals not to exceed every 4 hours to avoid establishing a pattern and recorded using the SF 702. The frequency of checks will be every 4 hours during nights, weekends, and holidays to provide for deterrence and early detection of entry. Security checks are not required if an operational IDS is present.

b. Particular attention will be directed to windows, doors, other points of possible entry, and locking devices.

c. All instances of suspected theft, loss, illegal entry, open or unlocked facilities or containers, and other incidents of a suspicious origin will be reported immediately to designated authorities. Surveillance will be maintained until responding personnel arrive at the scene.

4–3. Intrusion detection system and security lighting
a. Where IDS is required in this chapter, the IDS will consist of at least two types of sensors, a means of alarm annunciation at a monitoring location from which an armed response force can be dispatched, and electronically supervised circuitry between the two. The IDS will be designed in accordance with UFGS 28 10 05.

(1) If the resources are entirely within a container, detection may include a capacitance sensor on the container itself.

(2) If the resources are not entirely within a container, IDS sensors will be installed so that they detect intruders before a breach is made in any component of the vault, room, or building associated with providing delay. The vault, room, or building will provide delay greater than or equal to the time required for the response force to respond to the alarm.

b. Installation of IDS equipment will be per the applicable UFGS. A duress switch or holdup button will be included when required by Army policy or UFC, and may be considered elsewhere when locale conditions warrant it. The design review requirements of AR 190–13 apply.

c. A SOP for the activation, deactivation, and monthly test of the IDS will be published. The SOP will include instructions for maintaining an accurate IDS log. The DA Form 4930 (Alarm/Intrusion Detection Record) may be used or a comparable electronically-generated document with the same recorded data.

d. Storage areas will be provided operational interior and exterior lighting during the hours of darkness.

e. Where IDS is in use a sign will be prominently displayed warning that this particular area is protected by IDS. The IDS sign specifications in AR 190–11 will be used.

f. A CCTV system may be employed as a means to visually assess an intrusion alarm annunciation. If employed, the system will be installed in accordance with prescribing regulations and funded by command funds using core budget dollars which may be used to purchase, install, and maintain physical security equipment and supplies. ESS not specifically identified as a regulatory requirement by AR 190–17, AR 190–54, or AR 190–59 may be purchased and maintained by commands if the command opts to use these systems. CCTV systems, components, and supporting equipment and well as video telecom systems not required will be funded by commands, not MDEP Physical Security Matters (program QPSM) funds.

4–4. Lock and key control
Security requirements will be established to protect locks, keys, and combinations used to secure facilities, vaults, and containers. The number of personnel having access to locks, keys, and combinations will be the minimum necessary for efficient operations. Provisions of appendix D will be followed in establishing procedures.

4–5. Master keys

Master keys are authorized in Army medical treatment facilities. Spaces controlled by master keys will be segregated per UFC 4–510–01. Master keys will not be removed from the medical facility and will be issued to very limited personnel. Pharmacies entrance keys will be keyed separately from the master key system.

Section II

Security Standards for Controlled Medical Substances (Notes R, Q, and C)

4–6. Reliability of persons having unaccompanied access to controlled medical substances

a. Commander's program. Managing unaccompanied access to controlled medical substances is a commander's program. Commanders/directors must be aware of, and concerned with, the reliability at all times of personnel having unaccompanied access to controlled medical substances. A total team effort and interaction is necessary for this program to be successful.

b. 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/director retains the responsibility to review decisions to qualify or disqualify personnel. The commander/director will issue a written delegation of authority by memorandum for a certifying official who will have responsibility for the determination process.

c. 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 assist the certifying official in the continuing evaluation of personnel, but ultimately the decision to qualify or disqualify rests with the commander by means of the delegated certifying official.

d. Supporting form. The DA Form 7708 (Personnel Reliability Screening and Evaluation Form) will be used to document the process of determining the reliability of persons that are projected to have unaccompanied access to controlled medical substances, and continued evaluation of persons already having such access. AR 190–13 provides instructions for completing the DA Form 7708. The DA Form 7708 facilitates recording of the—

(1) Results of record checks of personnel, security, medical, law enforcement, and drug test information.
(2) Supervisor briefing to a prospective person.
(3) Continuing periodic evaluations of an incumbent person.
(4) Suspension or temporary disqualification of an incumbent person.
(5) Disqualification of an incumbent person.

e. Responsibility to inform. Supervisors at all levels have an inherent responsibility to inform the commander/director of 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-workers' reliability.

f. 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.

g. Documenting behavior patterns. To ensure commander/directors are aware of patterns of behavior that may indicate unreliability, commands/activities should establish a system to include documentation related to discipline of employees in both supervisor and employee records. These records will be periodically reviewed by certifying officials.

h. Security clearance. A security clearance is not required for unaccompanied access to controlled medical substances. However, if the commander/director becomes aware of behavior that may reflect adversely on an employee's loyalty as outlined in AR 380–67, a DA Form 5248–R (Report of Unfavorable Information for Security Determination) will be forwarded forthwith to Commander, U.S. Army Central Personnel Security Clearance Facility (PCCF–M), Fort Meade, MD 20755–5250.

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 AR 190–13.

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

l. Access roster.

(1) An access roster will be posted inside the storage area listing the names, duty positions, and date of full program enrollment of persons authorized unaccompanied access to controlled medical substances, or authorized custody or possession of keys and combinations to locks used to secure controlled medical substances. The list will be checked for accuracy every 30 days, and the check documented in unit files.

(2) Rosters of personnel having access to controlled medical substances contained in point-of-use machines will be maintained in a central, controlled area.

(3) Access to controlled medical substances will be denied to persons undergoing investigation, treatment, rehabilitation, judicial or non-judicial processes, or administrative action as a result of actual or suspected drug use. Access may be reinstated when suspicions or allegations against the person are determined to be unfounded, or when rehabilitation is successful under the provisions of AR 40–68.

4–7. In–transit security of controlled medical substances

Physical security during shipments of controlled medical substances listed in the section II of the glossary will be per the appropriate provisions of AR 40–61 or other Army regulations and command directives. In any event, in-transit security must be such that the spirit and intent of these regulations are not violated and that controlled medical substances are protected from unauthorized possession, use, and theft.

4–8. Disposal of controlled medical substances

Disposal of controlled medical substances will be per AR 40–3, AR 40–5, AR 40–61, and DA Pam 40–11.

4–9. General storage policy for controlled medical substances

a. Facilities, vaults, and containers used for storage of controlled medical substances will not be used for storage of classified material.

b. Schedule I drugs and substances (see glossary) will be secured in the same manner prescribed for Schedule II (Note R) controlled substances.

c. Point-of-use systems and cabinets may be used to secure Note R and Note Q controlled substances.

4–10. Bulk level storage of controlled medical substances

a. Bulk storage of Notes R, Q, and C controlled medical substances will comply with the physical security standards established in this chapter. For the purpose of this policy, bulk storage means storage above the using or dispensing level, and is usually found at the logistics warehouse and depot storage level.

b. Bulk storage requirements also apply to activities other than warehouses and depots having controlled medical substances in amounts that exceed normal operating stocks which are stored in a separate facility (building or room).

c. Bulk storage facilities will be designated and posted as restricted areas. Warning notice signs will be posted in English. In overseas locations, warning notices will also be posted in the host nation language. For both continental United States and overseas locations, the warning notice is also encouraged to be posted in other languages predominant to the area as a safety and legal precaution.

d. Access to storage areas will be strictly controlled at both the bulk storage and dispensing levels.

e. Refrigerated storage of Note Q (Schedule III–V, that is, Ativan syringes) outside or inside of point-of-use dispensers, vault, or security container will be secured in locked containers with padlocks per paragraph D–5*d*.

f. Note R substances will be stored in a General Services Administration (GSA) approved Class 5 container or a vault constructed per paragraph B–3 and using a Class 5–A vault door. For existing facilities where it is not practical to construct a vault per paragraph B–3, a storage site will be constructed per paragraph B–2. Small quantities of Note R substances may be stored in a GSA-approved Class 5 container or in point-of-use cabinets meeting the requirements of AR 40–3.

g. Note Q substances will be stored in secure structures per appendix B or in locked containers. If containers are used, the containers will be locked at all times except during restocking, inventory, or dispensing operations. Dual door protection may be eliminated if the entrance door is as specified in appendix B. General medical items or supplies will not be stored with Note Q items. At a minimum, storage will be in an area that is designated and posted as restricted with the level of protection consistent with the type of item and perceived local threat of theft or diversion to unauthorized use.

4–11. Pharmacy level storage of controlled medical substances

a. Pharmacies containing controlled items will be designated as restricted areas and constructed per paragraph B–2.

b. Pharmacies located in medical treatment facilities will be equipped with IDS per paragraph 4–3. A duress switch will be provided at the dispensing window. Personnel on duty will have access to the duress switch at all times during periods of operation. The IDS will be tested monthly. Coordination will be made with the servicing security force to schedule a test of the IDS. The test results will be annotated on DA Form 4930 or electronic equivalent form, and maintained for 1 year.

c. When operationally feasible, containers of Note R and Q substances will be positioned so as not be readily visible to the public.

d. Note C substances will be stored per Note Q or Note R substances, as applicable.

e. Containers with Note R and Q substances will be locked when access is not required for operational use. Lock and key control requirements prescribed in paragraph 4–4 apply.

f. Pharmacies with controlled medical substances will have interior and exterior lighting of sufficient intensity to enable electronic or visual surveillance by security forces, duty officers, or other designated personnel. Security checks will be conducted on an irregular basis during non-duty hours to avoid establishing a predictable pattern. Particular attention will be directed to doors, windows, and other possible points of entry. Doors will be locked at all times, except when authorized personnel are entering or exiting the pharmacy.

g. A CCTV system will be employed at high-risk facilities for surveillance and intrusion alarm assessment. Core budget dollars may be used to purchase, install, and maintain physical security equipment and supplies.

4–12. Point-of-use level storage of controlled medical substances

a. When authorized personnel are in continuous attendance, dispensing quantities of Note R substances may be stored in double locked containers, in point-of-use machines or automated dispensing systems per paragraph 4–25. If double locked containers are used, they will be constructed so that forced entry is readily apparent to visual examination.

b. When authorized personnel are not in continuous attendance, dispensing quantities of Note R substances will be stored in approved point-of-use containers or GSA-approved Class 5 containers.

c. Dispensing quantities of Note Q substances will be stored per paragraph 4–25. If not operationally feasible, containers constructed of a minimum of 20–gauge steel with a GSA-approved locking device may be used provided additional security measures are in place such as continuous visual surveillance, IDS, lighting, and secured inside a locked room. Level of security measures will be commensurate with the threat, risk, and/or vulnerability.

d. Containers having Note C substances will be secured per paragraph 4–25.

e. Security requirements.

(1) Personnel that inventory and/or stock point-of-use machines with medications to include narcotics will validate complete accuracy and will be monitored by supervisory personnel.

(2) Personnel access rosters for point-of-use machines will be established, posted inside the secured area and kept from public view.

4–13. Safeguards for controlled medical substances during non-duty hours

a. At the close of business, designated duty personnel will perform a security check prior to departure from rooms or facilities in which Notes R, Q, and C items and other controlled substances and sensitive medical items are stored. These security checks will be documented daily on SF 701 and, as a minimum, will make certain that no Note R, Q, and C items remain unprotected or exposed and that they are secured in designated containers.

(1) Containers are locked and checked properly with such action recorded on SF 702.

(2) All windows, doors, and other openings are secured to deter access to rooms in which containers are located.

(3) Other vulnerable equipment or property is stored properly and secured.

b. When duty personnel are not present, continuous surveillance will be provided for all bulk storage areas, buildings, and facilities in which Notes R, Q, and C items are stored. This will be provided by guard personnel or by IDS. A lock and key control program will be established per appendix D to enhance the protection of all storage containers and facilities.

4–14. Crash carts, emergency trays, and ambulances containing controlled medical substances

a. The number of crash carts and emergency trays (essential emergency assemblages) containing controlled medical substances will be kept to a minimum, and will be provided with maximum security consistent with requirements for immediate resource availability.

b. When controlled medical substances are issued to emergency medical team personnel assigned to ambulance or emergency vehicle response duties, the substances will not be stored in the vehicle while it is unattended to the maximum

extent practical. When not in transit or on a call, the ambulance will be checked every four hours when controlled medical substances are aboard.

c. Controlled medical substances aboard ambulances will be secured in a commercially-available lockable storage container having access by means of user-unique personal identification numbers or biometrics and an automated audit trail.

d. Emergency assemblages containing controlled medical substances will be sufficiently protected, but must not hamper ready and authorized visual inspection and immediate removal for use.

e. Accountability and control requirements of AR 40–3 also apply and will be met.

4–15. General security requirements for controlled medical substances

a. Commanders of medical treatment facilities having controlled medical substances will—

(1) Establish written measures to safeguard controlled medical substances at all times.

(2) Issue written appointment order for a physical security officer to make certain appropriate protection of all controlled medical substances per AR 40–3.

(3) Direct the conduct of a physical security inspection in accordance with AR 190–13.

(4) Request, as needed, a U.S. Army Criminal Investigation Command crime prevention survey for the purpose of detecting crime, evaluating the possibilities of easy criminal activity, and identifying requirements favorable to criminal activity.

(5) Report the theft, loss, recovery, or mismanagement of controlled medical substances per AR 190–45. All actual and suspected losses and inventory discrepancies or recoveries will be reported to the proper law enforcement agencies.

(6) Submit serious incident reports per AR 190–45 in the required time limits.

(7) Conduct daily and monthly inventories/audits per AR 40–3 and AR 40–61.

(8) Publish a written plan for the monitoring and surveillance of controlled medical substances accessed through automated medication dispensing systems per AR 40–3.

b. Unaccompanied access. Personnel have unaccompanied access to controlled medical substances provided they are in compliance with the occupational reliability program in paragraph 4–6 and are listed on the access control roster.

Section III

Security Standards for Other Medical Resources

4–16. Human organs and blood products

a. Human organ and blood products storage areas will be attended at all times or secured when authorized personnel are not present.

b. An electronic entry control system will be provided.

c. Keys and keycards will be controlled per appendix D and limited to the minimum number of personnel for operational necessity.

d. Access will be controlled at all times.

e. Signs will be posted at the activity entrances stating “Off Limits To Unauthorized Personnel.”

f. Surgical instruments will be secured when not in use.

g. Exterior lighting will be provided.

h. End-of-day security check requirements will be established, and actions recorded on SF 701.

i. Windows will be equipped with locking devices. Exterior windows located within 18 feet of the ground that provide entry will be provided with protective coverings that may consist of rods, bars, screens, or constructed of materials offering equivalent level of protection against forced penetration and burglary attempts. Openings greater than 96 square inches will be covered with screens or covers to prevent undetected and unauthorized entry.

j. Exterior openings such as windows will be secured with heavy gauge screens, bars, or be constructed of material offering equivalent level of protection against force entry attempts if the room is on the ground floor and shares the building exterior wall.

4–17. Radioactive materials

a. Radioactive materials storage areas will be controlled at all times, and secured when authorized personnel are not present.

b. An electronic entry control system will be provided.

c. Access will be controlled at all times.

d. Signs will be posted at the activity entrances stating “Off Limits To Unauthorized Personnel.”

e. Keys and keycards will be controlled per appendix D and limited to the minimum number of personnel for operational necessity.

f. Exterior lighting will be provided.

g. Stringent inventory requirements will be established per AR 385–10, DA Pam 385–24, and U.S. Army Medical Command supplemental policies.

4–18. Treasurer's office

a. Keeping and safeguarding public funds and related documents will be per DOD 7000.14–R, Volume 5, Chapter 3.

b. Cashier offices in a medical treatment facility will be constructed per UFC 4–510–01.

c. Written requirements will be established for handling and safeguarding cash instruments and confirm familiarity with those requirements by all employees. Requirements will address maintaining minimum cash on hand for cashiers, inventories, and duress requirements.

d. An electronic entry control system will be provided.

e. Access will be controlled at all times.

f. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

g. Keys and keycards will be controlled per appendix D of this regulation, and limited to the minimum number of personnel for operational necessity.

h. An intercom, small security window, or door viewer will be provided at entrance doors.

i. An IDS will be provided and monitored at a central location that can dispatch a response force. The IDS will include a duress alarm at dispensing windows.

j. Exterior lighting will be provided.

k. UFC 4–510–01 provides additional guidance for securing fund handling activities.

l. Windows will be equipped with locking devices. Exterior windows located within 18 feet of the ground that provide entry will be provided with protective coverings that may consist of rods, bars, screens, or constructed of materials offering equivalent level of protection against forced penetration and burglary attempts. Openings greater than 96 square inches will be covered with screens or covers to prevent undetected and unauthorized entry.

4–19. Emergency departments

a. Stringent security measures will be provided to the extent feasible without disrupting patient care due to the potential for violent behavior in emergency departments.

b. Security personnel will be posted in the emergency department when practical. If unable to do so, coordinate with law enforcement or security personnel for recurring patrol stops at the emergency department.

c. A secure area will be established to control access to patients awaiting medical care.

d. Only emergency vehicles will be allowed to park in designated areas.

e. Furniture will be secured to the floor.

f. Exterior doors will be configured so they cannot be opened from the outside without authorization.

g. An intercom system and a door control system will be provided to control access. (Funded by core budget dollars).

h. Make certain that walk-in patients report to a reception desk equipped with a duress switch that is tested monthly.

i. Designate a room (see detention ward) to secure volatile persons that pose a high risk for violence.

(1) The room will be located to avoid observation by other personnel to the extent feasible.

(2) Law enforcement or security personnel will remain with the person until treated and released or admitted. If admitted, the hospital commander will coordinate with supporting law enforcement personnel to guard the person if it becomes necessary.

4–20. Maternity wards

For the purpose of this regulation, the term maternity ward encompasses all aspects of newborn care including neonatal care, labor and delivery, neonatal intensive care, post partum wards, pediatric wards, pediatric intensive care units, newborn clinics, mother-baby wards, nursery labor and delivery, and post partum pediatric oncology wards.

a. Access will be controlled at all times.

b. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

c. An electronic entry control system will be provided (funded by core budget dollars).

d. Keys and keycards will be controlled per appendix D of this regulation, and limited to the minimum number of personnel for operational necessity.

e. Staff personnel will wear security badges that identify them as maternity ward staff.

f. An infant monitoring and pediatric abduction prevention system will be installed. The system will alert security and hospital personnel if a child is removed without authorization. The system will be capable of securing facility doors and elevators (funded by core budget dollars).

g. Develop written procedures to use in the event of abduction. Verify that all medical treatment facility personnel are familiar with the procedures. The procedures will be practiced annually.

h. A separate visitor area will be established. Authorized visitors may be admitted after verification.

i. Other security provisions per AR 40–400 will also be employed.

4–21. Medical supply storage areas

a. Access will be controlled at all times.

b. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

c. Keys and keycards will be controlled per appendix D of this regulation, and limited to the minimum number of personnel for operational necessity.

d. Storage areas/rooms securing high-value items or highly pilferable items will meet the construction requirements in appendix B for secure storage facility. Tools such as screwdrivers, bolt cutters, and crowbars that can be used to circumvent security will be secured when not in use.

e. Exterior lighting will be provided.

f. End-of-day security checks will be conducted and recorded on SF 701.

4–22. Precious metals

a. Precious metals in any form will be secured against theft, loss, or damage consistent with their monetary value and difficulty of replacement.

b. At a minimum, precious metals will be secured in a GSA-approved Class 5 container (funded by core budget dollars).

4–23. Sterilized surgical instruments

a. Instruments will be secured in a locked container when not in use, or placed under constant observation.

b. Monthly inventories will be conducted and discrepancies resolved.

c. An information technology-based medical instrument tracking system may be used.

4–24. Surgical suites and oral surgery laboratories

a. Access will be controlled at all times.

b. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

c. An electronic entry control system will be provided (funded by core budget dollars).

d. Rooms will be secured when not occupied by authorized personnel.

e. Keys and key cards will be controlled per appendix D and limited to the minimum number of personnel needed for operational necessity.

f. Exterior lighting will be provided.

g. Exterior opening such as windows will be secured with heavy gauge screens or bars if the room is on the ground floor and shares the building exterior wall.

h. Windows will be equipped with locking devices. Exterior windows located within 18 feet of the ground that provide entry will be provided with protective coverings that may consist of rods, bars, screens, or constructed of materials offering equivalent level of protection against forced penetration and burglary attempts. Openings greater than 96 square inches will be covered with screens or covers to prevent undetected and unauthorized entry.

4–25. Point-of-use machines and automated dispensing systems

a. Point-of-use machines and automated dispensing systems will be locked unless dispensing, or undergoing inventory, restocking, or maintenance, when located in controlled access rooms.

b. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

c. An electronic entry control system will be employed.

d. A CCTV system may be employed (funded by core budget dollars).

e. Exterior lighting will be provided.

f. A personnel access roster will be posted inside the secured area and kept from public view.

g. Authorized personnel will provide constant observation of point-of-use machines and automated dispensing systems when the room is unsecured.

h. See paragraph 4–12 for additional requirements for point-of-use machines and automated dispensing systems containing controlled medical resources.

i. Security requirements will be developed for inventory and stocking accuracy. A supervisor will verify inventory and stocking by signing and dating appropriate accountability documents.

j. Personnel will secure access codes per AR 25–2.

4–26. Behavioral health areas

For the purpose of this regulation, behavior health areas are those areas set aside for inpatient behavioral health treatment and intensive outpatient treatment within a hospital.

a. Areas will be able to be secured on command.

b. Furniture will be secured to the floor.

c. Authorized staff personnel will wear security badges.

d. A duress signaling capability will be provided to staff members for all patient areas. Duress buttons will be tested monthly and the results annotated in a logbook.

e. Keys and keycards will be controlled per appendix D and limited to the minimum number of personnel for operational necessity.

4–27. Detention wards

A detention ward provides for long term care of personnel injured during the alleged commission of a criminal act.

a. A secure room will be provided for long term care of detained personnel. Locate the room away from other patients while still providing continuous observation, to the extent feasible.

b. Access will be restricted to authorized medical personnel. Legal and religious personnel may obtain access, as needed, but will be issued a visitor badge. Off-site law enforcement personnel when not responding to emergencies will require a visitor pass.

c. Signs will be posted at the activity entrances stating "Off Limits To Unauthorized Personnel."

d. Ward construction will be supplemented with impact resistant material. Locks, keys, and key cards will be controlled per appendix D and limited to the minimum number of personnel needed for operational necessity.

e. Access will be controlled at all times by an electronic entry control system.

f. Competent medical authority will determine the use of restraints.

g. Family members will be authorized to visit per the medical authority or servicing legal counsel office. Security personnel will monitor the visit in keeping with legal confidentiality requirements.

h. For long term care, security will be provided by the servicing law enforcement organization or the detainee's military unit. Hospital security personnel may be utilized to provide additional support, but are not required to provide primary supervision.

4–28. Ambulances

a. While parked and not in operation, the vehicle will be secured by engaging commercial locking devices. The ambulance will be parked in an area that is under constant observation, if possible.

b. All medical kits including those containing controlled medical substances that are stored in the vehicle will be secured. If it does not affect medical readiness, remove the kit containing the controlled medical substances and place it in a secure location.

c. The vehicle operator will retain vehicle keys after stopping at the scene of a medical emergency. Ambulances equipped with an ignition disabling device are exempt from vehicle operator key retention.

4–29. Warrior transition units

a. A CCTV system will be provided and monitored from a central location that can dispatch a response force (funded by core budget dollars).

b. The CCTV system will be strictly limited to common use areas.

c. Written requirements will be established for the security of digital media, access to system components, length of time to maintain recordings and authority to view recordings, at a minimum.

4–30. Community-based medical homes

a. Community-based medical homes are Army-run primary care clinics located off-post in communities supporting Army Families.

b. A memorandum of agreement will be established between the clinic's senior commander and civilian emergency management for IDS monitoring, law enforcement response, fire response, and other related emergency cooperative measures.

c. Minimum physical security measures and security procedural measures for medical resources prescribed in the chapter will be applied.

4–31. Patient information

Patient information will be protected per the Health Information Portability and Accountability Act of 1996, AR 40–400, and AR 40–66.

a. Rooms containing patient information will be—

(1) Access will be controlled at all times by an electronic entry control system.

(2) Secured when not occupied by authorized personnel.

(3) Establish end-of-day security checks and record on SF 701.

(4) Locks, keys, and key cards will be controlled per appendix D and limited to the minimum number of personnel needed for operational necessity.

b. Information systems containing patient information will be—

(1) DOD common access card-enabled.

(2) Continuously staffed or secured by removal of the common access card.

(3) Evaluated for emanations security similar to the process provided in AR 380–27.

(4) Containers having patient information will be locked when authorized personnel are not in attendance.

4–32. Medically sensitive items

a. Unused needles and syringes and other medically sensitive items will be stored in a locked container. Keys to these cabinets will be controlled per appendix D.

b. Used and unused needles and syringes will not be stored in the same cabinet or container. Pending final destruction, used needles and syringes may be temporarily stored in closed one–way puncture resistant receptacles such as Sharps containers that must be of a tamper–resistant design and must be either—

(1) Locked to a mounting device which is securely fastened to the building structure.

(2) Located in a room or area which is locked or under continuous visual surveillance of ward or clinic personnel.

Section IV

Security Standards for Non-Biological Select Agents and Toxins Infectious Agents and Toxins

4–33. General

These standards only apply to non-biological select agents and toxins infectious agents and toxins (IAT). (See AR 190–17 for security standards for biological select agents and toxins.) IAT security is a mature concept in biological research and medical laboratories. Several of the security measures in this section are embedded in the biosafety levels that serve as the foundation for good laboratory practices throughout the biological laboratory community. Security requirements aid in the prevention of accidental or incidental access to IATs and complement safety requirements. Presumptive non-biological select agents and toxins samples will be secured in accordance with biosafety level 3 requirements. The following security standards, however, are oriented towards external threats and are intended to prevent unauthorized IAT removal.

4–34. Minimum security standards

The following physical protective measures and security procedural measures will be implemented—

a. Biosafety level 1.

(1) Access to IAT rooms or suites will be limited to designated personnel having an operational need.

(2) Rooms arranged as a suite having a common access door will be secured at the common access door when not attended.

(3) An end-of-day security check of rooms/suites will be conducted and recorded on a SF 701.

(4) Key and lock requirements for access to rooms/suites and to keys, locks, and protective seals protecting resources will be controlled per appendix D.

(5) Signs will be posted at entrances to rooms/suites stating "Off Limits To Unauthorized Personnel."

(6) IAT containers will be locked when unattended.

(7) A security plan will be prepared and integrated into the overarching laboratory/hospital physical security plan.

(8) Inventories will be scheduled and conducted per guidance issued by the Office of the Surgeon General.

b. Biosafety level 2.

(1) Measures required for biosafety level 1 will be implemented.

(2) Each room containing IAT will be secured when not attended in addition to the common suite door. This includes individual doors to rooms located in a suite of rooms.

(3) All external doors will have overhead lighting.

c. Biosafety level 3 (not to the level of select agents).

(1) Measures required for biosafety levels 1 and 2 will be implemented.

(2) Entry to IAT rooms and suites will be controlled at all times. Control may be through manpower and/or procedural means, mechanical means, or electronic means.

(3) Unoccupied rooms/suites containing IAT will be checked on an irregular basis not to exceed 8 hours.

(4) An IDS may be provided if the commander/director determines the threat warrants it (funded by core budget dollars).

Chapter 5
Security of U.S. Army Museums

Section I

Inspections and Personnel Selection

5–1. General

This chapter prescribes specific physical security standards, policies, requirements, and guidance to safeguard historically significant items in the care of the Army museum system. Historically significant items will be protected to deter theft and vandalism without damaging the item or affecting the educational, training, and aesthetic value of the items. All AA&E not rendered inoperable and not on display will be stored, secured, and inspected per AR 190–11. Arms in storage may remain in operable condition. All other items will be secured and inspected as indicated in this regulation. ESS not specifically identified as a regulatory requirement by AR 190–17, AR 190–54, or AR 190–59 may be purchased and maintained by commands for museums if the command opts to use these systems. CCTV systems, components, and supporting equipment and well as video telecom systems not required will be funded by commands, not MDEP QPSM funds.

5–2. Inspections

Physical security inspections of museum facilities will be conducted per the criteria outlined in this regulation. Inspections of museum arms storage facilities will be per AR 190–11.

5–3. Museum personnel selection

Military and civilian personnel assigned or attached (including special duty personnel) to staff an Army museum must be honest, responsible, and emotionally stable. Local file checks will be made by the supporting military law enforcement official in response to a written request before personnel are assigned or attached (including special duty personnel) to museum duties. National Crime Information Center checks can only be used to determine if the person has any outstanding warrants. Temporarily detailed, contracted, and volunteer personnel will work under close supervision of the permanently assigned staff. Those museum personnel considered for unaccompanied access to operable and inoperable museum AA&E will be processed and granted access per AR 190–11.

Section II

Museum Structures and Indoor and Outdoor Displays

5–4. Structural requirements

Museum facilities traditionally house one-of-a-kind, irreplaceable items of historical significance. Such items are generally considered invaluable because they are irreplaceable and should be considered sensitive property. They should be reasonably protected. The degree of protection necessary must be determined locally and in partnership between the museum curator, supporting military law enforcement official or equivalent security officer, and supporting facility engineers. Museum buildings and apertures providing access to the building should be modified or constructed to delay a determined intruder long enough for a security force to respond. Museum facilities will meet the minimum standards of this regulation. Security measures will be implemented for those facilities protected under the National Preservation Act of 1966 to the

extent possible. Consistent with this act, IDS coverage should be included for all unbarred windows and doors other than those at arms storage facilities.

5–5. Locks and keys

a. Key and lock control. Key and lock control for museum AA&E and other museum items will be per appendix D for AA&E that is rendered inoperable. Keys to AA&E that cannot be rendered inoperable due to value, uniqueness, and so forth, will be secured per AR 190–11 and DODM 5100.76.

b. Key custodian. The museum director will be designated as the key custodian, whenever feasible. The commander/director or activity chief will appoint the primary and an alternate key custodian in writing.

c. Locks.

(1) Exterior doors used for access to museum facilities will be secured with deadbolts or other equivalent locks as advised by the servicing facility engineer.

(2) Vehicles and facilities where vehicles are stored will be secured per paragraph 3–11.

d. Keys.

(1) Museum facility keys will be maintained separately from arms storage, high-value item storage, and IDS keys.

(2) Keys will not be left unattended or unsecured at any time.

(3) Where an Army museum or exhibit is protected by an operational IDS, museum personnel as authorized by the museum curator or director may remove the keys to the museum or exhibit from the installation at which the museum or exhibit is located. Unless authorized by the commander, where an operational IDS is not installed, the museum keys will not be removed from the installation, but will be locked in a secure strongbox in a secured location on post, such as the DES. Museum personnel as authorized by the museum curator or director will retain custody of the keys in this strongbox.

(4) Where combination-locking devices are used to secure items such as containers and display cases, the combination will be controlled and safeguarded per appendix D.

(5) Duplicate keys will not be kept with operational keys. They will be maintained by the museum director, unless the director is also the key custodian. In the latter case, the keys will be maintained by the installation agency that supports the museum or by the supporting DES.

5–6. Security lighting

Interior and exterior lighting will be provided in all museum buildings in which sensitive property is located. Sensitive property is property requiring a high degree of protection and control because of its vulnerability to theft or potential for use in an illegal activity. As a minimum, all entrances will be lighted during hours of darkness. Use UFGS 28 10 05 to determine lighting requirements.

5–7. Intrusion detection systems

Installation of IDS may supplement existing security measures or provide a commensurate degree of protection. Requirements for IDS for AA&E are in AR 190–11. Requirements for obtaining IDS are in AR 190–13.

5–8. Exhibit or display cases

The viewing surfaces of exhibit or display cases will be constructed of at least 1/4-inch thick laminated glass, transparent acrylic plastic, or transparent polycarbonate plastic, securely fastened into frames or into the container. Where plate surfaces join at an angle, the edges will be bonded and rounded to prevent insertion of a pry tool. Cases with hinged openings must have all hinge butts concealed or spot welded or use a comparable security measure. Non-viewing surfaces of cases will be constructed to offer a higher degree of protection than the viewing surface.

5–9. Museum workshops

Museum workshops used for maintenance or restoration work will be secured at the close of each business day. Workshops containing AA&E will be secured per AR 190–11.

5–10. Security forces

a. Each museum will be attended by at least one member of the museum staff that will be tasked with museum security while it is open to the public. (This function can be combined with other duties.) Museums that are organized within several separate, non-connecting buildings will have museum or security personnel in each facility or an electronic monitoring system. The museum attendant will be especially alert to detect pilferage, damage, or theft. The installation of one-way mirrors and electronic sensing devices covering all parts of the museum should be considered. Museum parks and exterior displays will have electronic surveillance where practical and checked periodically by security patrols.

b. Museum commanders/directors or activity chiefs will verify that museums are on an assigned security patrol route and that special orders include an unscheduled check at least once every 8 hours by that patrol during non-duty hours on a daily basis and recorded through the use of a SF 702.

5–11. Museum parks
Large items of historical property that are displayed outdoors in museum parks will be anchored to prevent theft or damage from natural hazards. Pilferable component parts will be secured to a display or removed.

5–12. Museums in civilian communities
When museum facilities are located in civilian communities, museum commander/director or activity chief will liaise with local civil police agencies for security checks conducted by local police, and for a coordinated security plan.

5–13. Reporting loss of property
Loss of historical property other than AA&E will be reported by the supporting law enforcement official or equivalent security officer per AR 190–45. See AR 870–20 for reporting requirements for loss of appropriated and nonappropriated fund property.

5–14. Accountability of equipment
Accountability of historical properties will be per AR 870–5 and AR 870–20.

5–15. Museum weapons and ammunition
Security of museum weapons and ammunition will be per AR 190–11.

Chapter 6
Security of U.S. Army Corps of Engineers Civil Works and Like Project Resources

Section I

Introduction

6–1. Overview
a. U.S. Army Corps of Engineers (USACE) commanders and directors will apply the minimum physical security measures defined in this chapter to all civil works an like project resources within their responsibility.

b. Commonly encountered types of USACE civil works and like project resources are categorized in this chapter.

c. Determining the risk level for some USACE civil works and like project resources with a dam or (also known as embankment) will require obtaining the dam project's 1 percent exceedance reservoir level or (also known as reservoir elevation that occurs only 3 to 4 days every year) from the district's dam safety engineer, and/or their designated representative, in order to determine the proper risk level designation and associated minimum physical security protective measures. In these situations, the risk level obtained using DA Form 7278 may not reflect the same risk level as would be obtained with the exceptions outlined in this chapter. In those instances where a conflict exists, the exception outlined in this chapter defined for some USACE civil works and like project, resources will take precedence over the risk level resulting from using DA Form 7278.

d. Chapters 1 through 5 apply equally to USACE civil works and like project resources when applicable.

e. Section II of this chapter outlines common, and applicable to all, civil works and like projects general requirements and guidance.

f. Section III of this chapter outlines the minimum physical protective measures for most civil works and like project resource categories requiring a risk analysis. The measures are categorized by risk levels established using the risk analysis procedure in DA Pam 190–51 or as dictated by the exceptions outlined herein. Risk level I measures will be the minimum.

g. Section IV of this chapter outlines the minimum security standards for civil works and like project resources that do not require a risk analysis.

6–2. Restricted area requirements
a. Restricted areas will be per AR 190–13.

b. Designate, in writing, restricted area(s) as defined in AR 190–13, defined herein, or based upon the judgment of the responsible USACE commander/director or activity chief (hereafter "responsible commander").

c. Restricted area sign will be posted at USACE civil works and like project resource(s) entrances designated as restricted area(s). Restricted area signs will comply with signage requirements defined in AR 190–13.

Section II

General Requirements and Guidance

6–3. Fencing requirements

a. General.

(1) Fencing will be per chapter 3, unless otherwise specified herein.

(2) Fences will remain free and devoid of vegetation.

(3) Modifications to existing security, perimeter, or boundary fences should not be made solely to conform to the requirements of this regulation if the existing fence achieves the intended objective and goals for installing the fence.

b. Security fence.

(1) New security fencing will be a minimum a minimum fence fabric height of 7 feet (2.13m), excluding the top guard. Fence height including outriggers will be a minimum of 8 feet (2.44m).

(2) When new security fencing is required as a protective measure, the type and quantity of fencing in heights in excess of 7 feet excluding the top guard, and 8 feet with outriggers, and whether a different top guard or other features are required will be based on the appropriate security publication and the judgment of, and approved in writing by, the responsible commander.

(3) New security fencing will meet the minimum requirements of UFGS 32 31 13 and USACE drawing number STD 872–90–02, unless otherwise required based upon the appropriate security publication and the judgement of, and approved in writing by, the responsible commander.

(4) Establish a 10-foot wide clear zone on the inside and outside of the fence to the extent feasible, and keep it clear of obstacles, topographical features, and vegetation. Landscaping features within the clear zone will be kept to 1-foot in height or less to ensure an unobstructed view and prevent concealment for aggressors.

(5) Vegetation (for example, trees, tree limbs/branches, bushes, and so forth) will be trimmed to prevent their use by an aggressor as a climbing aid or over reaching from the unprotected side into the protected area.

c. Perimeter fence.

(1) New perimeter fencing fence height, including the outrigger, will be a minimum of 8 feet (2.44m).

(2) When new perimeter fence is required as a protective measure, the type and quantity of fencing, including heights in excess of 8 feet, and whether a different top guard or other features are required, will be based on the appropriate security publication and the judgment of, and approved in writing by, the responsible commander.

(3) New non-sensored, or unsensored, perimeter fencing will meet the requirements of UFGS 32 31 13 and USACE drawing number STD 872–90–03, unless otherwise required based on the appropriate security publication and the judgment of, and approved in writing by, the responsible commander. New sensored perimeter fencing will meet the requirements of UFGS 32 31 13.53 and USACE drawing number STD 872–90–04, unless otherwise required based on the appropriate security publication and the judgment of, and approved in writing by, the responsible commander.

(4) Establish a 10-foot wide clear zone on the inside and outside of the fence to the extent feasible, and keep it clear of obstacles, topographical features, and vegetation. Landscaping features within the clear zone will be kept to 1-foot in height or less to ensure an unobstructed view and prevent concealment for aggressors.

(5) Vegetation (for example, trees, tree limbs/branches, bushes, and so forth) will be trimmed to prevent their use by an aggressor as a climbing aid or over reaching from the unprotected side into the protected area.

(6) Perimeters encompassing walls or buildings in excess of 8 feet tall do not need to have barbed wire and an outrigger added to the top of the wall or building roof unless it is required based upon the judgment of the responsible commander.

d. Boundary and other non-security/non-perimeter fence.

(1) Fencing maybe used to delineate the civil works and like project's "property" boundary or the lands that are controlled by USACE. Boundary delineation varies within USACE and can include no fencing, right-of-way markers or farm style (for example, barbed wire, woven wire or wood) fencing. Delineation of the project's property boundary and other nonsecurity/nonperimeter fencing will be based on the judgment of the responsible commander.

(2) Barbed wire (3, 4, or 5 strand) or woven wire fencing will meet the requirements of UFGS 32 31 26 and USACE drawing number STD 872–90–11, STD 872–90–12, STD 872–90–13, or STD 872–90–14, unless otherwise specified.

6–4. Electronic security systems requirements

a. Design electronic security systems. Use UFC 4–021–02 to design ESS.

b. New electronic security systems. Any new ESS (for example, IDS, CCTV systems, ACS, and so forth) design must include and be coordinated with the USACE Electronic Security Systems Mandatory Center of Expertise per USACE Engineering Regulation (ER) 1110–1–8162. ESS not specifically identified as a regulatory requirement by AR 190–17, AR 190–54, or AR 190–59 may be purchased and maintained by USACE commands if the command opts to use these systems. CCTV systems, components, and supporting equipment and well as video telecom systems not required will be funded by commands, not MDEP QPSM funds.

c. Closed Circuit Television system.

(1) CCTV systems will be per chapter 3.

(2) Some USACE civil works and like projects may require two systems; one in support of operation and maintenance activities and another that is strictly dedicated to security. The operation and maintenance CCTV system will be a stand-alone CCTV system which is separate and apart from the security CCTV system.

(3) The security CCTV system will be fully integrated into the project's IDS.

(4) The ACS, if existing or new, will be integrated into the integrated IDS and security CCTV systems.

(5) Lighting in support of the security CCTV system will be compatible with the selected or specified camera type encompassing the security CCTV system.

(6) Lighting in support of a security CCTV system may require further coordination with state wildlife/fish and game agencies, where fish passage will be a key design component that will have to be addressed in the planning and design phases.

d. Intrusion Detection System.

(1) IDS will be per chapter 3.

(2) The IDS will be fully integrated into the project's security CCTV system.

(3) The end state of the fully integrated system is to enable assessment, without human intervention, of an alarm annunciation(s) via the integrated security CCTV system.

(4) IDS warning signs will be posted at resource entrance(s) to designate an IDS system is present. IDS signage will meet IDS warning sign requirements defined in AR 190–13.

(5) Control IDS keys and locks per appendix D.

(6) Additional IDS requirements are defined in AR 190–13.

e. Access Control System.

(1) IDS will be per chapter 3.

(2) The ACS, if existing or new, will be fully integrated into the project's IDS and security CCTV systems. A separate, stand-alone, ACS may be installed if no IDS or CCTV systems is present.

(3) Some USACE civil works and like project resources may have additional ACS requirements for interior and/or exterior doors which assist USACE in voluntarily complying with the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards. Check with the district, or division in some instances, reliability compliance officer for building access control requirements and applicability of ACS at civil works and like project resources, especially as it pertains to the powerhouse and powerhouse control room.

f. Monitoring services. Central monitoring services for ESS will be per chapter 3.

6–5. Security lighting guidance and requirements

Lighting guidance and requirements will be in accordance with chapter 3.

6–6. Vehicle barrier requirements

Any vehicle barrier installed in and/or adjacent to a civil works and like project roadway must be planned, designed, and constructed (for example, proper color, signage, and so forth) for safety consistent with the Federal Highway Administration's Manual of Uniform Traffic Code Devices and requirements from the Transportation Engineering Agency of the Surface Deployment and Distribution Command.

6–7. 2-minute resistant, non-tested forced entry door and other forced entry resistant components requirements

a. Use USACE "Doors (2-minute resistant, non-tested)" specification when a 2-minute, non-tested forced entry resistant door is required to establish the 2-minute, non-tested forced entry resistant personnel barrier perimeter.

b. Other forced entry resistant component requirements and "hardening" information can be found in UFC 4–020–01, UFC 4–020–02FA, and UFC 4–020–03FA.

6–8. Locks, electronic locks and locking systems, keys, locking devices, hasps and chains, and protective seals requirements

Follow standards per appendix D.

6–9. Control systems requirements

The commander/director or activity chief for all USACE civil works and like projects where control systems are present will coordinate requirements and implementation of physical security measures for the protection of control system assets with USACE's Critical Infrastructure Cybersecurity Center of Expertise (CESWL–OP–X).

6–10. Antiterrorism measures requirements

a. Physical security measures establish the normal, day-to-day, security posture for USACE civil works project resources. These measures should not be confused with AT Force Protection Condition measures. AT measures are typically implemented to increase security for limited periods of time, such as short-term, due to increases in threat or elevated water level conditions that require additional measures and security requirements above and beyond normal day-to-day operations.

b. Apply AT standards per AR 525–13.

6–11. Guidance for safety

Safety requirements will be in accordance with paragraph 3–7.

6–12. Security criteria deviation process

Use the process provided in AR 190–13 to request a waiver or exception to this policy.

6–13. Resources that do not fit the listed resource categories requirements

This publication and chapter cannot list or address all the types of resources encountered at USACE civil works and like projects so some resources will not correspond exactly to the categories in this publication, or some may relate to multiple chapter categories. If no category seems appropriate, the responsible commander for the resource shall develop and implement physical protective measures and, when appropriate, security procedural measures necessary to safeguard USACE civil works and like project resources. The measures will be reviewed by the supporting physical security officer and approved by the senior commander.

Section III

Minimum Security Standards for Resources Requiring Risk Analysis

6–14. Spillway gate structures, outlet works, and intake structures

a. Spillway gate structures. The following risk levels and minimum standards apply to a controlled (for example, gated) spillway. This section does not apply to uncontrolled (for example, not gated) earthen, rock, or concrete spillway structures, with or without concrete or rock overflow structures (for example, Ogee Weir, and so forth).

(1) Exceptions to this policy and risk calculation results include, if the 1 percent exceedance reservoir level is where—

(a) Water never reaches a spillway gate; only risk level I will be applied.

(b) Loss of all spillway gates does not result in appreciable consequences downstream (total discharge does not exceed downstream channel capacity), then only risk level I will be applied.

(c) Loss of all spillway gates results in marginal consequences downstream (total discharge barely exceeds downstream channel capacity), then only risk level II will be applied.

(d) Loss of all spillway gates results in unacceptable downstream consequences (total discharge greatly exceeds downstream channel capacity), then risk level III will be applied.

(2) Additional considerations must include addressing the different spillway gate control configurations. Spillway gate controls maybe controlled locally or at another USACE project location or combination of both. Local control may include primary control located at each spillway gate with, or without, remote secondary control (for example, in a powerhouse control room). Some spillway gate controls have dedicated power to them continuously, whereas some may not. In these instances, the requirements for protecting controls will be based upon the judgment of the responsible commander or as defined herein.

b. Outlet works and intake structures.

(1) Outlet works and intake structures encompass a large number of different combinations and configurations ranging from one to many (for example, 10+) conduits, where conduits range from those a few feet (for example, 3 to 4 feet) in

diameter to those in excess of 25 feet in diameter. Some outlet works and intake structures may be completely underwater whereas others may be partially submerged or "in the dry" or any combination thereof (for example, intake is completely submerged, and outlet is partially submerged) depending on the time of the year and the reservoir elevation. The partially submerged, 15–25+/– feet diameter conduit configurations that exist at some projects may permit something as large as recreational boat to enter the outlet works conduit(s), which may, or may not, also provide direct access to the intake structure and/or intake structure gates. Outlet works and their conduits may even be part of and/or be built directly into a spillway or be an integral part of a powerhouse structure. Outlet works and intake structures vary from having a single to multiple gates of various sizes. Some outlet works can be accessed from the downstream side slope, embankment crest road or near the toe of the dam. Some intake structures have no gates and are nothing more than a concrete overflow structure positioned in the reservoir serviceable only by boat. Some intake structures are accessible only by bridge (intake structure service bridge) or boat. Other intake structure configurations can encompass access from the upstream side slope, dam crest road, powerhouse, spillway, or government-owned land adjacent to the dam. In a "dry dam" (dam with no permanent reservoir) configuration, the outlet works and intake structure often times provide complete and unrestricted accessible by the public.

(2) Exceptions to this policy and risk calculation results include, if the 1 percent exceedance reservoir level is where:

(a) Water never reaches an outlet works/intake structure gate(s) or outlet works/intake overflow structure; risk level I will be applied.

(b) The loss of all outlet works/intake structure gates does not result in appreciable consequences downstream (for example, total discharge does not exceed downstream channel capacity); risk level I will be applied.

(c) The loss of all outlet works/intake structure gates results in marginal consequences downstream (for example, total discharge barely exceeds downstream channel capacity); risk level II will be applied.

(d) The loss of all outlet works/intake structure gates result in unacceptable consequences downstream (for example, total discharge greatly exceeds downstream channel capacity); risk level III will be applied.

c. Physical protective measures (risk level I).

(1) Install lockable forced entry resistant enclosures over exterior located (for example, outside) gate controls when continuous power is provided to the gate controls.

(2) Control access to the spillway gate structure, outlet works, and intake structures and appurtenant features (for example, gates, controls, power supply(s) cabinets, hoisting equipment, galleries, supervisory control and data acquisition equipment, pressure relief system, pumps, drains, and so forth).

(3) Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on the structure(s) if no fencing exists and/or on perimeter fencing and personnel and vehicle gates.

(4) Establish continuous unsensored personnel barrier perimeter(s) (for example, fence, building exterior, and so forth) and minimum, manual access control (for example, lockable fence gates, locked building doors, and so forth) on the landside approaches to these structure(s). Where the structure, or its components, can be accessed by the public (or an aggressor) with relative ease, additional protective measures (for example, securing access ladders, manhole covers, louvers, and so forth) will be necessary to prevent unauthorized access to and/or operation of the structure(s).

(5) Control keys and locks in accordance with appendix D.

d. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Establish a continuous unsensored personnel barrier perimeter at the spillway gate structure, outlet works and intake structure (buildings) comprised of, at a minimum, 2-minute, non-tested forced entry resistant components.

(3) Install IDS and CCTV (with security lighting at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness) systems in accordance with this chapter, based on the judgment of the responsible commander.

e. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Establish a sensored perimeter (IDS and CCTV systems) along/at the spillway gate structure, outlet works and intake structure, comprised of, at a minimum, 2-minute, non-tested forced entry resistant components. Typically this will involve installing USACE "Doors (2-minute resistant, non-tested)" specification doors on the structure's exterior doors and hardening any first floor openings (for example, windows, vents, louvers, hatches, man holes, and so forth) or other "portals" through the structures in excess of 96 square inches that are located less than 12 feet from the ground level and to similar openings above the first floor which can be reached from an elevated portion of the structure or an adjacent structure (for example, powerhouse, dam, spillway, intake structure, outlet work, surge tank, penstock, switchyard, and so forth) which provides ground level access. Long narrow openings with the shortest dimension measuring less than 6 inches are exempt from these requirements. In some instances these structures, or their components, can be accessed by the public

(or an aggressor) with relative ease, additional protective measures (for example, securing access ladders, and so forth) may be necessary to prevent unauthorized access or operation.

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(4) Designate the resource as a restricted area.

6–15. Service bridges

Spillway and intake structure service bridges can vary from being continuously public accessible bridges to ones that are only used and accessible by USACE personnel and authorized vehicles. Some service bridges are accessible from the dam crest road, especially in those instances where the dam crest road also serves as a continuously public accessible road within the community. The following risk levels and minimum standards can be applied to many of the commonly encountered service bridge configurations within USACE. Some site-specific conditions maybe encountered which are not addressed herein, in which case the resource shall meet the intent of the applicable risk level that applies to the site-specific conditions based on the judgment of the responsible commander.

a. Physical protective measures (risk level I).

(1) Install lockable bar gate or fence gate or similar vehicle barrier(s) across the continuously publicly accessible service bridge road (typically near the bridge abutment(s)). In some instances, the continuously publicly accessible road that permits direct and unrestricted access to the service bridge cannot be closed indefinitely but the capability to close the road will be established. Keep vehicle barriers in a road open condition. Operate barriers in a road-closed condition based on the judgment of the responsible commander.

(2) Install lockable bar gate or fence gate or similar vehicle barrier(s) across the USACE access controlled service bridge road (typically near the bridge abutment(s)). Keep vehicle barriers in a road-closed condition. Operate barriers in a road open condition based on the judgment of the responsible commander.

(3) Install an unsensored personnel barrier perimeter(s) (for example, fence) and, at a minimum, manual access control (for example, lockable personnel fence gate) at or near the service bridge abutment based on the judgment of the responsible commander. Keep personnel barrier gates in the closed position.

(4) Control keys and locks in accordance with appendix D.

b. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Install “No parking, stopping, or standing on bridge” or “No parking or stopping on bridge” or similar signage when a continuously public accessible road resides on the service bridge.

(3) Install an unsensored personnel barrier perimeter(s) (for example, fence) and, at a minimum, manual access control (for example, lockable personnel fence gate) on the service bridge abutment. Keep personnel barrier gates in the closed position.

(4) Install appropriate signage (for example, “No Unauthorized Vehicles,” “Off Limits to Unauthorized Personnel,” “No Unauthorized Personnel,” “No Trespassing, U.S. Government Property,” or similar message) on service bridge fencing and personnel and vehicle gates. Ensure sign(s) are easily identifiable by the public when the barrier gates are in both a closed and open position.

(5) Discuss with the responsible commander vehicle attack scenarios to the service bridge(s) which may culminate in installing, or not, a continuous UFC 4–022–02 compliant vehicle barrier(s) perimeter (typically near the bridge abutment on the secure side of the service bridge personnel barrier perimeter (for example, fence)) complete with installation of UFC 4–022–02 compliant vehicle barriers across the continuously publicly accessible service bridge road(s). Operate barriers, if installed, in a road open or closed condition based on the judgment of the responsible commander.

(6) Discuss with the responsible commander vehicle attack scenarios to the service bridge (s) which may culminate in installing, or not, a continuous UFC 4–022–02 compliant vehicle barrier(s) perimeter (typically near the bridge abutment on the secure side of the service bridge personnel barrier perimeter (for example, fence)) complete with installation of UFC 4–022–02 compliant vehicle barriers across the USACE access controlled service bridge road(s). Keep vehicle barriers in a road-closed position. Operate barriers, if installed, in a road open condition based on the judgment of the responsible commander.

(7) Install, as needed, additional UFC 4–022–02 compliant passive vehicle barrier(s) adjacent to any vehicle barrier(s) installed in the service bridge road thus preventing an aggressor’s vehicle from circumventing the road vehicle barrier(s).

c. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Install a sensored personnel barrier perimeter (for example, fence) and, at a minimum, manual access control (for example, lockable personnel fence gate) at or near the service bridge abutment. Keep personnel barrier gates in the closed position.

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(4) Designate the resource as a restricted area.

6–16. Embankment—earthen, rock fill, and hydraulic fill dams

a. Embankment – earthen, rock fill, and hydraulic fill dams. The following risk levels and minimum standards apply to earthen, rock fill, and hydraulic fill dams. This section does not apply to concrete, roller-compacted concrete, or masonry dams.

b. Exceptions. Exceptions to this policy and risk calculation results include, if the 1 percent exceedance reservoir level results in—

(1) Greater than 40 feet below the crest of the dam (for example, >40 feet of freeboard), then only risk level I will be applied.

(2) Between 20 and 40 feet below the crest of the dam (for example, 20 to 40 feet of freeboard), then only risk level II will be applied.

(3) Less than 20 feet below the crest of the dam (for example, <20 feet of freeboard), then only risk level III will be applied.

c. Physical protective measures (risk level I).

(1) Install lockable bar gate or fence gate or similar vehicle barrier(s) across the continuously publicly accessible dam crest road (typically at or very near the dam abutments(s)), and across other continuously publicly accessible road(s) that traverse the dam which provide access to the dam crest road. In some instances, the continuously public accessible road that permits direct access to the dam (for example, dam crest road) cannot be closed indefinitely but the capability to close the road will be established. Keep vehicle barriers in a road open condition. Operate barriers in a road-closed condition based on the judgment of the responsible commander.

(2) Install lockable bar gate or fence gate or similar vehicle barrier(s) across the USACE access controlled dam crest road (typically at or very near the dam abutments(s)), and across other USACE access controlled road(s) that traverse the dam which provide access to the dam crest. Keep vehicle barriers in a road-closed condition. Operate barriers in a road-closed condition based on the judgment of the responsible commander.

(3) Ensure all instrumentation and inspection gallery doors, vault covers, manhole covers, penetrations (for example, piezometers, relief wells, drains, and so forth) greater than 6 inches in diameter are locked and keys and locks are controlled in accordance with appendix D.

d. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Install, minimum 2-minute, non-tested forced entry resistant components on all instrumentation and inspection gallery doors, vault covers, manhole covers, penetrations greater than 6 inches diameter (for example, piezometers, relief wells, drains, and so forth).

(3) Install “No parking, stopping, or standing on dam” or “No parking or stopping on dam” or similar sign message adjacent to the continuously publicly accessible road that resides on the dam crest.

(4) Discuss with the responsible commander vehicle-borne improvised explosive devices attack scenarios (also known as freeboard and explosive cratering depths) to the embankment which may culminate in installing, or not, UFC 4–022–02 compliant vehicle barrier(s) across the continuously publicly accessible dam crest road (typically at or very near the dam abutments(s)), and on other continuously publicly accessible road(s) that traverse the dam which provide access to the dam crest road. Operate barriers, if installed, in a road open or closed condition based on the judgment of the responsible commander.

(5) Discuss with the responsible commander vehicle-borne improvised explosive devices attack scenarios (also known as freeboard and explosive cratering depths) to the embankment which may result in installing, or not, installing UFC 4–022–02 compliant vehicle barrier(s) across the USACE access controlled dam crest road (typically at or very near the dam abutments(s)), and on other USACE access controlled road(s) that traverse the dam which provide access to the dam crest. Keep vehicle barriers in a road-closed position. Operate barriers, if installed, in a road open or closed condition based on the judgment of the responsible commander.

(6) Install, as needed, additional UFC 4–022–02 compliant passive vehicle barrier(s) adjacent to any vehicle barrier(s) installed in the road(s) thus preventing an aggressor’s vehicle from circumventing the road vehicle barrier(s).

e. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Install IDS, where feasible and where necessary, on openings or penetrations into the dam which are greater than 96 inches, or openings greater than 6 inches wide, through which destructive devices could be introduced by an aggressor.

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

6–17. Powerhouses

a. Powerhouses. USACE powerhouses also encompass a large number of different combinations and configurations ranging from those that have one or two generating units (defined as "units" hereafter) to those that may contain 10+ or more. In rare cases, more than one powerhouse may be present at the project. Powerhouses can be located as a separate structure at or near the downstream toe of the dam or they may be an integral part of the dam and located adjacent to the dam crest road. Those located at the toe of the downstream dam side slope will typically have surge tanks on top of the powerhouse or be located in a separate building adjacent to the powerhouse structure. Some powerhouses are also connected to the pool or reservoir via intake structure(s) and penstocks with surge tanks and a surge tank building. Sometimes penstocks are buried in or beneath the dam, and sometimes they are not. Those that are not buried are often exposed and can be accessed by maintenance personnel, and aggressors. Exposed penstocks usually do not have unrestricted public accessible to them without going through a controlled perimeter and having an USACE escort. Sometimes public accessible, unescorted and escorted, visitor centers may also reside in the powerhouse. Nearly all powerhouses have publicly accessible roads that permit vehicles to get into relative close proximity to the powerhouse structure(s). This section applies to only to the powerhouse structure(s). Unescorted public accessible powerhouse visitor centers are addressed in "unescorted public accessible powerhouse visitor center" below.

b. Powerhouse exceptions. Exceptions to this policy and risk calculation results include, if the 1 percent exceedance reservoir level and powerhouse configuration and generating capacity is such that—

(1) The loss of all powerhouse units does not result in appreciable consequences to the electric grid, then only risk level I will be applied.

(2) The loss of all powerhouse units' results in marginal consequences to the electric grid, then only risk level II will be applied.

(3) The loss of all powerhouse units' results in unacceptable consequences to the electric grid, then risk level III will be applied.

(4) If the powerhouse is designated a "black start" facility, then risk level III will be applied.

c. Physical protective measures (risk level I).

(1) Establish continuous unsensored personnel barrier perimeter(s) (for example, unsensored fence, exterior doors/windows, and so forth) with, at a minimum, manual access control (for example, lockable personnel fence gate, door, and so forth) around the powerhouse and appurtenant structure(s).

(2) Install lockable bar gate or fence gate or similar vehicle barrier(s) across all roads that permit access to the powerhouse. Keep vehicle barriers in a road-closed position. In some instances, the continuously public accessible road that permits direct access to the powerhouse (for example, dam crest road) cannot be closed indefinitely but the capability to close the road will be established. In these cases, operate the barriers in a road open or closed condition based upon the judgment of the responsible commander.

(3) Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on or adjacent to the powerhouse personnel doors if no perimeter fence exists, and on perimeter fence and personnel and vehicle gates.

(4) Control keys and locks in accordance with appendix D.

d. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Establish a continuous unsensored personnel barrier (for example, fence) perimeter around the powerhouse and appurtenant structures.

(3) Establish a continuous unsensored personnel barrier perimeter comprised of, at a minimum, 2-minute, non-tested forced entry resistant components on the exterior walls of the powerhouse and appurtenant structure(s). Typically this will involve installing USACE "Doors (2-minute resistant, non-tested)" on the powerhouse exterior doors and hardening any first floor openings (for example, windows, vents, louvers, hatches, man holes, and so forth) or other "portals" through the powerhouse in excess of 96 square inches that are located less than 12 feet from the ground level and to similar openings above the first floor which can be reached from an elevated portion of the powerhouse or an adjacent structure (for example, dam, spillway, intake structure, outlet works, surge tank, penstock, switchyard, and so forth) which provides ground level access. Long narrow openings with the shortest dimension measuring less than 6 inches are exempt from these requirements. In some instances the powerhouse, or its components, can be accessed by the public (or an aggressor) with relative ease, additional protective measures (for example, securing access ladders, manhole covers, and so forth) may be necessary to prevent unauthorized access or operation.

(4) Discuss with the responsible commander vehicle attack scenarios to the powerhouse which may culminate in installing, or not, a continuous UFC 4–022–02 compliant vehicle barrier(s) perimeter (typically on the secure side of the powerhouse and appurtenant structures personnel barrier perimeter (for example, fence)) complete with installation of UFC 4–022–02 compliant vehicle barriers across the continuously publicly accessible powerhouse accessible road(s). Operate barriers, if installed, in a road open or closed condition based on the judgment of the responsible commander.

(5) Discuss with the responsible commander vehicle attack scenarios to the powerhouse which may culminate in installing, or not, a continuous UFC 4–022–02 compliant vehicle barrier(s) perimeter (typically on the secure side of the powerhouse and appurtenant structures personnel barrier perimeter (for example, fence)) complete with installation of UFC 4–022–02 compliant vehicle barriers across the USACE access controlled powerhouse road(s). Keep vehicle barriers in a road-closed position. Operate barriers, if installed, in a road open condition based on the judgment of the responsible commander.

(6) Install, as needed, additional UFC 4–022–02 compliant passive vehicle barrier(s) adjacent to any vehicle barrier(s) installed in the road(s) thus preventing an aggressor's vehicle from circumventing the road vehicle barrier(s).

e. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Establish a sensored personnel barrier perimeter(s) (for example, sensored fence) on the exterior of (building perimeter) or around the powerhouse and appurtenant structure(s) via integrated IDS and CCTV system.

(3) Establish a sensored personnel perimeter (also known as install IDS and CCTV systems) along/at the powerhouse and appurtenant structure(s), comprised of, at a minimum, 2-minute, non-tested forced entry resistant components.

(4) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(5) Designate the resource as a restricted area.

6–18. Powerhouse control rooms and unescorted public accessible powerhouse visitor centers

a. Powerhouse control rooms. USACE powerhouse control rooms come in a variety of configurations and locations within the powerhouse. Additionally, there are portions of certain powerhouses that enable the public unescorted access to elevated viewing platforms within the powerhouse. Some powerhouses have visitor centers in them, with unrestricted and/or unescorted public access.

b. Physical protective measures (risk level I).

(1) Access into the control room will be controlled.

(2) Install appropriate signage (for example, "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel" or similar message) on or adjacent to doors in the visitor center that provide access to the controlled areas of the powerhouse.

(3) Control keys and locks in accordance with appendix D.

c. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Establish a continuous unsensored personnel barrier perimeter at the powerhouse control room comprised of, at a minimum, 2-minute, non-tested forced entry resistant components.

(3) Establish a continuous unsensored interior personnel barrier perimeter comprised of a minimum of 2-minute, non-tested forced entry resistant components between the unrestricted publicly accessible visitor center and the other controlled access areas of the powerhouse and appurtenant structure(s).

(4) Install appropriate signage (for example, "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel" or similar message) on or adjacent to doors that provide access to the control room.

(5) Designate the powerhouse control room as a restricted area.

d. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Establish a sensored personnel perimeter(s) (also known as install IDS and CCTV systems) along/at the powerhouse control room, comprised of, at a minimum 2-minute, non-tested forced entry resistant components.

(3) Establish a sensored interior personnel barrier perimeter along the interior, comprised of, at a minimum 2-minute, non-tested forced entry resistant components between the unrestricted publicly accessible visitor center and the other controlled access areas of the powerhouse and appurtenant structure(s).

(4) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

6–19. Switchyards

a. U.S. Army Corps of Engineers. Location and ownership of switchyards vary within USACE. Switchyards can be located adjacent to the powerhouse, or in rare instances, the switchyard can be located on the roof of the powerhouse.

Some switchyards are owned, operated, and maintained by others and are not the responsibility of USACE despite being located on project property. Most switchyards are already fenced, some smaller ones are not. The configuration of the switchyard can also vary considerably. Many times there are "cable tunnels" and/or "power tunnels" that are located beneath the switchyard which can provide direct access to the powerhouse. Sometimes access to these "tunnels" is via a hatch cover, manhole, or small building/structure with a door. Many of the tunnels require exhaust vents that maybe louvered or screened. This section applies to switchyards owned, operated, and maintained by USACE.

b. Physical protective measures (risk level I).

(1) Access to USACE switchyards will be controlled.

(2) Control keys and locks in accordance with appendix D.

c. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Establish a continuous unsensored personnel barrier perimeter(s) comprised of, at a minimum, 2-minute, non-tested forced entry resistant components at entrances located in the switchyard (for example, cable tunnel and/or power tunnel) which provide direct access to the powerhouse. Typically this will involve installing USACE "Doors (2-minute resistant, non-tested)" on the cable tunnel and/or power tunnel structure and hardening of any "portals" (for example, windows, vents, louvers, hatches, and so forth) that provide access to the powerhouse in excess of 96 square inches that are located less than 12 feet from the ground level and to similar openings above the first floor which can be reached from an elevated portion of the structure or an adjacent structure which provides ground level access. Long narrow openings with the shortest dimension measuring less than 6 inches are exempt from these requirements.

(3) Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on switchyard structures that provide access into the powerhouse and/or on switchyard perimeter fencing and personnel and vehicle gates.

d. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Install IDS and CCTV systems along non-tested forced entry resistant components perimeter. Typically this will involve installing IDS with CCTV system coverage of alarm points at the cable tunnel and/or power tunnel structure doors and hardened "portals" (for example, windows, vents, louvers, hatches, and so forth) in excess of 96 square inches that provide access to the powerhouse.

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(4) Designate the resource as a restricted area.

6–20. Navigation locks

a. Physical protective measures (risk level I).

(1) Control access to the navigation lock and appurtenant features.

(2) Do not allow the public unrestricted access to gates, control rooms, operating machinery, or power supplies unless escorted by USACE personnel in conjunction with planned and approved visits.

(3) Control keys and locks in accordance with appendix D.

b. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Establish a continuous unsensored personnel barrier perimeter at the navigation lock control structure(s) and appurtenant assets/structures comprised of, at a minimum, of 2-minute, non-tested forced entry resistant components. In some instances the structure, or its components, can be accessed by the public (or an aggressor) with relative ease, additional protective measures (for example, securing building access ladders, manhole covers, louvers, and so forth) may be necessary to prevent unauthorized access to and/or operation of the structure(s).

(3) Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on or adjacent to project resources and on perimeter fencing and personnel and vehicle gates.

c. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Establish a sensored perimeter (also known as install IDS and CCTV systems) along/at the lock control structure(s), minimum 2-minute, non-tested forced entry resistant components perimeter(s).

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(4) Designate the resource as a restricted area.

6–21. Levee drainage structures

a. Physical protective measures (risk level I and II).

(1) Control access to drainage structure service bridge, if present, unless structure is in a remote or rural area where implementation of this is impractical.

(2) Install appropriate signage (for example, "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on or adjacent to drainage structure.

(3) Lock hatch covers and access doors.

(4) Install chain and lock on gate operating/lifting mechanisms to prevent unauthorized operation.

(5) Remove handles (for example, wheels, hand cranks, and so forth), to prevent unauthorized operation, based upon the judgment of the responsible commander.

(6) Control keys and locks in accordance with appendix D.

b. Physical protective measures (risk level III).

(1) All measures required for risk level I and II will be implemented.

(2) Install IDS and CCTV on the drainage structure.

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(4) Designate the resource as a restricted area.

6–22. Levee pumping stations

a. Physical protective measures (risk level I).

(1) Control access to pumping station pumps.

(2) Control keys and locks in accordance with appendix D.

b. Physical protective measures (risk level II).

(1) All measures required for risk level I will be implemented.

(2) Establish a continuous unsensored personnel barrier perimeter at the pumping station comprised of, at a minimum, 2-minute, non-tested forced entry resistant components. Typically this will involve installing USACE "Doors (2-minute resistant, non-tested)" on the pump station and hardening any first floor openings (for example, windows, vents, louvers, hatches, and so forth) or other "portals" through the pump station structure/building in excess of 96 square inches that are located less than 12 feet from the ground level and to similar openings above the first floor which can be reached from an elevated portion of the pumping station or an adjacent structure (for example, levee, drainage structure, and so forth) which provides ground level access. Long narrow openings with the shortest dimension measuring less than 6 inches are exempt from these requirements.

(3) Install appropriate signage (for example, "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on pump station and/or perimeter fence and personnel and vehicle gates.

c. Physical protective measures (risk level III).

(1) All measures required for risk levels I and II will be implemented.

(2) Establish a sensored personnel perimeter (install IDS and CCTV systems) along/at the pumping station, comprised of, at a minimum 2-minute, non-tested forced entry resistant components.

(3) Install security lighting, which is compatible with the CCTV system, at each alarm point/zone to enable assessment of every alarm location(s) during the hours of darkness.

(4) Designate the resource as a restricted area.

6–23. Petroleum, oils, and lubricants not at bulk storage facility

Apply the standards in chapter 3.

Section IV

Minimum Security Standards for Resources Not Requiring Risk Analysis

6–24. General Services Administration vehicles and U.S. Army Corps of Engineers-owned vehicles, boats, watercraft, and equipment

a. GSA vehicles and USACE-owned vehicles, boats, watercraft, and equipment are stored in both unfenced and fenced motor pools. On occasion, these resources are stored in a building; these are characterized herein as a "building motor pool."

b. Security measures.

(1) Establish, in writing, a district and/or project site-specific vehicle, boat, watercraft, and equipment key control plan or SOP. Include the SOP as a separate annex/appendix to the project's site-specific physical security plan.

(2) GSA vehicles and USACE-owned cars (passenger car), trucks (pickup), sport utility vehicles, mini-vans and other similar type vehicles may be stored in an unfenced, fenced, or building project motor pool.

(3) Other USACE-owned vehicles not listed above (for example, commercial truck, drill rig, water truck, dump truck, semi-trailer truck, truck trailer, and so forth), will be stored, when not in use, in a fenced or building project motor pool.

(4) USACE-owned equipment (includes all-terrain vehicle, utility terrain vehicle, tractor, forklift, skid steer, specialty vehicles/equipment, trailer, implements, and other like equipment) and heavy equipment (for example, loader, excavator, backhoe, dozer, motor grader, crane, and so forth) will be stored, when not in use, in a fenced or building project motor pool.

(5) USACE-owned watercraft will be stored, when not in use, in a fenced or building project motor pool. This does not include, nor applies to, USACE-owned tugboats, barges, and other specialty watercraft that are rarely taken out of the water and remained moored or docked, when not in use, on/at USACE-owned marinas, harbors, ports, or the like.

(6) Unfenced project motor pool requirements. No additional requirements.

(7) Fenced project motor pool requirements.

(a) Privately owned vehicles will be permitted to park in fenced motor pools based upon the judgment, and approved in writing, of the responsible commander.

(b) Entry to and exit from fenced project motor pools will be controlled. Exit/entry gates will, at a minimum, be secured (locked) in a closed position during nonduty hours. It is recommended to keep the exit/entry gates closed during duty hours, to the maximum extent feasible.

(c) Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on motor pool perimeter fence and personnel and vehicle exit/entry gates. Ensure sign(s) are easily identifiable by the public when the exit/entry gates are in both a closed and open position.

(d) Fencing securing civil works and like project motor pools will be in accordance with perimeter fencing requirements.

(e) Control motor pool keys and locks in accordance with appendix D.

(8) Building motor pool requirements.

(a) Privately owned vehicles will not be permitted to park in building project motor pools.

(b) Entry to and exit from building project motor pools will be controlled. Building doors will, at a minimum, be secured (locked) in a closed position during non-duty hours. It is recommended to keep the building doors closed during duty hours, to the maximum extent feasible.

(c) Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) on or adjacent to personnel and vehicle entry/exit doors.

6–25. Spillway outlet channel

a. The spillway outlet channel can vary from being grass to being rock lined channel to a very pronounced concrete chute/channel. Some grass/rock lined spillway channels are readily accessible or provide direct access to the public, where public accessible roads or walking paths can and do traverse across and through the grass/rock lined channel. Accessibility and applicability of any physical security or procedural measures at the grass lined channels will have to be handled on a case-by-case basis where site-specific measures are driven by the responsible commander's desired end state. Concrete lined spillway channels typically do not have or permit public access to them. The minimum standards provided herein are for the non-public accessible concrete lined chutes/channels.

b. Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) as needed on the public accessible portions of the outlet channel.

6–26. Transformers

a. Transformer locations and ownership vary within USACE. Transformers are often located adjacent to the powerhouse or in the switchyard. Transformers owned, operated, or maintained by others are (typically) not the responsibility of USACE to secure, despite being located on project property. This section applies to those transformers owned, operated, and maintained by USACE.

b. Security measures.

(1) Access to transformers will be controlled.

(2) Install appropriate signage (for example, "Off Limits to Unauthorized Personnel," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) as needed at, on, or adjacent to the transformer area(s).

(3) Control keys and locks in accordance with appendix D.

6–27. Penstocks, fish facilities, visitor center (stand-alone structure), administrative building, maintenance building, warehouse, and free access recreational areas

Security measures—

a. Access to penstocks, fish facilities, visitor center (stand-alone structure), administrative building, maintenance building, or any combination of the above, will be controlled based upon the judgment of the responsible commander.

b. Control access into free access recreational areas as deemed appropriate based upon the judgment of the responsible commander.

c. Install appropriate signage (for example, "No Unauthorized Vehicles," "Off Limits to Unauthorized Personnel," "No Unauthorized Personnel," "No Trespassing, U.S. Government Property," or similar message) as needed at, on, or adjacent to these resources.

d. Control keys and locks in accordance with appendix D.

6–28. U.S. Army Corps of Engineers-owned and privatized utilities

a. Utility systems include natural gas, water, wastewater, electricity, and communications services and infrastructure. Utility systems that serve civil works and like projects may be designated in writing a MEVA and/or restricted area based on the judgment of the responsible commander. The MEVA and/or restricted area designation could apply to utility services, regardless of ownership or operation, to include USACE-owned and privately owned resources.

b. Security measures.

(1) Access to the utility will be controlled.

(2) Provide locks on utility structures (for example, cabinets, perimeter fence, and so forth) to the extent feasible.

(3) Control keys and locks in accordance with appendix D.

6–29. Critical communications facilities

Apply the standards in chapter 3.

6–30. Hand tools, tool sets, and kits and shop equipment

Apply the standards in chapter 3.

6–31. Supply rooms

Apply the standards in chapter 3.

6–32. Postal unique items

Apply the standards in chapter 3.

6–33. Minimum security standards for office machines

Apply the standards in chapter 3.

Appendix A

References

Section I

Required Publications

AR 25–2
Information Assurance (Cited in para 4–25*j*.)

AR 40–3
Medical, Dental, and Veterinary Care (Cited in para 4–8.)

AR 40–61
Medical Logistics Policies (Cited in4-7.)

AR 190–11
Physical Security of Arms, Ammunition, and Explosives (Cited in para 1–4*e*(2).)

AR 190–13
The Army Physical Security Program (Cited in para 1–4*b*(1).)

AR 190–45
Law Enforcement Report (Cited in para 4–15*a*(5).)

AR 380–5
Department of the Army Information Security Program (Cited in para 3–9*d*.)

AR 380–27
Control of Compromising Emanations (Cited in para 4–31*b*(3).)

AR 380–67
Personnel Security Program (Cited in para 4–6*h*.)

AR 525–13
Antiterrorism (Cited in para 2–3*d*.)

AR 525–26
Infrastructure Risk Management (Army) (Cited in para 3–19*g*(6).)

AR 710–2
Supply Policy Below the National Level (Cited in para 3–9*a*(2).)

AR 870–5
Military History: Responsibilities, Policies, and Procedures (Cited in para 5–14.)

AR 870–20
Army Museums, Historical Artifacts, and Art (Cited in para 5–13.)

Controlled Substance Act of 1970
(Cited in para B–3*e*.) (Available at https://www.deadiversion.usdoj.gov/21cfr/21usc/.)

DA Pam 190–51
Risk Analysis for Army Property (Cited in para 2–2*a*.)

DODD 3020.40
Mission Assurance (Cited in para 3–19.)

DODI 5200.08
Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB) (Cited on title page.)

DODM 4160.21
Defense Materiel Disposition Manual: Instructions for Hazardous Property and Other Special Processing Materiel (Cited in para 3–17*c*(3).)

ER 1110–1–8162
Engineering and Design, Design and Construction Policy for Electronic Security Systems (Cited in para 6–4*b*.) (Available at http://www.publications.usace.army.mil/.)

MIL–STD–130N
Identification Marking of U.S. Military Property (Cited in para C–1*b*(4).)

STD 872–90–03
FE6 Chain-Link Security Fence Details for Non-Sensored Fence (Cited in para 3–2*b*(3).) (Available at https://pdc.usace.army.mil/library/drawings/fence/.)

STD 872–90–04
FE6 Chain-Link Security Fence Details for Sensored Fence (Cited in para 6–3*c*(3).) (Available at https://pdc.usace.army.mil/library/drawings/fence/.)

STD 872–90–11
Farm Style 3 Strand Barbed-Wire Fence Details (Cited in para 6–3*d*(2).) (Available at https://pdc.usace.army.mil/library/drawings/fence/.)

STD 872–90–12
Farm Style 4 Strand Barbed-Wire Fence Details (Cited in para 6–3*d*(2).) (Available at https://pdc.usace.army.mil/library/drawings/fence/.)

STD 872–90–13
Farm Style 5 Strand Barbed-Wire Fence Details (Cited in para 6–3*d*(2).) (Available at https://pdc.usace.army.mil/library/drawings/fence/.)

STD 872–90–14
Farm Style Woven-Wire Fence Details (Cited in para 6–3*d*(2).) (Available at https://pdc.usace.army.mil/library/drawings/fence/.)

UFC 3–460–01
Design: Petroleum Fuel Facilities (Cited in para 3–19*b*(1).) (Available at http://www.wbdg.org/ffc/dod.)

UFC 3–530–01
Interior and Exterior Lighting Systems and Controls (Cited in para 3–3.) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–010–01
DOD Minimum Antiterrorism Standards for Buildings (Cited in para 3–26*f*.) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–020–01
DOD Security Engineering Facilities Planning Manual (Cited in para 1–8*a*.) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–020–02FA
Security Engineering: Concept Design (FOUO) (Cited in para 6–7*b*.) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–020–03FA
Security Engineering: Final Design (FOUO) (Cited in para 6–7*b*.) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–021–02
Electronic Security Systems (Cited in para 6–4*a*.) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–022–02
Selection and Application of Vehicle Barriers (Cited in para 6–15*b*(5).) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–022–03
Security Fences and Gates (Cited in para 3–2*a*(1).) (Available at http://www.wbdg.org/ffc/dod.)

UFC 4–510–01
Design: Military Medical Facilities (Cited in para 4–5.) (Available at http://www.wbdg.org/ffc/dod.)

UFGS 28 10 05
Electronic Security Systems (ESS) (Cited in para 3–4*a*.) (Available at http://www.wbdg.org/ffc/dod.)

UFGS 28 20 02
Central Monitoring Services for Electronic Security Systems (Cited in para 3–4*c*.) (Available at http://www.wbdg.org/ffc/dod.)

UFGS 32 31 13
Chain Link Fences and Gates (Cited in para 3–2*b*(3).) (Available at http://www.wbdg.org/guides-specifications.)

UFGS 32 31 13.53
High-Security Chain Link Fences and Gates (Cited in para 6–3*c*(3).) (Available at http://www.wbdg.org/guides-specifications.)

UFGS 32 31 26
Wire Fences and Gates (Cited in para 6–3*d*(2).) (Available at http://www.wbdg.org/guides-specifications.)

UL 437
Standard for Key Locks (Cited in para D–6*c*(1).) (Available at https://standardscatalog.ul.com/.)

UL 1037
Standard for Antitheft Alarms and Devices (entire unit) (Cited in para D–6*c*(1).) (Available at https://standardscatalog.ul.com/.)

UL 1332
Standard for Organic Coatings for Steel Enclosures for Outdoor Use Electrical Equipment (Cited in para D–6*c*(1).) (Available at https://standardscatalog.ul.com/.)

UL 1610
Standard Central-Station Burglar-Alarm Units (Cited in para D–6*c*(1).) (Available at https://standardscatalog.ul.com/.)

Section II

Related Publications

AR 11–2
Managers' Internal Control Program

AR 25–1
Army Information Technology

AR 25–30
Army Publishing Program

AR 30–22
Army Food Program

AR 40–5
Preventive Medicine

AR 40–7
Use of U.S. Food and Drug Administration-Regulated Investigational Products in Humans Including Schedule I Controlled Substances

AR 40–66
Medical Record Administration and Health Care Documentation

AR 40–68
Clinical Quality Management

AR 40–400
Patient Administration

AR 58–1
Management, Acquisition, and Use of Motor Vehicles

AR 95–1
Flight Regulations

AR 95–2
Air Traffic Control, Airfield/Heliport, and Airspace Operations

AR 190–17
Biological Select Agents and Toxins Security Program

AR 190–54
Security of Nuclear Reactors and Special Nuclear Materials

AR 190–59
Chemical Agent Security Program

AR 380–40
Safeguarding and Controlling Communications Security Material (U)

AR 385–10
The Army Safety Program

AR 420–1
Army Facilities Management

AR 708–1
Logistics Management Data and Cataloging Procedures for Army Supplies and Equipment

AR 710–3
Inventory Management Asset and Transaction Reporting System

AR 725–50
Requisitioning, Receipt, and Issue System

AR 735–5
Property Accountability Policies

AR 740–26
Physical Inventory Control

ATP 3–39.32
Physical Security

DA Pam 25–403
Guide to Recordkeeping in the Army

DA Pam 30–22
Operating Procedures for the Army Food Program

DA Pam 40–11
Preventive Medicine

DA Pam 385–24
The Army Radiation Safety Program

DA Pam 710–2–1
Using Unit Supply System (Manual Procedures)

DA Pam 750–8
The Army Maintenance Management System (TAMMS) User's Manual

DOD 4525.6–C
DOD Postal Supply Catalog

DOD 4525.8–M
DOD Official Mail Manual

DODD 4270.5
Military Construction

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

Federal Highway Administration's Manual of Uniform Traffic Code Devices
(Available at https://mutcd.fhwa.dot.gov/.)

Federal Supply Catalog
(Available at http://www.federalsupply.com/.)

NATO Standard Design Fencing
(Available at https://pdc.usace.army.mil/forums/general/fence.)

Nonstandard Drug Enforcement Administration (DEA) Schedule II, III, IV, and V Controlled Substances
(Available at https://www.dea.gov/druginfo/ds.shtml.)

North American Electric Reliability Corporation's Critical Infrastructure Protection Standards
(Available at http://www.nerc.com/pa/stand/pages/cipstandards.aspx.)

PL 104–191
Health Information Portability and Accountability Act of 1996

TB 43–0209
Color, Marking, and Camouflage Painting of Military Vehicles, Construction Equipment, and Materials Handling Equipment

TM 10–1670 series
As required by Army resources listed in this publication.

UL Standard 1981
Central-Station Automation Systems

21 CFR 1308.11
Schedule I

21 USC 812
Schedules of controlled substances

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://www.armypubs.army.mil); and standard forms (SF) are available on the U.S. General Services Administration website (https://www.gsa.gov).

DA Form 11–2
Internal Control Evaluation Certification Statement

DA Form 1687
Notice of Delegation of Authority–Receipt for Supplies

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 2062
Hand Receipt/Annex Number

DA Form 3161
Request for Issue or Turn-In

DA Form 4930
Alarm/Intrusion Detection Record

DA Form 5248–R
Report of Unfavorable Information for Security Determination

DA Form 5513
Key Control Register and Inventory

DA Form 7278
Risk Level Worksheet

DA Form 7708
Personnel Reliability Screening and Evaluation Form

SF 700
Security Container Information

SF 701
Activity Security Checklist

SF 702
Security Container Check Sheet

Appendix B

Storage Structure Security

B–1. General

This appendix includes construction standards for secure storage structures and vaults to be used in securing the resources identified by this regulation. The construction standards for each type of storage structure vary according to the risk level associated with the stored resources. These standards will provide the minimum acceptable security for the stored resources according to their associated risk levels. Fully effective protection of assets against forced entry requires providing building components which delay aggressors for a time at least equal to the time required for a response team to arrive at the facility in response to an alarm. This further requires IDS to detect aggressors before they breach the surface of the secure storage structure or vault. Refer to UFC 4–020–02FA for further guidance on delay times and complementary installation of IDS. The measures required by this appendix may be replaced with compensatory measures where the required measures are infeasible. The servicing facility engineer will make all determinations of equivalent construction and delay time provided by construction.

B–2. Secure storage structure standards

Buildings, areas, and rooms may be considered secure storage structures if they meet the following standards for doors, windows, walls, ceilings, and floors. All building components within the secure storage structure should provide an equivalent degree of security.

a. Doors.

(1) *Risk level I.*

(a) Doors will be a minimum of 1 3/4-inch thick solid core wood or hollow steel. Hollow steel doors will be industrial type construction with at least 20-gauge skin plate thickness and will be internally reinforced with vertical steel stiffeners. Door frames will be constructed of a minimum of 18–gauge steel. Doors with locking systems exposed to the outside will be kept to the absolute minimum number needed based on operational considerations. In addition, the doors will meet the following installation requirements:

(b) Door hinge mounting screws should not be exposed to the exterior of the facility. If screws are exposed, they will be spot welded, peened, covered, or filled with material in a way to prevent easy removal. Alternatively, use hinges with non-removable hinge pins or with security studs. Nails will not be used to mount hinges or any other door hardware.

(c) Door hinge pins should not be exposed to the exterior of the facility. If they are exposed, they will have fixed-pin hinges, be spot welded, covered, filled, or otherwise secured to prevent easy removal.

(d) Doors secured from the inside will be secured with a deadbolt-locking device, crossbar, or similar locking device resistant to jimmying and manipulation from the outside. Locking devices will conform to American National Standards Institute/Builders Hardware Manufacturers Association (ANSI/BHMA) A 156.13 for mortise locks and latches.

(2) *Risk level II.*

(a) Doors will be a minimum of 16–gauge minimum hollow steel construction, or 1 3/4-inch solid core wood door with a 20-guage steel skin, with a minimum of frame construction of 16-gauge steel. Installation requirements for risk level I also apply.

(b) Alternatively, doors or pairs of doors will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 equal to or greater than the response time.

(3) *Risk level III.*

(a) Doors will be a minimum of 1 3/4-inch solid core wood with wood block cores and 12-gauge minimum steel plate on both sides of the door, or doors will be 12-gauge minimum hollow steel doors reinforced with vertical stiffeners at 6 inches on center.

(b) Door frames will be constructed of 16–gauge steel minimum and will be grouted full. Alternatively, doors or pairs of doors will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 and UFC 4–020–02FA equal to or greater than the response time.

b. Windows. The following apply to all first floor openings, except doors, in excess of 96 square inches that are located less than 12 feet from the ground level and to similar openings above the first floor which can be reached from an elevated portion of the structure or an adjacent structure which provides ground level access. Long narrow openings with the shortest dimension measuring less than 6 inches are exempt from these requirements. If window air conditioning is used, provide steel bars, 9-gauge expanded metal mesh, or welded steel grating per the following risk levels:

(1) *Risk level I.* Operable windows will have adequate individual locking devices. Windows will also be covered with either 1/2–inch diameter bars spaced at 6 inches on center each way, 9-gauge expanded metal mesh, or 9-gauge chain link fence fabric in steel frames.

(2) *Risk level II.* Windows will be inoperable except where operable windows are required by other criteria. Operable windows will have adequate locking mechanisms such that they cannot be opened from the outside. They will be covered with bars or mesh as for risk level I and the glass will be covered with 4mil fragment retention film, 1/2-inch thick laminated glass or polycarbonate security glazing. Alternatively, windows will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 and UFC 4–020–02FA equal to or greater than the response time.

(3) *Risk level III.* Windows will be inoperable and they will be covered with bars or mesh as for risk level I and will have 1/2-inch thick laminated glass, or plastic security glazing. Alternatively, windows will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 and UFC 4–020–02FA equal to or greater than the response time.

c. Walls.

(1) *Risk level I.* Walls will be constructed with of at least 1/2-inch plywood, 1-inch tongue-in-groove wall boards, or 26–gauge steel siding (typically) added to the exterior side of wood or metal stud wall with gypsum wall board on the interior face.

(2) *Risk level III.* Walls will be constructed of 8–inch minimum thickness reinforced concrete masonry or 4-inch minimum thickness reinforced concrete. Alternatively, walls will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 and UFC 4–020–02FA equal to or greater than the response time.

d. Floors and ceilings. The following requirements do not apply to slab on grade floors. No special requirements apply for such floors.

(1) *Risk level I.* Floors and ceilings will be constructed with at least 1/2–inch plywood, 1–inch tongue-in-groove solid wood boards, or 24–gauge steel deck added to the exterior side of either a floor or ceiling.

(2) *Risk level II.* Floors and ceilings will be constructed as for risk level I with the addition of 5/16–inch expanded metal mesh or 10–gauge 6x6 woven wire fabric. Alternatively, floors and ceilings will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 and UFC 4–020–02FA equal to or greater than the response time.

(3) *Risk level III.* Floors and ceilings will be constructed of 4-inch minimum thickness reinforced concrete. Alternatively, floors and ceilings will provide delay time against unlimited hand tools in accordance with UFC 4–020–01 and UFC 4–020–02FA equal to or greater than the response time.

B–3. Controlled substance storage vault and pharmacy storage structural standards

a. UFC 4–510–01 will be used for new and existing vaults.

b. GSA-approved Class 5–A vault doors will be used for new construction.

c. A GSA-approved container may be used for storage of small quantities of controlled substances.

d. These standards apply only to the storage of controlled substances, and will not be applied to entire pharmacies.

e. Drugs classified as schedule I or II controlled substances under the Controlled Substance Act of 1970 must be stored in safes or vaults. Drugs classified as Schedule III–V may also be stored in safes or vaults as deemed appropriate by the using military department.

f. Controlled substance storage vaults located at RC SAF with civil support team or similar activities will be protected by an IDS.

Appendix C

Marking of Army Property

C–1. Purpose of marking property

a. Many items of Army property cannot be distinguished from similar civilian items and are attractive targets for pilferage. These items can be easily disposed of and detection is difficult.

b. Marking individual items of Army property will enhance the security of the property by—

(1) Deterring the theft or pilferage of the items.

(2) Increasing the difficulty of disposing of the property because illegal possession can result in prosecution and because markings are not always easily removed.

(3) Increasing the chances of recovery of the property and prosecution of the criminal perpetrator by providing a positive means of identifying the property and tracking it.

(4) Markings will be made in accordance with MIL–STD–130N.

C–2. Determining whether to mark property

a. The decision to mark Army property rests with the commander/director or activity chief and is not mandatory except for museum AA&E. In making the decision to mark Army property other than museum AA&E, the commander should consider such risk factors as—

(1) Vulnerabilities and threat to property losses.

(2) Monetary replacement value of the property.

(3) Criticality of the property to include effects of loss and mission performance.

b. If the property has no serial number and is reported lost, the chances of return will depend on the ability of the recovering agency to determine the owner through the reporting system. If there is no identifying data on the property, the chances of return are virtually nonexistent.

C–3. Marking museum weapons and ammunition

Weapons, with or without serial numbers, will be marked with a catalog number as follows—

a. Location of catalog number. The numbers should be placed on the inside of the trigger guard or on the breach of the barrel opposite the lock.

b. Marking methods.

(1) *Semipermanent markings.* Semipermanent markings can be applied by using a radiograph or quill pen and non–waterproof black India ink or oil paint (watercolors are not recommended as they may not adhere). After the paint has dried, apply a coat of varnish over the numbers. (See paragraph C–3*b*(2) regarding records maintenance.)

(2) *Permanent markings.* Permanent markings can be applied with a scriber or engraving tool. Such labeling, which can never be removed from the object, should be made only by specific arrangement with the responsible curator and written permission of the U.S. Army Center of Military History. This type of labeling is discouraged if the historical value of the item will be impaired through its application; however, if this is the case, a detailed description of the item should be kept. This includes recording potentially unique characteristics such as scratches and discoloration and their dimensions and location. The description will be retained on file by the chief curators, as directed in AR 870–20. Photographs, especially color, are extremely useful.

C–4. Marking other Army property

a. Standard marking system. Marking property is sensible if it identifies a specific item as belonging to a particular organization. The recommended standard marking of Army property follows:

(1) Use a "USA" prefix to alert the recovering agency that the property belongs to the U.S. Army.

(2) Have a unit identifier. Use the unit identification code. An abbreviation of the office, unit, or activity designation, such as vehicle bumper markings outlined in technical bulletin (TB) 43–0209, may also be provided.

(3) Include as the last item in the code a sequential number or letter that identifies the specific item from like items in the using organization. This procedure could be used if more than one item of a type exists and no serial numbers exist to distinguish between these items.

b. Recording marked items. Records of marked items including a brief description, serial number, and name of person to whom hand receipted, preferably the user, should be retained on file.

c. Identifying and locating owning units of Army property. Usually the installation or unit provost marshal or security officer will be the initiator of action to identify and locate the property owner. The provost marshal or security officer maintains liaison with civilian law enforcement agencies to ensure they are aware of the standard Army marking system

and is the point of contact upon recovery of the property. The unit should notify the provost marshal or equivalent security officer when the Army property is determined missing.

Appendix D

Keys, Locks, Locking Devices, Hasps and Chains, and Protective Seals

D–1. General

a. Guidance on security requirements for keys, locks, locking devices, hasps and chains, and protective seals is contained in this appendix. Additional requirements for AA&E are in AR 190–11.

b. Only approved locks and locking devices (including hasps and chains) will be used. All questions regarding locks and locking devices (including hasps and chains) meeting military or Federal specifications will be addressed to the Naval Facilities Engineering and Expeditionary Warfare Center, Code CI8, DOD Lock Program, 1100 23rd Avenue, Port Hueneme, CA 93043–4370, commercial (805) 982–1212 (DSN 551–1212), (800) 290–7607, or http://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html.

c. Under no circumstances will any keys, locks, or alternate keys or locks be placed in a security container that contains or stores classified material.

d. Access to protected resources will be limited to the minimum number of persons needed for operational necessity.

e. Maintain accountability of keys, key cards and other entry control tokens, and combinations to locking devices and systems to include both issued and non-issued stock.

D–2. Key control officer, key custodian, and alternate key custodian

a. A key control officer—

(1) Will be appointed, in writing, by the responsible commander or director to monitor the unit, or organization, key control program. The designation memorandum will be included in the physical security plan at the battalion level and higher headquarters.

(2) Sign over all unit, or organizational keys, to include key box keys to the primary and alternate key custodians.

(3) Ensure that key and lock inventories are conducted semiannually.

(4) When a key control officer or alternate on orders need to sign for a key(s) they will have key control custodian sign the key(s) over to them on a key control register.

b. A primary and alternate key custodian will—

(1) Be appointed, in writing, by the responsible commander or director to issue and receive keys and maintain accountability for office, unit, or activity keys. The designation memorandum will be included in the physical security plan.

(2) Make certain that personnel designated to issue, receive, and account for keys in their absence, clearly understand local key control security requirements.

(3) Maintain a key control register at all times to ensure continuous accountability for keys of locks used to secure Government property.

(4) Be listed on an access roster.

(5) When a key control custodian or alternate need to sign for a key(s) they will have the other key control custodian sign the key(s) over to them on a key control register.

D–3. Key control register

Keys will be signed out to authorize personnel in person, not digitally on a key control register. The key control register, DA Form 5513 (Key Control Register and Inventory) is approved for use to meet the requirements of this regulation. When not in use, the key control register will be kept in a locked container that does not contain or store classified material and to which access is controlled.

D–4. Key depository

a. A lockable container, such as a safe or filing cabinet, or a key depository (made of at least 26–gauge steel, equipped with a tumbler–type or keyed locking device and permanently affixed to a wall) will be used to secure keys.

b. The key depository will be located in a room where it is kept under 24–hour surveillance or in a room that is locked when unoccupied.

c. An electronically-controlled key depository may be used if it is constructed of at least 26–gauge steel, can be affixed to a wall, and produces an inventory report with information equivalent to that contained in the DA Form 5513. If the key depository is designed as a drawer-style system that is positioned on the floor, the system will be secured to an immovable object such as to the floor or to a building support beam unless the empty weight exceeds 500 pounds and is not mounted on rollers.

D–5. Locks

a. The following limitations apply:

(1) Keyed-alike locksets and master-keyed locksets will not be used for multiple vehicles, but can be used for a single vehicle and its compartments.

(2) Control of keys for keyed-alike locksets and master-keyed locksets will be limited to the least practical number of responsible persons designated by the responsible commander.

b. If a master-keyed lockset is not authorized, a key operated, pin-tumbler deadbolt with a one-inch throw, or a key operated low security padlock, will be used to safeguard unclassified, nonsensitive resources if a lock is required. Selection will be based on the protected resource value, mission essentiality, and vulnerability to criminal attack. All questions regarding approved locks and locking devices will be addressed to the DOD Lock Program per paragraph D–1.

c. Padlocks, key/lock cores, and keys not in use will be secured in a locked container that does not contain or store classified material. Access to the container will be controlled.

d. The low security padlocks, sometimes referred to as secondary locks, are used for administrative control, on gates barring access to in-process/production facilities, for securing weapons racks contained within secured areas, and where secondary locks are specified. These padlocks provide only minimal resistance to forced or surreptitious entry and must not be used to secure classified material. Low security padlocks must be key-retaining and be stamped with "US," or "US Set" if a padlock set. Key-retaining means the key must be captive (unmovable) in the cylinder when the padlock is unlocked.

e. As with other padlocks, when used chains will be commensurate with its shackle strength. NSNs for approved locks are available at http://www.navfac.navy.mil/go/locks.

f. Electronic locks and locking systems may be used unless specifically prohibited, and will have the following minimum design criteria—

(1) Be compliant with Federal Information Processing Standard.

(2) Have back-up battery power of at least 4 hours.

(3) Be placed in the fail-secure mode.

(4) Have appropriate life-safety hardware.

(5) Have a mechanical key override.

(6) Have serial-numbered key devices accounted for on a DA Form 5513 or an electronic form containing equivalent information.

(7) Padlocks, a 1-inch throw deadbolt, or mortise locks will be used if the standards above cannot be met.

g. AR 735–5 establishes guidance concerning financial liability for the loss of a key due to negligence or willful misconduct.

D–6. Rapid-entry key boxes

a. Emergency personnel such as police and firefighters will be provided card keys, key codes, lock combinations, keys, or other similar entry control devices needed to enter the perimeter of facilities. Emergency personnel are not authorized entry control devices to designated restricted areas. A single rapid-entry box can be utilized by all emergency personnel; there is no need to install separate boxes for each organization such as police and firefighters.

b. Entry control devices (for example, key, card, access code record) may be secured in a rapid-entry key box affixed to the exterior of the facility or adjacent to it to avoid emergency personnel having to maintain a large amount of entry control devices.

c. Rapid-entry key box specifications will meet—

(1) Underwriters Laboratory (UL) standards 437, 1037, 1332, and 1610.

(2) A factory mutual equivalency to the UL standards.

(3) A nationally recognized test laboratory equivalency to the UL standards.

(4) Organizations outside the continental United States will employ a local equivalency per the status of forces agreement.

d. Keys to rapid-entry boxes will be inventoried and signed for at each shift change. Entry control devices maintained within the rapid-entry boxes will be inventoried on a monthly basis.

D–7. Key and lock accountability

a. A key/code control custodian will be appointed in writing by the responsible commander, director, or designated representative.

b. The number of personnel having keys or electronic lock codes will be kept to the fewest personnel feasible consistent with efficient operations.

c. Locks will be re-keyed when a person leaves the organization without turning the key back into the custodian, or a key is lost, codes changed when a person leaves the organization or a code compromised.

d. Codes used to activate electronic locks, pushbutton locks and other locking devices will be changed on a semiannual basis at a minimum. If a code is a unique number and only assigned to one person, the code does not need to be changed unless it is compromised. Issuances of codes will be recorded on the SF 700 (Security Container Information) or an equivalent form.

e. A SOP will be published for the control of badges, keys, combinations, and/or cards. The SOP will include requirements for the revocation of keys, revising authorization lists, changing of locks, codes and combination to lock, and surrendering of keys and key cards.

f. Sharing of individually issued combinations/ codes is prohibited.

g. Keys, key cards, other electronic key tokens, lock combinations, and electronic locks not installed will be accounted for at all times. Keys to locks in use will be checked at the end of each duty day. Differences between keys on hand and the key control register will be reconciled.

h. Padlocks and their keys will be inventoried by serial number semiannually. A written record of the inventory will be retained until the next inventory is conducted.

i. When a key to a padlock is lost or missing, an inquiry will be conducted and the padlock replaced or immediately reconciled.

j. A key and lock inventory will be maintained and list—

(1) Keys.

(2) Locks.

(3) Key serial numbers.

(4) Lock serial numbers.

(5) Location of locks.

(6) Number of keys maintained for each lock. This list will be secured in the key depository.

k. Locks and keys which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate. Custodian should take care as to not mark the key and lock with the same serial numbers/markings to avoid easy identification by unauthorized users.

D–8. Additional key and lock controls for Intrusion Detection System and Intrusion Detection System key containers

a. Keys to IDS (operational and maintenance) or key containers will not be removed from the installation or USACE civil works and like projects except to provide for protected storage elsewhere. Keys to locks securing key containers will be afforded physical protection equivalent to that provided by the key itself. Keys to containers and IDS will be maintained separately from other keys, and will be accessible only to those personnel whose official duties require access to them.

(1) A current roster of these personnel will be kept within the unit, agency, or organization.

(2) The roster will be protected from public view.

(3) The roster will be signed by the responsible commander or designated official and will contain the names of personnel authorized to receive keys from the key custodian (see para D–8*d*).

(4) At no time will keys be in the custody of a person not listed on the roster.

b. Keys to containers and IDS may be secured together in the same container. However, under no circumstances will keys and locks or alternate keys or locks be placed in any security container that contains or stores classified material.

(1) When arms and ammunition are stored in the same areas, keys to those storage areas may be maintained together, but separately from other keys that do not pertain to AA&E storage. The number of keys will be held to the minimum essential. Keys may not be left unattended or unsecured at any time.

(2) Keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, will be kept separate from other IDS keys. Access will be permitted only to authorized maintenance personnel.

(3) IDS operational keys will be stored in containers of at least 20-gauge steel equipped with GSA-approved padlocks or GSA-approved built-in changeable combination locks, or in GSA-approved containers that do not contain classified material.

(4) Containers weighing less than 500 pounds will be fastened to the structure with bolts or chains equipped with secondary padlocks to preclude easy removal. Any bolting or welding directly to GSA-approved containers permanently voids their GSA approval unless recertified by a GSA-approved inspector.

c. An investigation will be immediately conducted in the event of lost, misplaced, or stolen keys. The affected locks or cores to locks will be immediately replaced. Replacement or reserve locks, cores, and keys will be secured to preclude access by unauthorized personnel.

d. A key and lock custodian will be appointed in writing. Only the commander and the key custodian (or alternate, if appointed) will issue keys to personnel on the key access roster (para above). When a key control officer or alternate on orders need to sign for a key(s) they will have key control custodian sign the key(s) over to them on a key control register.

e. The key and lock custodian's duties will also include procurement and receipt of keys and locks and investigation of lost or stolen keys. The key and lock custodian will maintain a record to identify each key and lock and combinations to locks used by the activity, including replacement or reserve keys and locks. The record will show the current location and custody of each key and lock.

f. A key control register will be maintained at the unit level to—

(1) Enforce continuous accountability for keys.

(2) Enforce positive control of keys.

(3) Establish responsibility for the custody of stored AA&E. DA Form 5513 will be used for this purpose.

(4) Completed key control registers will be retained in unit files for a minimum of 1 year.

(5) When authorized personnel are charged with the responsibility for safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys.

g. When the sealed container of keys is transferred from one person to another, the unbroken seal is evidence that the keys have not been disturbed. The seal need not be broken for daily or monthly inventory of keys. However, evidence of tampering with a sealed container will require an inventory of the keys and such other action as may be required by the commander concerned. The seal will be broken and the keys inventoried during the 100 percent semiannual or higher headquarter inspections and resealed once complete.

h. If the keys are not placed in a sealed container, an inventory of keys will be made by serial number or other identifying information of the key (for example, stamped number on key). The inventory and change of custody will be recorded.

i. Inventory records will be retained in unit files for a minimum of 1 year.

j. Combinations to locks on GSA-approved vault doors or GSA-approved containers will be changed semiannually or upon change of custodian or of other person having knowledge of the combination, or when the combination has been subject to possible compromise. Combinations will also be changed when a container is first put into service. The combination shall be recorded using SF 700 (Security Container Information), sealed in the envelope provided, and stored in a container meeting storage requirements indicated in AR 380–5. No other written record of the combination will be kept. Controls will be established to make certain that the envelopes containing combinations to locks are not made available to unauthorized personnel.

k. Replacement of lock cylinders and broken keys for high-security locks may be requested through the DOD Lock Program per paragraph D–1.

D–9. Additional lock and key requirements for aircraft and vehicle storage

Facilities in which vehicles or aircraft are stored with sensitive items aboard will be secured by approved low security padlocks. Aircraft will be secured with manufacturer-installed or approved modification work order door-locking devices when not in use. All hatches and other openings to track vehicles which cannot be secured from the inside will be secured on the outside with approved low security padlocks.

D–10. Chains

Chains for securing Army resources will be heavy-duty hardened steel or welded, straight link galvanized steel, 5/16-inch thickness or equivalent in accordance with DODM 5100.76.

D–11. Use and control of protective seals

a. Seals custodian. A primary or alternate seal custodian will—

(1) Be appointed in writing to issue and receive seals and maintain seal accountability for all commands using protective seals.

(2) Make certain that persons designated to issue, receive, and account for seals in their absence, clearly understand local seal control requirements.

(3) Maintain a seal control register at all times to ensure continuous accountability for seals used to secure Government property.

b. Purpose of the seal. The purpose of the seal is to show whether the integrity of a storage facility, vehicle, rail shipment, or container has been compromised. A plain seal is not a lock, although combination items referred to as seal–locks are available. The purpose of a seal, no matter how well constructed, is defeated if strict accountability and disciplined application are not maintained.

c. Ordering and storing seals. Seal construction specification should include—

(1) *Durability.* Seals must be strong enough to prevent accidental breakage during normal use.

(2) *Design.* Seals must be sufficiently complex to make unauthorized manufacture of a replacement seal difficult.

(3) *Tamperproof.* Seals must readily provide visible evidence of tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.

(4) *Individually identifiable.* Seals must have embossed serial numbers and owner identification.

(5) *Unused seals.* Seals not issued for actual use will always be secured in a locked, metal container with controlled access. Only seal custodians and alternates will have access. Recorded monthly inventories will be conducted to preclude undetected loss of seals.

d. Accounting for seals. Seal custodians will maintain seal logbooks, in hard cover, rather than in loose–leaf books.

(1) Issue of seals to a using office, unit, or activity custodian will reflect date of issue, name of recipient, and seal serial numbers.

(2) Issue of a seal for actual use by a custodian will reflect the seal number, date and time applied, identification of items to which applied (and location on item if other than main door(s)), and the name of the person applying the seal. For outbound loaded trailers, railcars, and container shipments, the appropriate trailer, railcar, or container number and load destination will be noted.

e. Application of seals.

(1) Seal all doors and openings, not merely the main one.

(2) Run seal straps through hasp only once. Seals wrapped around several times become illegible.

(3) Listen for an audible click when inserting point of seal into sheath.

(4) For positive closure, tug down on strap and twist the point section inserted into the locking mechanism.

f. Checking seals. Commands using seals will develop requirements for checking them. These requirements will include actions to be taken to break a seal and actions to be taken upon finding a broken seal.

g. Disposition of used seals.

(1) All shipping documents will reflect seal number(s). All seals will be verified with seal log, shipping documents, or other appropriate documents before removal and disposal.

(2) Seals must be defaced sufficiently upon removal so that they cannot be used to simulate a good seal. They may be disposed of in normal trash.

(3) If the user seal log is located on the same installation, the custodian will be advised of the destruction of the seal, or the seal will be returned to the custodian. The custodian will annotate the date and time removed and the name of the person removing the seal across from the original entry on the seal log.

h. Changing seals. The colors of seals will be changed periodically as an additional physical security measure.

Appendix E

High-Value Asset Security Cage

E–1. Overview

The HVASC is available from the U.S. Army Integrated Logistics Support Center. The HVASC was developed to provide a secure, efficient means to store high-value items in a place such as a supply room rather than using arms room space. The HVASC meets the double barrier requirement in this regulation if high-value resources are stored in a properly locked HVASC located in a locked room. In this case, a locked room does not require the construction standards in appendix B of this regulation.

E–2. Ordering

a. The HVASC is available through supply channels as a class II item in four configurations.

(1) NSN 5411–01–522–4821 (HVASC, supply, green).

(2) NSN 5411–01–522–4823 (HVASC, supply, tan).

(3) NSN 5411–01–522–4822 (HVASC, portable, green).

(4) NSN 5411–01–522–4816 (HVASC, portable, tan).

b. Supply configuration: One security container, weight: 1061 pounds; height: 72 inches; width: 60 inches; depth: 33.50 inches.

c. Portable configuration:

(1) Lower container, weight: 531 pounds; height: 37 inches; width: 33 inches; depth: 44.75 inches.

(2) Upper container, weight: 412 pounds; height: 29 inches; width: 33 inches; depth: 45 inches.

(3) Assembled container, weight: 943 pounds; height: 66 inches; width: 33 inches; depth: 45 inches.

E–3. High-value asset security cage security

a. Containers weighing less than 500 pounds will be fastened to the structure (or fastened together in groups totaling more than 500 pounds) with bolts or chains equipped with secondary padlocks.

b. Containers weighting more than 500 pounds but have attached wheels or are easily moveable will be fastened to the structure with bolts or chains equipped with secondary padlocks.

Appendix F

Control of Bolt Cutters

F–1. General

Bolt cutters are subject to requirements for accountability, security, and handling. The purpose of this control is increase key accountability, contain costs incurred by replacing cut padlocks, and incidences of unauthorized removal of equipment.

F–2. Requirements

a. When not in use, bolt cutters will be secured in the unit supply room in a container secured with an authorized lock. The keys to these storage areas will be controlled per appendix D of this regulation.

b. A hard-covered logbook will be maintained by supply personnel for the control and accountability of bolt cutters.

(1) Primary and alternate key control personnel are the only personnel authorized to be issued the bolt cutters. When issued, supply personnel will notate in the log book the date of issue, name of recipient, purpose for issue (exact location of lock to be cut), and the initials of the supply person who is issuing the bolt cutters.

(2) Supply personnel will then have the key control custodian sign for the bolt cutters using DA Form 3161 (Request for Issue or Turn-In) or DA Form 2062 (Hand Receipt/Annex Number).

(3) Bolt cutters will be signed back into the supply room prior to the end of the day they were signed out.

(4) Upon turn-in, supply personnel will notate the bolt cutter logbook with the time and date the lock was cut, the time the bolt cutters were turned in, and their initials. Supply personnel will destroy/shred the DA Form 3161/DA Form 2062 that was used to sign out the bolt cutters.

c. Key control personnel in possession of bolt cutters are responsible for its security while in their care and they will be carried on their person at all times or secured as stated above.

d. In the event of the loss of bolt cutters, a statement of charges will be initiated against the key control person who signed for them.

e. If the bolt cutters cannot be stored in the supply room due to mission requirements, the following applies:

(1) The responsible commander or director of the activity will designate an individual in writing to be responsible for the security and accountability of bolt cutters and will approve the storage area in writing. Bolt cutters are prohibited from being stored in arms rooms.

(2) Issue and receipt requirements will be followed as notated in paragraphs F–2*a* and F–2*b*.

(3) Bolt cutters will be secured under double barrier protection (for example, container secured with a low security padlock inside a locked office/room).

(4) Keys to bolt cutter storage areas will be controlled per appendix D.

Appendix G

Internal Control Evaluation Checklist

G–1. Function

This checklist covers basic administration for the protection of unclassified sensitive and non-sensitive Army resources.

G–2. Purpose

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

G–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 internal controls must be formally evaluated at least once every 3 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification Statement).

G–4. Test questions

a. Are physical security inspections being conducted by a credentialed physical security inspector per AR 190–13 to determine compliance with minimum physical protective standards and security procedural standards?

b. Is the DA Pam 190–51 risk analysis process used for the categories of Army resources under this regulation?

c. What are the number of physical security inspections completed compared to the number inspections required by AR 190–13?

d. Is the DA Pam 190–51 risk analysis process being conducted for resources to be located in new or renovated facilities or facility additions?

e. Are incidents involving the loss, theft, misuse, or damage of Army resources promptly reported to the supporting law enforcement organization whenever the loss appears to involve unlawful conduct or as required by AR 190–11 or AR 735–5?

f. Have end–of–day security checks using the SF 701 been established?

g. Are only approved locks and locking systems being used per appendix D?

h. Is the U.S. Army Criminal Investigation Command's capability of conducting a crime prevention survey considered for the purpose of detecting crime, evaluating the possibilities of easy criminal activity, and identifying requirements conducive to criminal activity?

i. Are plans of actions and milestones in place to resolve deficiencies in meeting minimum physical protective standards and security procedural standards?

j. Are security criteria deviations (for example, waivers and exceptions to this policy) documented, and being reviewed at every level in the chain of command, per AR 190–13?

k. Are staff required to be on orders assigned by the Commander/director?

l. Are minimum security standards for resource categories being conducted in accordance with the appropriate risk levels prescribed in section II of chapter 3 and section III of chapter 6?

m. Is the (SMS(CM)) being used to conduct, track, and manage all physical security inspections, surveys, and risk assessments?

G–5. Supersession

This is an initial evaluation for the protection of unclassified sensitive and non-sensitive Army resources.

G–6. Comments

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

Glossary

Section I

Abbreviations

AA&E
arms, ammunition, and explosives

ACS
Access Control System

ANSI/BHMA
American National Standards Institute/Builders Hardware Manufacturers Association

AR
Army regulation

ARIMS
Army Records Information Management System

ARNG
Army National Guard

AT
antiterrorism

CCI
controlled cryptographic item

CCTV
Closed Circuit Television

CFR
Code of Federal Regulations

CG
commanding general

CIIC
controlled inventory item code

CONEX
container express

COTS
commercial off-the-shelf

DA Form
Department of the Army form

DA Pam
Department of the Army pamphlet

DEA
Drug Enforcement Administration

DES
Directorate of Emergency Services

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DODM
Department of Defense manual

ER
Engineering Regulation

ESS
electronic security system

GSA
General Services Administration

HVASC
high-value asset security cage

IAT
infectious agents and toxins

IDS
Intrusion Detection System

LESD
launched electrode stun device

MDEP
Management Decision Package

MEVA
mission essential and vulnerable area

MIL–STD
military standard

MOS
military occupational specialty

NSN
national stock number

OCIE
organizational clothing and individual equipment

PA&E
personal arms and equipment

POL
petroleum, oil, and lubricants

RC
Reserve Component

RRS–A
Records Retention Schedule–Army

SAF
stand-alone facility

SF
standard form

SMS(CM)
Security Management System (Countermeasures)

SOP
standing operating procedure

STD
standard

TB
technical bulletin

TM
technical manual

TSC
training support center

UFC
Unified Facilities Criteria

UFGS
Unified Facility Guide Specification

UFGS
Unified Facilities Guide Specifications

UL
Underwriters Laboratory

USACE
U.S. Army Corps of Engineers

USAR
U.S. Army Reserve

USC
United States Code

Section II

Terms

Aggressor
Any person seeking to compromise an asset. Aggressor categories include criminals, terrorists, and protestors.

Air items and airdrop systems
Parachute systems for personnel and cargo airdrop that include military type-classified and COTS parachute systems intended for the use in the premeditated airdrop of personnel, supplies, and equipment. These items and systems include associated ancillary air items such as parachutist oxygen systems and automatic activation devices. They are portable life-sustaining precision equipment by nature of their implementation.

Army resources
Assets which are critical resources and include personnel, information, equipment, facilities, activities, and operations.

Badge
A security credential worn on the possessor's outer garment and validates their authority for access to a restricted area.

Biosafety
The safe handling and containment of infectious microorganisms and hazardous biological materials.

Biosafety level 1
For work involving well-characterized agents not known to consistently cause disease in immunocompetent adult humans, and present minimal potential hazard to laboratory personnel and the environment.

Biosafety level 2
For work involving agents that pose moderate hazards to personnel and the environment.

Biosafety level 3
For work involving clinical, diagnostic, teaching, research, or production facilities where work is performed with indigenous or exotic agents that may cause serious or potentially lethal disease through the inhalation route of exposure.

Biosafety level 4
For work involving dangerous and exotic agents that pose a high individual risk of aerosol-transmitted laboratory infections and life-threatening disease that is frequently fatal, for which there are no vaccines or treatments, or a related agent with unknown risk of transmission.

Black start
The process of restoring an electric power station or a part of an electric grid to operation without relying on the external transmission network.

Bulk storage
Storage in a facility above the using or dispensing level specifically applicable to logistics warehouse and depot stocks. This applies to activities using controlled medical substances and items (such as pharmacies, wards, or clinics) only when a separate facility (building or room) is used to store quantities that exceed normal operating stocks.

Cable seal lock
A seal in which the cable is passed through the locking hardware of a truck trailer or railcar door and the bullet nose is inserted into the barrel and the end of the cable until securely anchored. Once locked any force exerted to separate the lock point from the lock body will strengthen its connection. (DODM 5100.76)

Central monitoring station
A central monitoring station will be provided at which alarms will present audible and visual alerts and from which a response force will be dispatched. The response force is not required to be collocated with the central monitoring station. The central monitoring station will alarm with audible and visual alerts whenever the system detects possible intrusion into the protected area or when the system is turned off, malfunctions, or is placed in maintenance mode. Some means of communication will be provided between the protected area and the central monitoring station to coordinate status changes. Telephone communication will be considered.

Chains
Chains used to secure racks or containers will be of heavy-duty, hardened steel chain, welded, straight link steel. The steel will be galvanized of at least 5/16-inch thickness or of equal resistance required to force, to cut, or break an approved padlock. An example of such a chain is Type 1, Grade C, Class 4 NSN 4010–0–149–5583, NSN 4010–00–149–5575, or NSN 4010–00–171–4427.

Closed Circuit Television
Television that serves a number of different functions, one of which is physical security. As it pertains to the field of physical security, CCTV is used to augment, not replace, existing IDS or security patrols. It is not used as a primary sensor, but rather as a means of assessing alarms. CCTV also may be used as a surveillance means, but if used in this way, it will augment, not replace, existing IDS.

Controlled inventory item code
CIIC is a one positon alphanumeric code that indicates the security classification and/or security risk or pilferage controls for storage and transportation of DOD assets. AR 710–2 states that a controlled inventory item is material that requires a high degree of protection and control and that material having ready resale value is especially subject to theft, because of statutory requirements, found in the Army Master Data File contained on Federal Logistics on the Defense Logistics Agency website.

Controlled medical substance
A drug or other substance, or its immediate precursor, listed in current schedules of Section 812, Title 21, United States Code (21 USC 812).

Director of Emergency Services
On an installation, activity, or site where no provost marshal, law enforcement, or security representative is otherwise assigned, the command may designate the DES to be the chief of police or chief of security.

Double barrier protection
Two separate physical containment structures which deter unauthorized access to the degree required by AR 190–51.

Double locked container
A steel container of not less than 26 gauge which is secured by an approved locking device and which encases an inner container that also is equipped with an approved locking device. Cabinet, medicine, combination with narcotic locker, NSN 6530–00–702–9240, or equivalent, meets requirements for a double locked container.

Duress (holdup) alarm
A method by which authorized personnel can covertly communicate a situation of threat to a security control center or to other personnel in a position to notify a security control center.

Entry control (when pertaining to a restricted area)
Actions, requirements, equipment, and techniques employed in restricted areas to make certain that persons who are present in the areas at any time have authority and official reason for being there.

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.

High–value asset security cage
A cage that provides security for high-value items in both garrison and field environments available as a supply cage and a portable cage.

Industrial and utility equipment
Equipment used in the manufacture or in support of the manufacture of goods and equipment used to support the operation of utilities such as power and water distribution and treatment.

Infectious agents and toxins
A viable microorganism, or its toxin which causes or may cause human disease, and includes those agents and includes those agents classified as risk group 2 or higher, as defined in the latest edition of the Biosafety in Microbiological and Biomedical Laboratories, but less than the collection of agents and toxins designated as "select" by the U.S. Centers for Disease Control and Prevention.

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.

Key and lock control system
A system of identifying both locks and their locations and personnel in possession of keys and/or combinations.

Keyed–alike locks
A group of locks that are operated by the same key.

Launched electrode stun device
A non-lethal device used to propel wire probes conducting energy to affect the sensory and motor functions of the nervous system.

Locked container
A container or room of substantial construction secured with an approved locking device. For pharmacy operating stocks, lockable automated counting systems meet requirements for a locked container.

Master key
A key that operates all the master-keyed locks or cylinders in a group of locks, each lock or cylinder usually operated by its own change key. To combine a group of locks or cylinders such that each is operated by its own change key as well as by a master key for the entire group,

Master key system
A keying arrangement which has two or more levels of keying, or a keying arrangement which has exactly two levels of keying.

Medically sensitive items
Standard and nonstandard medical items designated by medical commanders to be sufficiently sensitive to warrant a stringent degree of physical security and accountability in storage. Included within this definition are all items subject to misappropriation or misuse.

Motor pool
For the purpose of this policy, a motor pool is defined as a group of motor vehicles used as needed by different organizations or individuals and parked in a common location when not in use. On an Army installation, a non-tenant Army activity with 10 or less assigned commercial-type vehicles but no local organizational maintenance support does not have a motor pool, under this policy, even though the vehicles are parked together.

Note C controlled medical items
Sets, kits, and outfits containing one or more component Note Q or Note R items.

Note Q controlled medical items
All standard drug items identified as Note Q in the Federal Supply Catalog, Nonstandard Drug Enforcement Administration (DEA) Schedule III, IV, and V Controlled Substances.

Note R controlled medical items
All items identified as Note R in the Federal Supply Catalog, Nonstandard DEA Schedule II Controlled Substances.

Operations security and security targeted against traditional criminal activity are included.
a. Physical security requirements include, but are not limited to, the application of physical measures to reduce vulnerability to the threat; integration of physical security into contingency, mobilization, and wartime plans; the testing of physical security requirements and measures during the exercise of these plans; the interface of installation operations security, crime prevention and physical security programs to protect against the traditional criminal; training of guards at sensitive or other storage sites in tactical defense against and response to attempted penetrations; and creating physical security awareness.
b. Physical security measures are physical systems, devices, personnel, animals, and requirements 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 IDSs ; 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 CCTV. Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans.

Perimeter fence
Fences for the security of unclassified, non-sensitive items that meet the requirements of USACE STD 872–90–00 series. The minimum height will be 6 feet. Use of NATO Standard Design Fencing is also authorized.

Perimeter wall
Any wall over 6 feet tall which delineates a boundary and serves as a barrier to personnel and/or vehicles. These walls may be constructed of reinforced concrete, masonry, or stone.

Physical 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 equipment
A generic term for any item, device, or system that is used primarily to protect Government property, including nuclear, chemical, and other munitions, personnel, and installations, and to safeguard national security information and material, including the destruction of such information and material both by routine means and by emergency destruct measures.
a. *Interior physical security equipment.* Physical security equipment used internal to a structure to make that structure a secure area. Within DOD, DA is the proponent for those functions associated with development of interior physical security systems.
b. *Exterior physical security equipment.* Physical security equipment used external to a structure to make the structure a secure area. Within DOD, the Department of the Air Force is the proponent for those functions associated with the development of external physical security systems; however, the Army will develop lights, barriers, and robotics.

Physical security inspection
A formal, recorded assessment of physical protective measures and security requirements measures implemented by a unit or activity to protect its resources.

Physical security measures
Physical security measures used to counter risk factors that usually do not change over a period of time such as mission impact, cost, volume, and criticality of resources and vulnerabilities. The measures are usually permanent and involve expenditure of funds.

Physical security plan
A comprehensive written plan providing proper and economical use of personnel, land, and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

Physical security procedures
See physical security.

Physical security program
The interrelationship of various components that complement each other to produce a comprehensive approach to security matters. These components include, as a minimum, the physical security plan; physical security inspections and surveys; participation in combating terrorism committees and fusion cells; and a continuing assessment of the installation's physical security posture.

Pilferable resources
Any resource that can be stolen and does not fall under the other resource categories discussed in this publication.

Pilferage–coded items
Items with a code indicating that the material has a ready resale value or civilian application and, therefore, is especially subject to theft.

Portable
Capable of being carried in the hand or on the person. As a general rule, a single item weighing less than 100 pounds or 45.34 kilograms is considered portable by one person.

Protection in depth
A system providing several supplementary security barriers. An example is the use of a perimeter fence, a secure building, a vault, and a locked container to provide four layers of protection.

Resource
Personnel and/or materials provided as a means of support (does not refer to monetary source for purposes of this guidance).

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

Risk
The degree or likelihood of loss of 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 resource loss. This analysis will be used to decide the level of security warranted for protection of resources.

Risk factors
Elements that make up the total degree of resource loss liability. Factors to be considered in a risk analysis include the importance of the resource to mission accomplishment; the cost, volume, criticality, and vulnerabilities of the resources; and the severity of threats to the resources.

Risk level
An indication of the degree of risk associated with a resource based on risk analysis. Risk levels may be Levels I, II, or III, which correspond to low, medium, and high.

Risk value
Degree of expectation or likelihood of resource loss. The value may be classified as low, medium, or high.

Schedule I drug
Any drug or substance by whatever official name (common, usual, or brand name) listed by the DEA in Section 1308.11, Title 21, Code of Federal Regulations (21 CFR 1308.11), intended for clinical or non-clinical use. A list of Schedule I drugs and substances is contained in AR 40–7.

Seal
A device to show whether the integrity of a shipment has been compromised. Seals are numbered serially, are tamperproof, and shall be safeguarded while in storage. The serial number of a seal will be shown on government bills of lading. A cable seal lock provides both a seal and locking device.

Security lighting
The amount of lighting necessary to permit visual surveillance.

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.

Sensitive items
Material requiring a high degree of protection to prevent unauthorized acquisition. This includes arms, ammunition, explosives, drugs, precious metals, and other substances and items determined by the Administrator, DEA to be designated Schedule Symbol II, III, IV, or V under the Controlled Substance Act of 1970.

Stand–alone facility
A site with single or multiple U.S. military assets, and/or Federal civilian employees, which are physically located off a standard military installation and are embedded within communities.

Surveillance
The ability to watch or view a resource or area using personnel designated and assigned to perform this function or by using monitored CCTV equipment.

Unified Facilities Criteria
UFC documents provide planning, design, construction, sustainment, restoration, and modernization criteria, and apply to the military departments, the defense agencies, and the DOD field activities in accordance with DODD 4270.5. UFC are distributed only in electronic media and are effective upon issuance.

Unified Facilities Guide Specifications
UFGSs are for use in specifying construction for the military Services.

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.