Army Regulation 190–51

Military Police

Security of Unclassified Army Property (Sensitive and Nonsensitive)

Headquarters
Department of the Army
Washington, DC
30 September 1993

UNCLASSIFIED

SUMMARY of CHANGE

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

This revision--

- Consolidates paragraphs 6 through 9, 11, 13, 15 through 17, and 19 of AR 190-18 into chapter 5 and AR 190-50 into chapter 4.

- Consolidates all responsibilities, to include controlled substances and museums (chap 1).

- Adds requirements for conducting risk analyses during construction planning for assets of units or activities that will occupy new or renovated facilities or facility additions (para 2-2).

- Adds some minimum security measures and terrorism counteraction measures asset categories. Security measures now consist of physical protective measures, security procedural measures, and terrorism counteraction measures (sections II and III, chap 3).

- Broadens asset categories and adds security measures for assets not previously in the regulation (for example, mission-critical and high-risk personnel (para 3-19), general civilian and or military personnel (para 3-20), and industrial and utility equipment (para 3-21)).

- Consolidates all storage structure requirements and allows for alternative construction based on delay time for the different construction being equal to or greater than the response time (app B).

- Adds intrusion detection system requirements in some situations to increase delay after detection (para B-1).

- Consolidates all marking requirements (app C).

- Authorizes exact replication of any DA or DD forms prescribed in this regulation generated by the automated Military Police Information Management System in place of the official printed version of the form (app A, sec III).

Headquarters
Department of the Army
Washington, DC
30 September 1993

*Army Regulation 190–51

Effective 30 October 1993

Military Police

Security of Unclassified Army Property (Sensitive and Nonsensitive)

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

MILTON H. HAMILTON
Administrative Assistant to the Secretary of the Army

History. This UPDATE printing publishes a consolidation of three regulations pertaining to physical security; AR 190–18, AR 190–50, and AR 190–51. Because the structure of the revised text has been reorganized, no attempt has been made to highlight changes from earlier printings.

Summary. This regulation implements DODD 5200.8, Security of DOD Installations and Resources, and sets forth physical security policies, procedures, and standards for the safeguarding of U.S. Army property. It provides guidance for protection of both sensitive and nonsensitive supplies and equipment, controlled cryptographic items, controlled medical substances and sensitive items, and historically significant items in the care of the U.S. Army museum system. 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 property specified in this regulation.

Applicability. This regulation applies to elements of the Active Army, the Army National Guard, the U.S. Army Reserve, the Reserve Officers' Training Corps, and U.S. Army contractors which use or handle both sensitive and nonsensitive unclassified U.S. Army property. This publication applies during partial and full mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Operations and Plans. The Deputy Chief of Staff for Operations and Plans has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The Deputy Chief of Staff for Operations and Plans may delegate this authority, in writing, to a division chief within the proponent agency in the grade of colonel or the civilian equivalent. The approval authority will coordinate all questions regarding the scope of authority to approve exceptions with HQDA (DAJA–AL), Washington, DC 20310–2200.

Army management control process. This regulation is subject to the requirements of AR 11–2. It contains internal control provisions but does not contain checklists for conducting internal control reviews. These checklists are contained in Department of the Army Circular 11–89–2.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (DAMO–ODL–S), 400 Army Pentagon, Washington, DC 20310–0400.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMO–ODL–S), 400 Army Pentagon, Washington, DC 20310–0400.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12–09E, block 2568, intended for command levels A, B, C, D, and E for the Active Army, Army National Guard, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes paragraphs 6 through 9, 11, 13, 15 through 17, and 19 of AR 190–18, 1 April 1984; AR 190–50, 31 March 1986; and AR 190–51, 31 March 1986.

UNCLASSIFIED

Contents—Continued

Contents—Continued

Contents—Continued

Appendixes

Glossary

Index

Chapter 1
Introduction

1–1. Purpose

This regulation prescribes policies, procedures, and responsibilities for safeguarding unclassified U.S. Army property, both sensitive and nonsensitive. Its policy objectives are to—

a. Establish standardized, minimum acceptable security requirements for specified categories of U.S. Army property.

b. Provide a risk analysis method that allows commanders the flexibility to tailor physical security posture and resources to meet local needs.

c. Reduce loss, theft, misuse, and damage of Army assets cost effectively.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

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

1–4. Responsibilities

a. Deputy Chief of Staff for Operations and Plans (DCSOPS) will—

(1) Provide overall staff responsibility for the security of unclassified Army property (sensitive and nonsensitive).

(2) Coordinate with the Army Staff (ARSTAF) and major Army commands (MACOMs) to establish policy, procedures, and standards pertaining to security of Army property.

b. The Director of Information Systems for Command, Control, Communications, and Computers will resolve any conflicts in U.S. Army policy concerning the control of controlled cryptographic items (CCI).

c. Installation commanders, major United States Army Reserve Commands (MUSARC), and state adjutants general (AG) 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 Army Regulation (AR) 190–13.

(2) Ensure a risk analysis is conducted for the assets of units and activities which are to occupy new or renovated facilities or facility additions. Risk analyses for assets 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.

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

d. The numbered armies in the continental United States (CONUSA), installation, division, MUSARC, separate brigade commanders, and state AGs, upon declaration of war or when operating in a designated hostile area, may prescribe procedures suspending specific provisions of this regulation to account for local conditions while ensuring maximum practical security for Government personnel and property. This authority may be delegated to commanders in the grade of lieutenant colonel.

e. Unit commanders or activity chiefs will control and safeguard all supply and equipment areas within their command or activity. They will—

(1) Promptly report to the provost marshal or equivalent organization, investigate, and resolve incidents involving loss, theft, misuse, or damage of Army resources.

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

(3) Implement security measures associated with the conduct of risk analysis using this regulation and Department of the Army (DA) Pamphlet 190–51.

(4) Ensure physical security officers are appointed, in writing, to perform, as a minimum, the duties outlined in AR 190–13.

(5) Ensure security plans outlining responsibilities and procedures for the proper control and accountability of assets are written and appropriately disseminated.

(6) Ensure assets are secured by approved locking devices (locks, chains, seals, etc.) as outlined in appendix D.

f. Units, activities, and installations involved in supply operations will protect their own supplies and equipment as indicated in this regulation.

g. Facility commanders will ensure physical security inspections are conducted per AR 190–13. In addition, commanders may request the U.S. Army Criminal Investigation Command (USACIDC) to conduct crime prevention surveys for the purpose of detecting crime, evaluating the possibilities of easy criminal activity, and identifying procedures conducive to criminal activity.

h. 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, etc.).

(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.

i. 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. Security measures and standards

a. Physical security measures or standards more stringent than those contained in this regulation, as appropriate, will be developed jointly by the tenant activity commander, the installation physical security officer, and host installation commander. Such measures will be based on a threat analysis developed from the risk analysis in DA Pam 190–51 using Technical Manual (TM) 5–853–1. 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 normal budget documents. Tenant activities must identify their security requirements to the host installation.

c. Installation of intrusion detection systems (IDS) will be according to the applicable Office of the U.S. Army Corps of Engineers guide specifications and with applicable Army regulations (to include AR 190–13).

d. Provision of security measures beyond those required by this regulation will be per TM 5–853–1.

1–6. Waivers and exceptions

a. Waivers and exceptions for all unclassified Army property discussed in this regulation will be considered individually.

(1) Requests for waivers and exceptions will be submitted, in writing, with complete justification and a statement of compensatory measures in effect through command channels and through the MACOM commander or appropriate staff element having staff cognizance to HQDA (DAMO–ODL–S), 400 ARMY PENTAGON, WASH, DC 20310–0400. Waivers will not be granted for periods exceeding 12 months. Exceptions will be regarded as permanent; however, they will be reviewed and revalidated every 2 years by HQDA (DAMO–OL–S), which retains the authority to revoke exceptions.

(2) Requests for waivers or exceptions will be coordinated with the law enforcement activity, provost marshal, or security officer. When structural deficiencies exist, requests also will be coordinated with the supporting Director of Engineering and Housing (DEH) or equivalent organization.

(3) Active and reserve component provost marshals will submit through command channels and their MACOM to HQDA (DAMO–ODL–S) a list of exceptions to physical security requirements and indicate whether the exceptions are to be continued or canceled.

b. Waivers and exceptions to the requirements of this regulation will be kept to a minimum.

(1) Authority to grant waivers and exceptions is delegated to HQDA (DAMO–ODL–S).

(2) Requests for waivers and exceptions will include an adequate description of circumstances requiring the action and a description of compensatory measures. Requests will be submitted, in writing, through command channels to HQDA (DAMO–ODL–S) for individual evaluation. Blanket waivers or exceptions are not authorized.

(3) Waivers normally will be valid up to but not to exceed 1 year. A permanent exception from the specific requirements of this regulation will be permitted only under the conditions described below.

(a) Unique circumstances at a given unit, facility, or installation are such that conformance to the established standards is impossible, highly impracticable, or unnecessary.

(b) Security afforded is equal to or greater than that provided by the standard criteria.

Chapter 2
Risk Analysis

2–1. General

a. To provide the most practical protection for Army assets, commanders must identify the assets to be protected and analyze the risks to those assets from espionage, sabotage, terrorism, damage, misuse, and theft. Analysis of these risks will assist in determining the type and minimum level of protection needed to safeguard the identified resources adequately and economically.

b. The objectives of risk analyses are to—

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

(2) Allow commanders 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 an asset–specific threat analysis.

2–2. Use of risk analysis

a. The background and explanation of step–by–step procedures for determining security requirements and conducting a risk analysis for categories of Army property are in DA Pam 190–51.

b. A risk analysis will be conducted for those installations or facilities that the installation or MUSARC commanders or the State AGs determine mission essential or vulnerable as indicated in AR 190–13 and which include one or more of the categories of U.S. Army property addressed in this regulation. A risk analysis will be conducted on all mission essential and vulnerable areas (MEVAs)—

(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 or activity commander.

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

(6) When an incident occurs in which an asset is compromised.

c. The risk analysis will be conducted jointly by designated representatives of the installation commander, the using unit or activity, and the supporting installation provost marshal or equivalent security officer representative.

2–3. Implementation of risk analysis

a. Based on the risk analysis results, the unit commander or activity chief will implement the physical protective measures and security procedures described in chapters 3, 4, or 5 of this regulation, as appropriate.

b. Results of the risk analysis and physical protective measures, security procedural measures, and terrorism counteraction measures to be implemented will be recorded on DA Form 7278–R (Risk Level Worksheet), with all attachments as necessary. Instructions for the use of DA Form 7278–R are in DA Pamphlet 190–51. Copies of these records will be kept by the supporting provost marshal or equivalent security officer at the unit or activity concerned and at the reserve component provost marshal's office where applicable. The results will be used in planning and assessing physical security programs under AR 190–13.

c. The risk analysis may be reviewed and portions of the results changed at the discretion of the installation CONUSA or MUSARC commander or State AG. This could be based on a significant change in risk factors to a specific category of Army property, to a particular unit or activity, or to the overall installation. Any discretionary changes made by the installation commander will be coordinated with the installation provost marshal or equivalent security officer.

Chapter 3
Physical Security Standards by Category of Army Property

Section I
Security overview

3–1. General

a. In this chapter, common types of U.S. Army property are classified in readily understandable categories for quick reference. Guidance for each category of property listed includes references to the primary directives for management and accountability of that category of property and minimum security standards to be implemented.

b. Section II of this chapter outlines physical protective, security procedural, and terrorism counteraction measures for particular categories of property maintained at U.S. Army installations or facilities. The measures are categorized according to their risk levels established using the risk analysis procedure in DA Pam 190–51. Risk Level I physical

protective and security procedural measures will be treated as minimums. Physical protective and security procedural measures primarily address threats related to theft of the asset. Additional terrorism counteraction measures address terrorist threats related to the killing of people or the destruction of assets. Such measures are only included for asset categories for which they apply.

c. Section III of this chapter outlines minimum required security measures to be implemented for other specified categories of property. Although these categories of Army property do not require the conduct of risk analysis using DA Pam 190–51, the principles of risk analysis should be applied and risk factors considered.

d. For those categories of U.S. Army property where perimeter fencing is required as a protective measure, the type and quantity of fencing, including the height (6 or 7 feet) and whether a top guard or other features are required, will be based on the judgment of the installation commander and the guidance found in Field Manual (FM) 19–30. Unless otherwise specified, perimeter fence will meet the requirements of U.S. Army Corps of Engineers Drawing No. 40–16–08, Type FE–5. Copies of this drawing normally may be obtained from the installation engineer. If the drawing is not available locally, requests may be forwarded to the Commander, U.S. Army Corps of Engineers, Huntsville, Division, ATTN: CEHND–ED–ES–1, P.O. Box 1600, Huntsville, Alabama 35807–4301. The minimum height will be 6 feet. Use of North Atlantic Treaty Organization (NATO) standard design fencing is also authorized. Modifications to existing perimeter fences should not be made solely to conform to the requirements of this regulation if the existing fencing provides a similar deterrent to penetration.

e. In those instances where security lighting is required, FM 19–30 will be used as a guide in deciding lighting patterns and minimum protective lighting intensities and requirements.

f. Conflicts between security and safety requirements must be identified in writing. Waiver or exception requests must list compensatory measures and be forwarded through the local provost marshal and MACOM to HQDA (DAMO–ODL–S) for approval.

3–2. Categories of Army property

Items of property will not always correspond exactly to the categories listed in sections II or III. Some items may fall into two categories. When this situation occurs, the unit commander directly responsible for the asset is responsible for determining the most appropriate category for the item in question. If none is appropriate, the commander will develop and carry out those security procedures and physical protective measures necessary to safeguard the property.

Section II
Minimum Security Standards for Categories of Army Property Using Risk Analysis

3–3. Aircraft and components at Army aviation facilities

a. Property management and accountability directives.

(1) AR 95–1.

(2) AR 190–16.

(3) AR 710–2.

(4) AR 735–5.

(5) DA Pam 710–2–1.

b. Aircraft with arms, ammunition, and explosives (AA&E) aboard. Army aircraft with AA&E aboard will be secured as indicated in AR 190–11 and this regulation. Army National Guard aircraft with AA&E aboard will be secured as indicated in NGR 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 IDS.

(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 practicable. 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 or NGR 190–11.

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

d. Aircraft with classified equipment. U.S. Army aircraft with classified equipment aboard will be secured as indicated in AR 380–5, Technical Bulletin (TB) 380–41, and paragraph 3–18 of this regulation. Classified components which can be readily removed without damage to them should be placed in secure storage as indicated in AR 380–5.

e. Physical protective measures.

(1) *Risk Level I.*

(a) 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.

(b) Keys to locking devices and ignitions will be controlled. Key control and accountability must be established per

appendix D. Aircraft keys will not be issued for personal retention. Duplicate keys will not serve as operational keys at maintenance facilities.

(c) 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.

(d) 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.

(2) *Risk Level II.*

(a) All measures required for Risk Level I will be implemented.

(b) Aviation facility aircraft parking areas will be protected by a perimeter fence.

(3) *Risk Level III.*

(a) All measures required for Risk Levels I and II will be implemented.

(b) 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.

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

f. Security procedural measures.

(1) *Risk Level I.*

(a) Each Army aviation facility will have a written physical security plan. FM 19–30 will be used as a guide. 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. Aviation facilities located on other than Army property will coordinate the physical security plan with the appropriate host authorities. A copy of the physical security plan will be maintained by the State AG or MUSARC provost marshal for reserve component aviation facilities.

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

(c) For aircraft parked at Active Army aviation facilities and for U.S. Army Reserve (USAR) and Army National Guard (ARNG) activities where guards or roving patrols are available, aircraft will be checked at least every 4 hours by a roving guard.

(d) 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.

(e) Access to aviation facility aircraft and aircraft components will be controlled at all times. The airfield will be designated as a restricted area as specified in AR 190–13. Measures such as badges, passes, or similar identification credentials are encouraged.

(f) Privately–owned vehicles will be prohibited from the flight line or other areas where aircraft are parked, except when authorized, in writing, by the aviation facility or airfield commander.

(g) 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 nonduty hours to prevent unauthorized use.

(2) *Risk Level II.*

(a) All measures required for Risk Level I will be implemented.

(b) 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.

(c) Aircraft parked at Active Army aviation facilities will be checked at least once every hour by a roving guard.

(3) *Risk Level III.*

(a) All measures required for Risk Levels I and II will be implemented.

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

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

(d) At USAR and ARNG facilities where guards or roving patrols are available, aircraft will be checked at least every 2 hours. 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 2 hours during nonoperational hours.

g. Terrorism counteraction measures. Due to the likely form of a terrorist attack against these assets, the physical protective measures and security procedural measures established above will also be applicable for protection against terrorist threats. Aviation facilities will develop a terrorism counteraction contingency plan.

3–4. Aircraft and components not at Army aviation facilities

The property accountability requirements outlined in the references in paragraph 3–3*a* will be followed and paragraphs 3–3*b*, *c*, and*d* will be implemented. Physical protective measures for Risk Level I in paragraph 3–3 will also be implemented. In addition, the security procedures indicated below will apply.

a. 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 aviation facility and local law enforcement authorities of the aircraft location, identification, length of stay, and ways to contact crew members.

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

3–5. Vehicles and carriage–mounted/towed weapons systems and components

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 738–750.

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 and paragraph 3–18 of this regulation. Classified components that can be readily removed without damage should be placed in secure storage as indicated in 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. FM 19–30 will be used as a guide for determining fencing requirements.

e. Physical protective measures.

(1) *Risk Level I.* Army vehicles parked in noncombat areas will be secured with a locking mechanism. These vehicles will be locked as follows:

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

(b) Tactical vehicles and M880 series vehicles. Immobilize steering wheel with a chain and a U.S. Government approved padlock as specified in TB 9–2300–422–20. Activate installed door and ignition–locking devices. Hood, spare tires, and fuel tank should also be secured with approved locking devices if the local environment warrants this action. Brass padlocks supplied with vehicles may be used to secure vehicles, 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 (CUCV) will be secured by activating installed door and ignition locks and immobilizing the steering wheel with chain and U.S. Government approved padlock as specified in TB 43–001–39–7. Alternatively, such vehicles may be stored in a secure structure.

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

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

(2) *Exceptions.* 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 should be removed from unaccompanied vehicles.

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

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

(e) Vehicles, without installed locking mechanisms, under the continuous surveillance of a guard or located in a secure storage structure (app B).

(f) Vehicles of specific units outside the United States when so designated by the MACOM commander. Basis for a

unit exemption will be an impact on readiness. The 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 installation commander, locking would create a potential unacceptable hazard to life or property. In this case, compensatory security measures as outlined in paragraph 3–14 will be taken.

(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 (app 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 2½-ton truck.

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

(4) *Master–keyed locksets.* Use of master–keyed locksets to secure Army vehicles or motor pools will be prohibited except under the following conditions:

(a) When the lockset is used within one vehicle to secure the vehicle and its various storage compartments. Master–keyed locksets will not be used to secure more than one vehicle.

(b) When the lockset is used to secure the manifold access doors and hatches of petroleum, oil and lubricants (POL) trucks (one set per truck) and, if they have hardened steel shackles, for the storage compartments of wreckers, heavy equipment, etc. (one set per vehicle). The same set will not be used on more than one vehicle. Master–keyed locks will not be used to secure vehicle steering wheels.

(5) *Keys and locks.* Keys and locks will be controlled according to appendix D.

(6) *Items used to defeat security measures.* 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.

(7) *Risk Level II.*

(a) All measures required for Risk Level I will be implemented.

(b) Vehicle parking areas, except those for empty trailers, will be lighted during the hours of darkness.

(c) Vehicles will be parked at least 20 feet from the perimeter of the parking area or as far from the perimeter as possible.

(8) *Risk Level III.*

(a) All measures required for Risk Levels I and II will be implemented.

(b) 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.

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

f. Security procedural measures.

(1) *Risk Level I.*

(a) For Active 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.

(b) USAR and ARNG units and activities 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.

(c) 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 MUSARC commander, provided security measures are taken to safeguard Army vehicles and components remaining in the motor pool.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) 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 within the motor pool may be considered an alternative to guards. Consolidated motor pools will have memorandums of understanding to establish joint security procedures.

(c) 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 nonoperating hours.

(d) On Active Army installations, guards will check the motor pool on an irregular basis, but perform security checks not less than once every 2 hours.

(3) *Risk Level III.*

(a) All measures required for Risk Levels I and II will be implemented.

(b) The motor pool will be designated a restricted area under AR 190–13.

(c) Unit commanders, or their specifically designated representatives, will give written authorization before vehicles are dispatched.

(d) 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.

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

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

(g) At USAR and ARNG activities where guards or roving patrols are available, motor pools will be checked for tampering, sabotage, loss, or damage not less than once every 2 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 2 hours during nonoperational hours.

g. Terrorism counteraction measures. Due to the likely nature of a terrorist attack against these assets, the physical protective measures and security procedural measures established above will also be applicable for protection against terrorist threats.

3–6. Communications and electronics equipment and night vision devices

Communications and electronics test, measurement, and diagnostic equipment (TMDE) and other high–value precision equipment, night vision devices that are not part of a weapons system, and tool kits are protected as follows:

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) 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—

(a) A locked or guarded separate building or an enclosed van, trailer, or armored vehicle protected by a perimeter fence.

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

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

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

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

(2) 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 barrier.

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

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

(5) Tactical communications equipment remaining on vehicles will be secured to the vehicle with a medium security padlock. Vehicles will be secured per paragraph 3–5 of this regulation.

(6) Tool kits will be secured as specified in paragraph 3–22.

c. Physical protective measures (Risk Level II).

(1) Measures required for Risk Level I will be implemented.

(2) 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 of this regulation.

d. Physical protective measures (Risk Level III).

(1) All measures required for Risk Levels I and II will be implemented.

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

(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.

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

e. Security procedural measures (Risk Level I).

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

(2) Access to keys, padlocks, and protective seals protecting assets will be controlled per appendix D.

(3) Portable, pilferage–coded items temporarily assigned to a user will be issued on a hand receipt or a locally devised temporary receipt.

f. Security procedural measures (Risk Level II).

(1) Measures required for Risk Level I will be implemented.

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

(3) Periodic 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.

g. Security procedural measures (Risk Level III).

(1) Measures required for Risk Levels I and II will be implemented.

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

(3) The activity will be checked at least every 2 hours after normal duty hours by guards on Active Army installations.

(4) 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.

3–7. Organizational clothing and individual equipment (OCIE) 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.

(1) *Risk Level I.*

(a) Stocks will be secured in a separate building or room meeting the security standards in appendix B.

(b) "Off Limits To Unauthorized Personnel" signs will be posted at facility entrances.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) 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.

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

(c) IDS will be installed in the facility.

(d) Rooms or buildings will be constructed per secure storage structure guidance for at least Risk Level II in appendix B of this regulation.

(e) 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.

c. Security procedural measures.

(1) *Risk Level I.*

(a) Access to the facility and to keys, padlocks, and protective seals protecting assets will be controlled per appendix D.

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

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) 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.

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

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

(3) *Risk Level III.*

(a) Measures for Risk Levels I and II will be implemented.

(b) The facility will be checked at least once every 2 hours by roving guards.

3–8. OCIE not stored at central issue facilities

a. Risk Level I physical protective measures and the security procedures in paragraph 3–7 will be implemented for OCIE stored centrally in units.

b. Issued clothing will be marked as indicated in AR 700–84.

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

(3) Access to reserve component OCIE will be controlled by designated individuals. 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 reserve component OCIE will be placed in the unit key depository and access will be controlled by the unit key custodian.

d. Consideration should be given to marking items as indicated in appendix C.

3–9. Subsistence items stored at commissaries, commissary warehouses, and troop issue subsistence activities (TISAs)

a. Property management accountability directives.

(1) AR 30–1.

(2) AR 30–18.

(3) AR 30–19.

(4) AR 735–5.

b. Physical protective measures.

(1) *Risk Level I.*

(a) Commissaries, commissary and subsistence warehouses, and TISAs will meet the construction requirements for secure storage structures in appendix B.

(b) "Off Limits to Unauthorized Personnel" signs will be posted at entrances to subsistence storage facilities (see AR 420–70).

(c) 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.

(d) Subsistence items temporarily stored outside the facility, such as in secured vans and reefer trucks, will have protective lighting. Use FM 19–30 as a guide to determine the type of protective lighting.

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

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

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) 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.

(c) 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.

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

(c) IDS will be installed in the facility.

(d) 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.

c. Security procedural measures.

(1) *Risk Level I.*

(a) Access to the facility and to keys and padlocks and protective seals protecting assets will be controlled according to appendix D.

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

(c) Personal packages will be prohibited in ration breakdown and subsistence storage areas.

(d) 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.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) 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.

(c) 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.

(d) 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.

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

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

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

(c) The facility will be checked at least every 2 hours after normal operating hours by roving guards.

3–10. Subsistence items not at commissaries, commissary warehouses, and troop issue subsistence activities

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

3–11. Repair parts at installation level supply support activities and direct support units with an authorized stockage list (ASL)

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. Secured under AR 380 series requirements and paragraph 3–18 of this regulation.

c. Physical protective measures (Risk Level I).

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

(a) In a locked, separate building or room, meeting the secure storage structure standards in app B.

(b) In a locked, steel cage.

(c) 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 nonportable with stored parts.

(d) To the building in which located or other permanent structure.

(2) Nonportable 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 barrier.

(3) "Off Limits to Unauthorized Personnel" signs will be posted at the storage facility entrance (see AR 420–70).

d. Physical protective measures (Risk Level II).

(1) Measures required for Risk Level I will be implemented.

(2) Portable, pilferage–coded items will be separated from other stock and stored in a separate room, building, or container with controlled access.

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

e. Physical protective measures (Risk Level III).

(1) Measures required for Risk Levels I and II will be implemented.

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

(3) IDS will be installed in the storage 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 Levels I and II).

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

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

(3) Used parts will be processed as indicated in Department of Defense (DOD) 4160.21–M to recover parts when prescribed and protect and dispose of nonrecoverable parts, and will be protected and disposed of to preclude recycling.

g. 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 2 hours after normal operating hours by guards.

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

3–12. Repair parts not at installation level support activities and direct support units

a. Risk Level I physical protective measures and the security procedures in paragraph 3–11 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.

3–13. Petroleum, oils, and lubricants (POL) at bulk storage facilities

a. Property management and accountability directives.

(1) AR 703–1.

(2) AR 710–2.
(3) AR 735–5.
(4) DA Pam 710–2–1.

b. Physical protective measures.

(1) *Risk Level I.*

(a) Construction of storage facilities will be per DOD 4270.1–M.

(b) When not under the surveillance of personnel authorized to dispense the products, POL pumps will be locked and electrical power will be 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 type device. Use of such devices will be approved by the MACOM concerned.

(c) 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.

(d) Keys to POL storage areas, equipment, and buildings will be controlled per appendix D.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) Storage facilities will be bound by a perimeter fence. Gates and openings will be closed and locked.

(c) "Off Limits to Unauthorized Personnel" signs will be posted at the perimeter.

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

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

c. Security procedural measures.

(1) *Risk Level I.*

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

(b) When unattended, the facility will be checked at least once every 4 hours.

(c) POL credit cards, identification plates, and aviation fuel plates will be centrally controlled by a custodian, preferably at Director of Logistics (DOL) 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 individual 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.

(d) Privately–owned vehicles will not be permitted in storage facilities.

(e) All issues of fuel will be accounted for and supervised by authorized personnel.

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

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

(h) Keys to POL storage areas, equipment, buildings, and protective seals will be controlled per appendix D.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) Facility attendants will verify all POL quantities issued by personally reading the meter.

(c) When unattended, the facility will be checked at least once every 2 hours.

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

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

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

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

d. Terrorism counteraction measures. Due to the likely nature of a terrorist attack against this asset, the physical protective measures and security procedural measures established above will also be applicable for protection against terrorist threats.

3–14. POL not at bulk storage facilities

Property management and accountability directives in paragraph 3–13 will be followed. Risk Level I physical protective measures and security procedures in paragraph 3–13 will be implemented. In addition, the following security procedures will be implemented:

a. POL tank trucks that contain 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) Approved padlocks as specified in nonsparking brass locks for safety, if available.

b. Fuel pods on vehicles and fuel vehicle tanks will be secured with approved padlocks as specified in AR 190–13 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, whenever possible.

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 IDS. The need for implementing these additional measures will be determined by local threat and vulnerability.

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

3–15. Facility engineering supply and construction material storage areas

a. Property management and accountability directives.

(1) AR 420–17.

(2) AR 735–5.

b. Physical protective measures.

(1) *Risk Level I.*

(a) Buildings storing supply and portable construction material will meet the secure storage structure requirements in appendix B.

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

(c) Points of issue for supplies and construction material will be kept to a minimum.

(d) "Off–Limits to Unauthorized Personnel" signs will be posted at facility entrances.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

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

(c) Outside storage areas will be lighted during the hours of darkness.

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

(b) Buildings storing supplies and portable construction material will be lighted during the hours of darkness.

(c) An IDS will be installed in the storage building if it is fully enclosed.

(d) 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.

c. Security procedural measures.

(1) *Risk Level I.*

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

(b) Supplies will be issued only to authorized personnel for whom signature authorization cards, DA Form 1687 (Notice of Delegation of Authority–Receipt for Supplies), are on file.

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

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

(e) Entry of privately–owned vehicles into the storage building or outside storage areas will be prohibited.

(f) Entry of packages into the storage area will be prohibited.

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

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) Small, easily pilferable supplies and construction material and other items showing unexplained inventory loss will be inventoried once each month. A copy of the inventory will be kept until the next inventory.

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

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

(c) The storage building and outside storage areas will be checked at least every 2 hours by a roving guard during hours that the facility is not operational.

3–16. Audiovisual equipment, training devices, and subcaliber devices at training and audiovisual support centers (TASCs)

a. Property management and accountability directives.

(1) AR 108–2.

(2) AR 190–11.

(3) AR 710–2.

(4) AR 735–5.

(5) DA Pam 710–2–1.

b. Physical protective measures. Any training device that can be used to fire a projectile or explosive will be protected according to AR 190–11.

(1) *Risk Level I.* Equipment will be secured in a separate building or room under storage structure security standards stated in appendix B.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) Audiovisual equipment and portable, high–value subcaliber devices and training aids will be separated from other equipment and stored in a secure, separate container, room, or building with controlled access, meeting the security standards in appendix B.

(c) "Off–Limits to Unauthorized Personnel" signs will be posted at facility entrances.

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

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

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

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

(d) 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.

c. Security procedural measures.

(1) *Risk Level I.*

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

(b) Audiovisual equipment and portable, high–value subcaliber 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.

(2) *Risk Level II.*

(a) Measures required for Risk Level I will be implemented.

(b) The inventory check–out point will be next to the TASC exit to preclude personnel from remaining in the center when equipment has been checked out.

(c) Access to the equipment storage area will be limited to TASC personnel authorized to issue the equipment.

(d) The TASC will maintain separate property book accountability for all equipment.

(3) *Risk Level III.*

(a) Measures required for Risk Levels I and II will be implemented.

(b) The TASC will be checked at least once every 2 hours by a roving guard after normal duty hours.

3–17. Audiovisual equipment, training devices, and subcaliber devices at units or activities that are not training and audiovisual support centers

Risk Level I physical protective measures and the security procedures in paragraph 3–16 will be implemented.

3–18. Aircraft and vehicles with classified onboard equipment or components

Active Army, USAR, and ARNG vehicles and aircraft with classified components or onboard equipment will be secured per this regulation, AR 380–5, TB 380–41, and applicable security classification guides.

a. Army vehicles or aircraft with CONFIDENTIAL or SECRET components or equipment mounted either internally or externally on the vehicle or aircraft, on Active Army, USAR, or ARNG installations or facilities will be secured with Risk Level I physical protective and security procedural measures in paragraphs 3–3 and 3–5.

b. When the CONFIDENTIAL or SECRET component or equipment is mounted externally on the vehicle or aircraft, the vehicle or aircraft will be secured with the physical security measures in paragraph 3–3.

c. When located at other than Active Army, USAR, or ARNG facilities, Army vehicles or aircraft with CONFIDENTIAL or SECRET components or equipment mounted internally or externally will be secured with at least the

minimum physical security measures. These vehicles and aircraft will be guarded at all times by an appropriately cleared crew member, dedicated military, DA civilian, or contract guards.

d. Army vehicles or aircraft with TOP SECRET components onboard equipment will be under constant surveillance by appropriately cleared armed guards regardless of location.

e. Equipment or components should not be removed from vehicles or aircraft solely to fulfill a secure storage requirement. Frequent removal may cause increased equipment maintenance and may degrade operational readiness. However, classified equipment or components that can be readily dismounted without probable damage may be dismounted and placed in secure storage meeting the requirements of AR 380–5, TB 380–41, and this regulation.

f. In environments or unusual circumstances not clearly defined as requiring specific security measures under this regulation, the commander will designate proper equivalent security measures to protect those vehicles or aircraft that contain classified equipment or components.

g. Army vehicles or aircraft with classified equipment or components will be included in all aspects of the physical security program.

3–19. Mission–critical and high–risk personnel

a. Security procedural measures. MACOM commanders assigned the responsibility for designated geographical areas will designate mission–critical and high–risk personnel. Refer to AR 190–58 and AR 525–13 for additional guidance.

(1) *Risk Level I.* Access to those areas of the facility where mission–critical and high–risk personnel are located will be controlled continuously when the facility is occupied.

(2) *Risk Level II.* Access to the entire facility will be controlled continuously when the facility is occupied.

(3) *Risk Level III.*

(a) Access to the entire facility will be controlled at all times.

(b) Access to the area surrounding the facility will be controlled during times when the facility is occupied.

(c) Personnel not assigned to the facility who enter areas of the facility in which mission–critical or high–risk personnel are located will be searched for weapons and explosives on at least a random basis.

(d) Continuous surveillance of the area surrounding the facility will be provided at all times when the facility is occupied.

b. Terrorism counteraction measures.

(1) *Risk Level I.*

(a) Parking beneath facilities will be eliminated where possible.

(b) Parking will be kept as far away from the facility as possible, but at least 30 feet.

(c) Trash receptacles, landscaping features, and other features greater than 1 foot in height which potentially provide concealment for aggressors or bombs will be kept at least 30 feet from the facility.

(d) Locate mission–critical or high–risk personnel in the interior of the facility as far from the exterior as possible where feasible.

(2) *Risk Level II.*

(a) Windows into areas occupied by mission–critical or high–risk personnel will be covered by reflective 4–mil fragment retention film which will be backed up by heavy drapes.

(b) Windows and doors into areas occupied by mission–critical or high–risk personnel will be locked such that any attempt to enter through them when the facility is unoccupied will require forced entry, whose effects will be noticeable.

(c) Exterior walls will be constructed of reinforced concrete or reinforced concrete masonry.

(d) Duress alarms will be installed in areas occupied by mission–critical and high–risk personnel.

(3) *Risk Level III.*

(a) The facility will be surrounded by a perimeter fence at a distance from the facility of at least 50 feet.

(b) The facility will be constructed to resist the applicable weapons and explosives effects according to TM 5–853–1.

3–20. General civilian and or military personnel

a. Security procedural measures.

(1) *Risk Level I.* No such measures apply at this risk level.

(2) *Risk Level II.* Access to the facility will be controlled at all times that the facility is occupied.

(3) *Risk Level III.* Access to the facility and the area surrounding it will be controlled continuously when the building is occupied.

b. Terrorism counteraction measures.

(1) *Risk Level I.*

(a) Parking beneath facilities will be eliminated where possible.

(b) Parking will be kept as far away from the facility as possible, but at least 30 feet.

(c) Trash receptacles, landscaping features, and other features greater than 1 foot in height which potentially provide concealment for aggressors or bombs will be kept at least 30 feet from the facility.

(2) *Risk Level II.*

(a) Windows in the facility will be covered with 4–mil reflective fragment retention film which will be backed up by heavy drapes.

(b) Exterior walls will be constructed of reinforced concrete or reinforced concrete masonry or brick.

(3) *Risk Level III.*

(a) The facility will be surrounded by a perimeter fence at a distance from the facility of at least 50 feet.

(b) The facility will be constructed to resist the applicable weapons and explosives effects per TM 5–853–1.

3–21. Industrial and utility equipment

a. Security procedural measures.

(1) *Risk Level I.*

(a) Access into the area where the equipment is located will be controlled.

(b) Keys to facilities and equipment will be controlled per appendix D.

(c) The area will be designated a restricted area (see AR 190–13).

(2) *Risk Level II.* Measures for Risk Level I will be applied and equipment will be checked by roving patrols at intervals not to exceed every 4 hours when the facility is unattended.

(3) *Risk Level III.* Measures for Risk Levels I and II will be applied except that checks by roving patrols will be every 2 hours when the facility is unattended.

b. Terrorism counteraction measures.

(1) *Risk Levels I and II.*

(a) If the equipment is not located within a structure, the area will be surrounded by a perimeter fence.

(b) If the equipment is stored within a structure, the structure will meet the requirements of a secure storage structure for the appropriate risk level according to appendix B.

(2) *Risk Level III.*

(a) If the equipment is not located within a structure, the area or vulnerable items of equipment will be surrounded with an 8–foot–high reinforced concrete or masonry perimeter wall.

(b) If the equipment is located within a structure, the structure will meet the requirements of a secure storage structure for this risk level according to appendix B. The structure will be further enhanced to resist the applicable weapons and explosives effects according to TM 5–853–1.

Section III
Minimum Security Standards for Other Categories of Army Property

3–22. 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 U.S. Government approved key–operated tumbler–type lock, consisting of either a padlock (including brass padlocks issued with the tool boxes) or a factory installed built–in key–operated tumbler type lock. The individual who signed for the set or kit will retain the key. A duplicate key may be held by the supervisor or commander if it is stored in a locked container with controlled access.

c. 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 (user, tool room keeper, or guard), will be stored in a secure location. Nonportable items will be secured in the building or van in which they are located. Doors and windows will be closed and locked. Secure locations for portable items include:

(1) A locked building or room meeting the requirements for a secure storage structure in appendix B or a 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 (wall locker, desk, etc.) 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 through a locally devised receipt, sign–in/sign–out log, or exchangeable tag system. 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 to the maximum extent practical. If possible, access will be limited to the user, the individual designated as responsible for security items when not in use, and supervisory or command personnel.

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. Consideration should be given to marking these items as indicated in appendix C of this regulation.

3–23. Administrative and housekeeping supplies and equipment

a. Property management and accountability directives.

(1) AR 210–6.

(2) AR 230–1.

(3) AR 230–65.

(4) AR 380–19.

(5) AR 710–2.

(6) AR 735–5.

(7) DA Pam 710–2–1.

b. Minimum security standards for furniture and mess equipment.

(1) Work buildings or rooms in which these items are located will be secured when no responsible member permanently assigned to that particular activity is present.

(2) Furniture in day rooms or similar common areas used mainly during nonduty hours, and not normally staffed, will be protected by controlling access to these areas to the maximum extent practical. This may be done by requiring an individual desiring to use the facility to sign for the keys or having a charge–of–quarters duty officer, NCO, or other designated individual periodically check the facility.

(3) Occupants will secure Government furniture located in their quarters.

c. Minimum security standards for office machines.

(1) 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.

(2) Automated systems, including word processing systems, will be secured per AR 380–19.

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

d. Minimum security standards for expendable and consumable supplies.

(1) At unit and office levels, items not issued for actual use will be centrally stored in secure cabinets, containers, rooms, or buildings. Keys, locks, protective seals, and access to storage facilities will be controlled.

(2) Self–service supply center (SSSC) account cards or plastic credit cards will be stored in a locked container when not in use. Access to these items will be controlled and access will be limited to the fewest individuals feasible, consistent with efficient operations.

(3) Pilferable items will be stored in the SSSC and issued from a security area such as a cage. The SSSC will be protected by physical measures meeting the secure storage structure standards in appendix B.

3–24. Controlled cryptographic items (CCI)

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. CCI protective measures. CCI 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 procedures addressed in paragraphs*c* and *d* below establish minimum standards for controlling access to CCI (installed or uninstalled) to protect against tampering, loss, and unauthorized use and apply only to unkeyed CCI which are unclassified. Installed CCI, for the purposes of this regulation, means the equipment on hand 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 CCI are classified and will be protected per AR 380–40. DA Pam 25–380–2 will be used for additional guidance for safeguarding and handling CCI. Commanders should provide security protection for unclassified CCI 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 CCI.

(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 CCI will be parked and protected as indicated in paragraphs 3–3, 3–4, and 3–5.

(3) When commanders select double–barrier protection for CCI, 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 TB 380–40–22 and this regulation. Physical access will be limited only to authorized individuals.

(2) Access to keys and locks protecting CCI 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 CCI, controlling access to and use of CCI, and reporting of incidents of loss or tampering, as a minimum, will be published.

3–25. Unit supply rooms

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. Access to items stored in the supply room will be controlled at all times by the supply NCO or other designated individual. Lock and key control procedures as indicated in appendix D apply.

3–26. Postal unique items

Minimum security standards are in DOD 4525.6–M, Volumes I and II.

Chapter 4
Security of Medical Supplies and Equipment

Section I
Policy and Personnel Selection

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 policy

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

b. A Category 2 Serious Incident Report will be submitted per AR 190–40 for significant theft, loss, or recovery of

Government–owned or possessed narcotics; dangerous drugs; controlled substances; precious metals; radioactive or other sensitive materials, including sensitive medical material or equipment; or mismanagement of stock records or recovery procedures for those items that prevent a determination of loss.

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

4–3. Personnel selection

Personnel who are assigned duties that require access to controlled medical substances and sensitive items storage areas, including volunteers or those who have custodianship or possession of keys and combinations to locks securing such areas, will be carefully selected.

a. Selection criteria. Criteria for selection of these personnel include moral character, prior employment or military service history, maturity, and trustworthiness. Prior to assuming these duties—

(1) Designated persons will have satisfactorily undergone a local file check with area provost marshals, local civilian police, if not prohibited by law and per AR 190–27, and other agencies which might have information on file which would reflect on the honesty or stability of the individual. The National Crime Information Center (NCIC) cannot be used for this purpose. It can only be used to determine if the person has any outstanding warrants. NCIC warrant checks will be requested, in writing, from the supporting installation provost marshal office. Personnel exhibiting financial irresponsibility will be excluded from consideration. Non–Government workers (for example, volunteer workers) will not be given unescorted access to controlled medical substances and sensitive items. For new Government employees, results of investigations such as the National Agency Check and Inquiry required by DOD 5200.2–R should be known prior to granting them unescorted access.

(2) An interview with the lowest level commander having command responsibility for the security of subject items is required. The purpose of the interview is to appraise the individual's character, judgment, reliability, attitude, emotional or mental maturity, and sense of responsibility. DA Pam 611–1 may be used as a guide for conducting the interview. The interview will be documented in writing.

(3) The names and duty positions of personnel authorized unaccompanied access to controlled medical substances and medically sensitive items storage areas will be depicted on a roster, which will be posted inside the storage area.

b. Access reinstatement. Access to controlled substances denied to individuals undergoing investigation, treatment, rehabilitation, judicial or nonjudicial processes, or administrative action as a result of actual or suspected drug use may be reinstated when—

(1) Suspicions or allegations against the individual are determined to be unfounded.

(2) Rehabilitation is successful under the provisions of AR 40–66.

(3) Commander approves medical treatment facility credentials committee recommendations for reinstatement under the provisions of AR 40–66.

4–4. In–transit security of controlled medical substances and other medically sensitive items

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

4–5. Disposal of controlled medical substances and items

Disposal of controlled medical substances and items will be per the provisions of AR 40–2, AR 40–61, and this regulation.

Section II
Structural Standards for Bulk Storage Facilities

4–6. Storage of Notes R, Q, and C items

Bulk storage for Notes R, Q, and C controlled medical items (see glossary) will conform to the physical security standards established in this chapter. Protection of containers of Notes R, Q, and C medical items in bulk storage or the vault, room, or structure in which the containers are located will include IDS (para 4–13) which will be in operation at all times when supervisory or duty personnel are not present within or at the area or container. The criteria prescribed for the review of IDS in AR 190–13 apply. Bulk storage facilities will be designated and posted as restricted areas. In overseas commands and in continental United States border locations, areas will be posted both in English and in the host or bordering nation's language.

4–7. Note R items

Items identified as Note R will be stored in an approved safe or vault secured with a Class 5 vault door.

a. Small quantities of controlled medical substances may be stored in any General Services Administration (GSA) approved safe.

b. Minimum structural standards for a vault at a new facility are detailed in appendix B.

c. At an existing facility where it is not feasible to construct the type of vault described in appendix B, a storage site will be selected according to the alternate vault criteria described in appendix B.

4–8. Note Q items

Items identified as Note Q will be stored as provided in paragraph 4–7; however, dual door protection (although desirable) may be eliminated provided the entrance door is as specified in appendix B. Restricted area protection will be provided. General medical items or supplies will not be stored with Note Q items.

4–9. Note C items

Depending on content, Note C chests, kits, outfits, other assemblages, or withdrawn controlled medical items will be stored as provided in paragraphs 4–7 and 4–8.

4–10. Controlled medical substances or sensitive medical items

Controlled medical substances or sensitive items will be considered by the facility commander for storage in secure storage structures (app B) or in locked containers. Containers will be locked at all times except during restocking, inventory, or dispensing operations. As a minimum, storage should be in a restricted area and protection provided should be consistent with the type of item and perceived local threat of theft or diversion to unauthorized use.

Section III
Physical Security Measures and Control Procedures

4–11. Safeguards during nonduty 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 ensure that—

(1) No Note R, Q, and C items remain unprotected or exposed and that they are secured in designated containers.

(2) Containers are locked and checked properly with such action recorded on SF 702 (Security Container Check Sheet).

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

(4) 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.

4–12. Security checks

a. Military or security police or interior guards will make checks every 2 hours of all isolated structures. Facilities within hospitals or other medical or research, development, test, and evaluation (RDT&E) facilities, complexes, or structures may be checked by duty officers or other duty, medical, or unit personnel.

b. When the medical or RDT&E facility is not occupied, security checks will be conducted at irregular intervals not to exceed every 4 hours to avoid establishing a pattern. The frequency of checks will be increased to every 2 hours during nights, weekends, and holidays to provide for deterrence and early detection of entry.

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

d. 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.

e. Records of security checks will be made and will be maintained in activity files for 90 days.

4–13. Intrusion detection system and security lighting

a. To meet minimum requirements for a storage area, the IDS will consist of at least two types of intrusion 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.

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

(2) If the substances are not entirely within a container, IDS sensors will be installed such that they detect intruders before they breach any components of the vault, room, or building that are associated with providing delay to the

intruders. 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 U.S. Army Corps of Engineers guide specifications. When local conditions dictate, a duress switch or holdup button may be added. The design review requirements of AR 190–13 apply.

c. An SOP for the activation, deactivation, and daily testing of the IDS will be published by the security office or the provost marshal office. The SOP will include instructions for maintaining an accurate IDS log.

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

4–14. Lock and key control

Commanders will establish procedures for the protection of locks, keys, and combinations used to secure facilities, vaults, and containers in which controlled medical substances and sensitive items are stored. The number of people with access to keys and combinations will be the minimum necessary for efficient operations. Provisions of appendix D and FM 19–30 will be followed in establishing procedures.

Section IV
Physical Security Standards for Pharmacy Storage

4–15. Pharmacy storage structural standards

Pharmacy storage facilities will conform to the following physical security standards:

a. Pharmacy Note R items will be stored per paragraph 4–7 and as noted in appendix B.

b. Pharmacy Note Q items will be stored per paragraph 4–8 and as noted in appendix B. As a minimum, Note Q items will be stored in locked cells of automatic counting machines or in locked metal containers inside the pharmacy.

c. Depending on the content, pharmacy Note C items will be stored per requirements for Note Q or Note R items above.

d. The pharmacy structure will be constructed as a vault as detailed in appendix B except as noted.

4–16. Physical security measures and control procedures

The following are minimum standards and controls considered necessary to ensure that positive security is provided for pharmacies:

a. All storage in pharmacies will be designated as restricted areas. When operationally feasible, containers of Note R and Note Q items will be positioned so their locations are not visible to the public during operating hours.

b. Within reasonable limits, containers will be locked when access is not required for operational use. Lock and key control security procedures prescribed in paragraph 4–14 are applicable and will be adhered to in pharmacy operations.

c. Pharmacies and their storage areas (if containing controlled substances) will be provided with both interior and exterior lighting of sufficient intensity to enable visual surveillance by security forces, duty officers, or other designated personnel. Security checks will be conducted and documented every 4 hours during nonoperational hours. Particular attention will be directed to doors, windows, and other possible points of entry. Entrance doors will be locked at all times, except when authorized personnel are entering or exiting the pharmacy.

d. IDS will be provided for all U.S. Army Medical Center (MEDCEN) and medical department activity (MEDDAC) pharmacies. The minimum standards for intrusion detection equipment described in paragraph 4–13 apply. In addition, a duress switch or holdup button will be provided in a hidden location at the dispensing window to permit pharmacy personnel to notify the supporting police agency from which an armed response force can be dispatched. Personnel on duty will have access to the duress alarm actuator at all times during periods of operation. Coordination will be made with the installation police to schedule a test of the system at intervals not to exceed 90 days.

e. All instances of suspected theft, illegal entry, unlocked facilities or containers, and other suspicious incidents will be reported immediately to designated personnel, and action will be taken as indicated in paragraph 4–12*e*.

Section V
Medical Treatment Facilities and Research, Development, Test, and Evaluation (RDT&E) Laboratory Facilities

4–17. Medical treatment facilities and RDT&E laboratory structural standards

Clinics; hospital wards; clinical nursing units; medical specialty, dental, and veterinary facilities; and RDT&E laboratory facilities will conform to the physical security standards listed below.

a. When duty personnel are in attendance 24 hours a day, normal operating quantities of Note R items will be stored in double–locked containers. Containers must be constructed so that forced entry is readily apparent to visual examination. When duty personnel are not present 24 hours a day, normal operating quantities of Note R items will be stored in a GSA–approved safe and an additional barrier will be provided, such as securing safes inside a locked room.

b. Normal operating quantities of Note Q items will be stored according to the criteria in paragraph *a* above. If this is not possible, containers constructed of a minimum of 26–gauge steel with a single lock may be used, provided additional security measures are taken (for example, increased surveillance or improved lighting) and provided the steel container is secured inside a locked room.

c. Precious metals and fabricated dental appliances containing precious metals will be secured against theft, loss, or damage consistent with their monetary value and the difficulty of replacement.

4–18. Physical security measures and control procedures

a. All storage containers for Note R and Q items will be located in restricted areas.

b. Keys and combinations to containers of controlled medical substances, sensitive items, and precious metals will be issued only to individuals authorized access to these items. Containers will be secured after duty hours. To prevent loss or theft during operating hours, containers will be unlocked only when property is being inserted, removed, or when the container is under the observation of designated personnel. Lock and key control procedures prescribed in paragraph 4–14 will be followed.

c. Unit dose carts containing controlled substances will be kept in restricted areas when not in use.

d. To prevent loss or theft during the administration of medications, unit dose carts will be kept under the physical control or unobstructed observation of designated personnel.

e. Storage areas will be provided with interior and exterior lighting operational at all times during the hours of darkness.

4–19. Crash carts, emergency trays, and ambulances

a. The number of crash carts and emergency trays (essential emergency assemblages) that contain controlled substances will be kept to a minimum and will be provided with maximum security consistent with requirements for immediate availability. When controlled medical substances or items are issued to emergency medical team personnel assigned to ambulance or emergency vehicle response duties, the controlled substances or items will not be stored in the vehicle while it is unattended. Controlled substances and items must remain under control or observation of responsible personnel at all times and will be stored in restricted areas when possible.

b. Locking devices on emergency assemblages hinder immediate availability to controlled medical substances and sensitive items by medical treatment personnel and will not be used. Appropriate sealing devices will be used to indicate tampering and to assist in inventory, but they must be easily opened without the use of a key, combination, or other time–delaying device.

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

d. Accountability and control requirements of AR 40–2 also apply and will be met.

4–20. 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 as indicated in paragraph 4–14.

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 (“Sharps” containers). Sharps containers 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.

Chapter 5
Physical Security of U.S. Army Museums

Section I
Inspections and Personnel Selection

5–1. General

This chapter prescribes specific physical security standards, policies, procedures, 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 according to AR 190–11. Arms in storage may remain in operable condition. All other items will be secured and inspected as indicated in this regulation.

5–2. Inspections
Physical security inspections of museum facilities will be conducted per AR 190–13 and the criteria outlined in this regulation. Inspections of museum arms storage facilities will be per AR 190–11.

5–3. Museum personnel selection
Military or 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 provost marshal in response to a written request before personnel are assigned or attached (including special duty personnel) to museum duties. NCIC 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, provost marshal or equivalent security officer, and supporting facility engineers. Museum buildings and apertures providing access to the building should be modified or constructed so as 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
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, etc., will be secured per AR 190–11.

a. Key custodian. The museum director will be designated the key custodian, whenever feasible. The commander or designated deputy will appoint the primary and an alternate key custodian in writing.

b. Locks.

(1) Exterior doors used for access to museum facilities will be secured with U.S. Government–approved padlocks (procured under MIL–A–A–1927 (NSN 5340–00–158–3807 or NSN 5340–00–158–3805), grade II, hardened steel shackle and body) or deadbolt or other locks equal to these devices as determined by the servicing facility engineer if installation does not detract from the aesthetic value of the facility. Approved locking devices are contained in appendix D. The number of exterior doors with exterior exposed padlocks will be kept to the absolute minimum. All other exterior doors will be secured on the inside.

(2) Vehicles and facilities in which vehicles are stored will be secured as stated in paragraph 3–5.

c. 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) The use of a master or multiple key system is prohibited.

(4) Where an Army museum or exhibit is protected by an approved IDS and the IDS is operational, 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 approved 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 central military police station. Museum personnel, as authorized by the museum curator or director, will retain custody of the keys in this strongbox.

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

(6) 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 supporting facility engineers.

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 FM 19–30 to determine specific 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. Procedures for obtaining IDS are outlined in AR 190–13. Additional guidance may be found in FM 19–30.

5–8. Exhibit or display cases

The viewing surfaces of exhibit or display cases will be constructed of at least 1/4 inch–thick plate 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. Nonviewing surfaces of cases will be constructed to offer a higher degree of protection than the viewing surface.

5–9. Museum workshops

Workshops used by museum personnel for maintenance or restoration work will be secured at the close of each business day. Workshops containing AA&E will be secured as stated in paragraph 5–1.

5–10. Security forces

a. Each museum will be attended by at least one member of the museum staff, who 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, nonconnecting 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. To ensure adequate surveillance of all parts of the museum, the installation of one–way mirrors and electronic sensing devices should be considered. Museum parks and exterior displays will be provided electronic surveillance where practical and checked periodically by security patrols.

b. Commanders must ensure that all 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 nonduty hours on a daily basis.

5–11. Museum parks

Large items of historical property that are displayed outdoors in museum parks will be anchored to prevent theft. 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, the commander or his or her designated representative will establish liaison with local civil police agencies to ensure that—

a. Security checks are conducted by local police.

b. A coordinated plan for security exists.

5–13. Reporting loss of property

Loss of historical property other than AA&E will be reported by the provost marshal or equivalent security officer according to AR 190–40. 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.

5–15. Museum weapons and ammunition

Security of museum weapons and ammunition will be accomplished per the requirements of AR 190–11. Marking of museum weapons and ammunition will be per appendix C.

Appendix A
References

Section I
Required Publications

AR 40–2
Army Medical Treatment Facilities; General Administration. (Cited in paras 4–5 and 4–19.)

AR 40–61
Medical Logistics Policies and Procedures. (Cited in paras 4–4 and 4–5.)

AR 40–66
Medical Record and Quality Assurance Administration. (Cited in para 4–3.)

AR 190–11
Physical Security of Arms, Ammunition, and Explosives. (Cited in paras 3–3, 3–5, 3–16, 5–1, 5–2, 5–3, 5–5, 5–7, 5–15, and D–1.)

AR 190–13
The Army Physical Security Program. (Cited in paras 1–4,1–5, 2–2, 2–3, 3–3, 3–5, 3–14, 4–6, 4–13, 5–2, and 5–7.)

AR 190–40
Serious Incident Report. (Cited in paras 4–2 and 5–13.)

AR 190–58
Personal Security. (Cited in para 3–19.)

AR 380–5
Department of the Army Information Security Program Regulation. (Cited in paras 3–3, 3–5, and 3–18.)

AR 380–19
Information Systems Security. (Cited in para 3–23.)

AR 380–40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material. (Cited in para 3–24.)

AR 525–13
The Army Terrorism Counteraction Program. (Cited in para 3–19.)

AR 700–84
Issue and Sale of Personal Clothing. (Cited in para 3–8.)

AR 710–2
Supply Policy Below the Wholesale Level. (Cited in paras 3–3, 3–5, 3–6, 3–16, 3–22, 3–23, and 3–24.)

AR 710–3
Asset and Transaction Reporting System. (Cited in para 3–24.)

AR 870–5
Military History: Responsibilities, Policies, and Procedures. (Cited in para 5–14.)

AR 870–20
Historical Properties and Museums (Cited in para 5–13.)

DA Pam 25–380–2
Security Standards for Controlled Cryptographic Items. (Cited in para 3–24.)

DA Pam 190–51
Risk Analysis for Army Property. (Cited in paras 1–4, 1–5, 2–2, 3–1, and 3–24.)

DA Pam 611–1
The Army Interview. (Cited in para 4–3.)

DOD 4160.21–M
Defense Disposal Manual. (Cited in para 3–11.)

DOD 4270.1–M
Construction Criteria. (Cited in para 3–13.)

DOD 5200.2–R
Personnel Security Program. (Cited in para 4–3.)

DODD 5200.8
Security of Installations and Resources. (Cited in the Summary.)

FM 19–30
Physical Security. (Cited in paras 3–1, 3–3, 3–5, 3–9, 4–14, 5–6, and 5–7.)

TB 9–2300–422–20
Security of Tactical Wheeled Vehicles. (Cited in para 3–5.)

TB 43–001–39–7
Equipment Improvement Report and Maintenance Digest. (Cited in para 3–5.)

TB 380–40–22
Security Standards for Controlled Cryptographic Items (CCI). (Cited in para 3–24.)

TB 380–41 (series)
Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material. (Cited in paras 3–3 and 3–18.)

TM 5–853–1
Security Engineering, Designing for Security. (Cited in paras 1–5, 3–19, 3–20, 3–21 and B–1.)

Drawing No. 40–16–08
U.S. Army Corps of Engineers Drawing No. 40–16–08, Type FE–5. (Cited in para 3–1*d*.)
(If drawing is not available from the installation engineer, requests may be forwarded to the Commander, U.S. Army Corps of Engineers, Huntsville Division, ATTN: CEHND–ED–ES–1, P.O. Box 1600, Huntsville, Alabama 35807–4301.)

Section II
Related Publications

The National Guard regulation listed applies only to Army National Guard personnel.

AR 30–1
The Army Food Service Program.

AR 30–18
Army Troop Issue Subsistence Activity Operating Procedures.

AR 30–19
Army Commissary Store Operating Policies.

AR 40–7
Use of Investigational Drugs in Humans and the Use of Schedule I Controlled Drug Substances.

AR 58–1
Management, Acquisition and Use of Administrative Use Motor Vehicles.

AR 95–1
General Provisions and Flight Regulations.

AR 108–2
Army Training and Audiovisual Support.

AR 190–16
Physical Security.

AR 190–27
Army Participation in National Crime Information Center (NCIC).

AR 210–6
Furniture and Household Equipment Support for Family Housing and Bachelor Housing.

AR 230–1
The Nonappropriated Fund System.

AR 230–65
Nonappropriated Funds: Accounting and Budgeting Procedures.

AR 420–17
Real Property and Resource Management.

AR 420–70
Buildings and Structures.

AR 703–1
Coal and Petroleum Products Supply and Management Activities.

AR 708–1
Cataloging and Supply Management Data.

AR 725–50
Requisitioning, Receipt, and Issue System.

AR 735–5
Policy and Procedures for Property Accountability.

AR 740–26
Physical Inventory Control.

DA Pam 710–2–1
Using Unit Supply Systems Procedures Manual.

DA Pam 738–750
The Army Maintenance Management System (TAMMS).

DOD 4525.6–M
DOD Postal Manual, Volumes I and II.

NGR 190–11
Physical Security of Arms, Ammunition, and Explosives

TB 43–0209
Color, Marking, and Camouflage Painting of Military Vehicles, Construction Equipment, and Materials Handling Equipment.

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Forms that have been designated“approved for electronic generation (EG)” must replicate exactly the content (wording), format (layout), and sequence (arrangement) of the official printed form. The form number of the electronically generated form will be shown as –R–E and the date will be the same as the date of the current edition of the printed form.
Exact replication of any DA or DD forms prescribed in this regulation that are generated by the automated Military Police Management Information System may be used in place of the official printed version of the form.

DA Form 1687
Notice of Delegation of Authority–Receipt for Supplies.

DA Form 2028
Recommended Changes to Publications and Blank Forms.

DA Form 5513–R (approved for EG)
Key Control Register and Inventory.

Standard Form 700
Security Container Information.

Standard Form 701
Activity Security Checklist.

Standard Form 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 assets covered by this regulation. The construction standards for each type of storage structure vary according to the risk level associated with the assets stored. These standards will provide the minimum acceptable security for the assets stored 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 TM 5–853–1 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 structures 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.* 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 continuously spaced 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:

(a) 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. Nails will not be used to mount hinges or any other door hardware.

(b) Door hinge pins should not be exposed to the exterior of the facility. If they are, they will be spot welded, covered, filled, or otherwise secured to prevent easy removal.

(c) 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. Latch style door locks will not be used. Locking devices will conform to U.S. Army Corps of Engineers guide specifications.

(d) Doors secured from the outside will have locking devices conforming to U.S. Army Corps of Engineers guide specifications for the type of structure or with U.S. Government approved tumbler-type, key-operated padlocks. The servicing facility engineer will verify lock conformance with the guide specification.

(2) *Risk Level II.* Doors will be a minimum of 16–gauge minimum hollow steel construction with a minimum of frame construction of 16–gauge steel. Installation requirements for Risk Level I also apply. Alternatively, doors or pairs of doors will provide delay time equal to or greater than the response time.

(3) *Risk Level III.* Doors will be a minimum of 1 ¾-inch solid core wood with wood block cores and 12–gauge minimum steel plate on both sides or doors will be 12–gauge minimum hollow steel doors reinforced with vertical stiffeners at 6 inches on center. 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 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, bar, mesh, or fence fabric assemblies will completely enclose the air–conditioning unit protruding from the building or storage room exterior. If the window air conditioner is mounted through the wall, measures will be taken to ensure that it cannot be removed from the outside.

(1) *Risk Level I.* Operable windows will have adequate individual locking devices. Windows will also be covered with ½-inch diameter bars spaced at 6 inches on center each way, with ⅙-inch expanded metal mesh, or with 9–gauge chain link fabric.

(2) *Risk Level II.* Windows will be inoperable. They will be covered with bars or mesh as for Risk Level I and the glass will be covered with 4–mil fragment retention film or they will have ½-inch thick laminated glass or plastic security glazing. Alternatively, windows will provide delay time 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 ½-inch thick laminated glass or plastic security glazing. Alternatively, windows will provide delay time equal to or greater than the response time.

c. Walls.

(1) *Risk Level I.* Walls will be constructed of at least ½-inch plywood, 1–inch tongue–in–groove wall boards, or 26–gauge steel siding.

(2) *Risk Level II.* Walls will be constructed of 4–inch minimum thickness brick and stud construction or of 8–inch minimum thickness concrete masonry (unreinforced). Alternatively, walls will provide delay equal to or greater than the response time.

(3) *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 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 of at least ½-inch plywood, 1–inch tongue-in-groove wall boards, or 24–gauge steel deck.

(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 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 equal to or greater than the response time.

B–3. Controlled substance storage vault structural standards

Vaults for storage of controlled medical substances will meet the following construction standards for doors, windows, walls, ceilings, and floors as appropriate for the applicable risk level. These standards apply for both Note Q and Note R controlled medical substances except as noted. Separate standards are established for new construction and existing construction. Prefabricated modular vaults which provide similar resistance to forced entry may also be used.

a. New construction.

(1) *Doors.* Doors will be limited to the minimum number required. Doors for all risk levels will be Class 5 vault doors. Alternatively, doors or pairs of doors will provide delay equal to or greater than the response time.

(a) If the vault is required to remain open for frequent access, it must be equipped with a self–closing and self–locking "day gate" or its equivalent.

(b) If the vault is required to be open only briefly and infrequently, and if it is relocked immediately after use, a"day gate" is not required.

(c) Dual door protection is not required for storage of Note Q items provided the entrance door is of solid wood, a minimum of 1 3/4 inches thick, and covered on the exterior with sheet steel not less than 12 gauge United States standard (USS) secured with a high–security padlock and a high–security hasp and hung on security hinges.

(d) Doors will be secured with a Group 1R changeable combination lock, a high–security padlock (Military Specification MIL–P–43607 or NSN 5340–01–188–1560 or 5340–00–799–8248) and hasp (Military Specification MIL–H–43905 or MIL–H–29181A (YD)), or other comparable hasps and locking hardware as verified by the servicing facility engineer.

(2) *Windows.* Windows will not be allowed in vaults in new facilities.

(3) *Walls.*

(a) Risk Levels I and II. Walls will be constructed of a minimum of 8–inch–thick concrete reinforced vertically and horizontally on each face with ½-inch diameter reinforcing bars placed 9 inches on center and staggered to form a grid approximately 4½-inches square or with 8–inch thick reinforced concrete masonry with ½-inch diameter reinforcing bars placed at 8 inches on center in block cells filled with grout or mortar and with horizontal joint reinforcement at every course. Alternatively, walls may be constructed to provide delay equal to or greater than the response time.

(b) Risk Level III. Walls will be constructed of a minimum of 8–inch thick reinforced concrete as described above. Reinforced masonry will not be used for new construction at this risk level. Alternatively, walls may be constructed to provide delay equal to the response time.

(4) *Floors and ceilings.* Floors and ceilings for all risk levels will be constructed of a minimum of 8–inch thick concrete reinforced in both directions with ½-inch diameter reinforcing bars placed 9 inches on center and staggered to form a grid approximately 4½-inches square. This requirement does not apply to reinforced concrete floor slabs on grade, which may be constructed of 6–inch thick reinforced concrete. Alternatively, floors and ceilings may be constructed to provide delay equal to the response time.

b. Existing construction.

(1) *Doors.* Doors will be limited to the minimum number required. Door hinges will not be removable from outside of the vault. Security hinges are preferred, but if conventional hinges are used, hinge pins will be spot welded, peened, covered, or otherwise secured to prevent removal. Primary doors will be secured with a Group 1R changeable combination lock, a high–security padlock (Military Specification MIL–P–43607G or NSN 5340–01–188–1560 or 5340–00–799–8248) and hasp (Military Specification MIL–H–43905 or MIL–H–29181A (YD)), or other comparable hasps and locking hardware. Other doors will be secured from the inside with deadbolt locking devices, crossbars, or similar locking devices resistant to jimmying and manipulation from the outside.

(a) Risk Level I. Doors will be Class 5 vault doors or will consist of a two–door back-to-back system whose outer door is at least 1 3/4–inch solid core wood with wood block cores and 16–gauge minimum steel plate on the exterior side or a 12–gauge minimum hollow steel door reinforced with vertical stiffeners at 6 inches on center. The inner door will be constructed of a minimum of ½-inch steel bars welded to form a grid with openings that do not exceed 32 square inches or to be of construction comparable to the outer door. Door frames for doors other than Class 5 vault doors will be constructed of 16–gauge steel minimum and will be grouted full. Dual door construction may be eliminated for Note Q controlled medical substances. Alternatively, doors or pairs of doors will provide delay equal to or greater than the response time.

(b) Risk Levels II and III. Doors will be as for Risk Level I, except that where a two–door back–to–back system is used, the inner door will be of the same construction as the outer door. Dual door construction may be eliminated for Note Q controlled medical substances. Alternatively, doors or pairs of doors will provide delay equal to or greater than the response time.

(2) *Windows.* The number of windows or other openings (such as vents or ducts) greater than 96 square inches in area will be limited to the minimum number which is essential. All window and other openings over 96 square inches will be completely blocked with construction equivalent to that of the wall in which the opening is located where possible.

(a) Risk Levels I and II. Windows which cannot be blocked will be inoperable and they will be covered with bars or mesh and will have ½-inch thick laminated glass or plastic security glazing. The bars or mesh will be secured to a steel channel frame fastened to the wall with smooth–headed bolts or embedded into the structure to prevent removal. Bar assemblies will be constructed with vertical bars spaced at not more than 4 inches on center and horizontal members welded together, to the vertical bars, and to the frame and spaced so that openings between bars do not exceed 32 square inches. Mesh assemblies will consist of 5/16-inch expanded metal with openings of not more than 2 inches in any direction. Alternatively, windows will provide delay time equal to or greater than the response time. If window air conditioners are used, the bar or mesh assemblies will completely enclose the air–conditioning unit protruding from the storage vault and measures will be taken to ensure that the unit cannot be removed from the outside.

(b) Risk Level III. All windows will be completely blocked. If equivalent wall construction is not feasible for use in blocking windows, steel plate at least ¼-inch thick may be bolted to the wall to block the window openings. Alternatively, windows will provide delay equal to or greater than the response time.

(3) *Walls.* Walls will be constructed according to the risk level as specified below. Walls will be securely affixed to the floor and ceiling of the vault.

(a) Risk Level I. Walls will be constructed of at least ½-inch plywood, 1-inch tongue-in-groove wall boards, or 26–gauge steel siding. The interior of the walls will be lined with 5/16–inch expanded metal mesh. Alternatively, walls will provide delay equal to or greater than the response time.

(b) Risk Level II. Walls will be constructed of 8–inch thick reinforced concrete masonry with ½-inch diameter reinforcing bars placed at 8 inches on center in block cells filled with grout or mortar and with horizontal joint reinforcement at every course or of brick in an inner and outer course interlocked to provide 8 inches of thickness. Alternatively, walls may be constructed to provide delay equal to or greater than the response time.

(c) Risk Level III. Walls will be constructed of reinforced concrete masonry as described for Risk Level II. Brick construction will not be used. Alternatively, walls may be constructed to provide delay equal to or greater than the response time.

(4) *Floors and ceilings.*

(a) Risk Level I. Floors and ceilings will be constructed of at least ½-inch plywood, 1–inch tongue–in–groove wall boards, or 24–gauge steel deck. The underside of the floor and ceiling will be lined with 5/16–inch expanded metal mesh with a maximum opening of 2 inches in any direction suspended with smooth–headed bolts to prevent removal. These requirements do not apply for existing concrete floors on grade. Alternatively, floors and ceilings will be constructed to provide delay equal to or greater than the response time.

(b) Risk Levels II and III. Floors and ceilings will be constructed of reinforced concrete. Alternatively, floors and ceilings may be constructed to provide delay equal to or greater than the response time.

B–4. Pharmacy storage structure standards

Pharmacy construction will meet the requirements of paragraph B–3 for new and existing construction with the following exceptions and additions.

a. Doors. Doors may be a minimum of 1 3/4–inch solid wood with security hinges, hinges on the inside face, or hinges which are spot welded, peened, covered, or otherwise secured to prevent easy removal. Locks will be as specified in paragraph B–3*b*.

b. Exterior windows. Windows, as a minimum, will be covered with bars or mesh as specified in paragraph B–3*b*.

c. Dispensing windows. During nonduty hours, dispensing windows will be secured from the inside (so that locks or bolts are inaccessible from the outside) with a solid wood door at least 1 3/4 inches thick, a steel roll–up door, steel mesh or steel bars as specified for windows in paragraph B–3*b*, or a means which provides equivalent security.

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.

C–2. Determining whether to mark property

a. The decision to mark Army property rests with the commander 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 rapidograph 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 (2) below 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 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 curators. Photographs, especially color, are extremely useful.

C–4. Marking other Army property

a. Standard marking system. Marking property is worthwhile only if it identifies a specific item as belonging to a particular organization. The recommended standard marking of Army property should—

(1) Use a "USA" prefix which alerts 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 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 individual 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 (including Hasps and Chains), and Protective Seals

D–1. General

a. Guidance on procedures for keys, locks, and locking devices (including 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 the identity of approved commercial equivalent locks and locking devices (including hasps and chains) meeting military specifications shall be addressed to the Naval Civil Engineering Laboratory (NCEL), ATTN: Code L56, Port Hueneme, CA 93043–4328. Personnel can obtain the most current version of these specifications by contacting the NCEL.

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–2. Key custodian and alternate custodian

A primary or alternate key custodian is the person who will—

a. Be appointed, in writing, to issue and receive keys and maintain accountability for office, unit, or activity keys.

b. Ensure that individuals designated to issue, receive, and account for keys in his or her absence, clearly understand local key control procedures.

c. Maintain a key control register at all times to ensure continuous accountability for keys of locks used to secure Government property.

d. Be listed on an access roster.

D–3. Key control register

Keys will be signed out to authorized personnel, as needed, on a key control register. The key control register, DA Form 5513–R (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 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.

D–5. Locks

a. The use of any master key system or multiple key system is prohibited except as noted elsewhere in this regulation.

b. U.S. Government key–operated, pin–locking deadbolts which project at least 1 inch into the door frame or tumbler–type padlocks will be used to safeguard unclassified, nonsensitive Army supplies and equipment if a lock is required. Selection will be based on the value of items protected, mission essentiality, and vulnerability to criminal attack. All questions regarding approved locks and locking devices will be addressed to the NCEL as indicated in paragraph D–1 above.

c. Padlocks 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–6. Key and lock accountability

a. Keys and combinations to locks will be accounted for at all times. Keys to locks in use which protect the property of an office, unit, or activity will be checked at the end of each duty day. Differences between keys on hand and the key control register will be reconciled.

b. 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.

c. When a key to a padlock is lost or missing, an inquiry will be conducted and the padlock replaced or recored immediately.

d. A key and lock inventory will be maintained which includes a list of all of the following:

(1) *Keys.*

(2) *Locks.*

(3) *Key serial numbers.*

(4) *Lock serial numbers.*

(5) *Location of locks.*

(6) *The number of keys maintained for each lock.* This list will be secured in the key depository.

e. Padlocks 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.

D–7. Additional key and lock controls for IDS and key containers

a. Keys to IDS (operational or maintenance) or key containers will not be removed from the installation 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 container itself. Keys to containers and IDS will be maintained separately from other keys, and will be accessible only to those individuals whose official duties require access to them.

(1) A current roster of these individuals 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 designated official and will contain the names of those individuals authorized to receive keys from the key custodian (para *d* below).

(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 key 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 low security padlocks or GSA–approved built–in three–position changeable combination locks, or in GSA–approved Class 5 or Class 6 containers that do not contain or store classified material. Combinations will be recorded on SF 700 (Security Container Information), sealed in the envelope provided, and stored in a container per AR 380–5.

(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.

c. In the event of lost, misplaced, or stolen keys, an investigation will be conducted immediately. The affected locks or cores to locks will be replaced immediately. Replacement or reserve locks, cores, and keys will be secured to preclude access by unauthorized individuals.

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 those individuals on the key access roster (para*a* above). Personnel listed on the roster may transfer custody, in writing, among themselves.

(1) 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.

(2) A key control register will be maintained at the unit level to—

(a) Ensure continuous accountability for keys.

(b) Ensure positive control of keys.

(c) Establish responsibility for the custody of stored AA&E. DA Form 5513–R may be used for this purpose. Completed key control registers will be retained in unit files for a minimum of 90 days and then disposed of per established MACOM procedures.

e. When individuals are charged with the responsibility for safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys.

(1) A sealed container is a locked and sealed key container or a sealed envelope (SF 700, per AR 380–5) containing the key or combination to the key container.

(2) When the sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. The seal need not be broken for 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.

(3) 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.

(4) Inventory records will be retained in unit files for a minimum of 1 year and then disposed of per established MACOM procedures.

f. Combination to locks on vault doors or GSA–approved Class 5 or Class 6 security containers will be changed annually or upon change of custodian, or 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, 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 ensure that the envelopes containing combinations to locks are not made available to unauthorized personnel.

g. Replacement of lock cylinders and broken keys for high–security locks may be requested through normal supply channels. Requests will be coordinated through the key control custodian. MACOMs are designated as approval authorities for any deviation in key procurement procedures.

D–8. 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 secondary 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 secondary padlocks.

D–9. Chains

When a chain is required for security of unclassified, nonsensitive equipment and supplies, specifications for approved chains will be obtained from the NCEL as indicated in paragraph D–1 above.

D–10. Use and control of protective seals

a. 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.

b. 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) *Ordering and issuing.* A single office on an installation will be responsible for ordering and issuing seals. The source for the seals will be instructed to ship the seals to the attention of a seal custodian in that office.

(6) *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.

c. Accounting for seals. Seal custodians will maintain seal logbooks, preferably 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.

d. 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 "click" when inserting point of seal into sheath.

(4) To ensure positive closure, tug down on strap and twist the point section inserted into the locking mechanism.

e. Checking seals. Commands using seals will develop procedures for checking them. These procedures will include actions to be taken to break a seal and actions to be taken upon finding a broken seal.

f. 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 individual removing the seal across from the original entry on the seal log.

g. Changing seals. The colors of seals will be changed periodically as an additional physical security measure.

Glossary

This is the consolidated glossary for the Physical Security Handbook.

Section I
Abbreviations

AA&E
arms, ammunition, and explosives

AC
Active Component

ACSI
Assistant Chief of Staff for Intelligence

ADP
automatic data processing

AE
ammunition and explosives

AFB
Air Force Base

AFH
Army family housing

AFI
annual formal inspection

AFSPA
Air Force Security Police Agency

AG
Adjutant General

AGS
Armed Guard Surveillance

AIF
Army Industrial Funds

AMC
U.S. Army Material Command

AMDF
Army Master Data File

AP
acquisition plan

APSEAG
Army Physical Security Equipment Action Group

AR
Army regulation

ARDEC
U.S. Army Armament Research, Development and Engineering Center

ARNG
Army National Guard

ARSTAF
Army Staff

ASA (IL&E)
Assistant Secretary of the Army (Installations, Logistics, and Environment)

ASA (RDA)
Assistant Secretary of the Army (Research, Development, and Acquisition)

ASI
additional skill identifier

ASI H3
ASI for physical security inspector

ASI P7
ASI for patrol/narcotics or contraband detector dog handler

ASI Z6
ASI for patrol/explosives detector dog handler

ASL
authorized stockage list

ASP
ammunition supply point

AT
antiterrorism

ATC
Air Training Command

ATCOM
U.S. Army Aviation and Troop Command

BASOPS
base operations

BATF
Bureau of Alcohol, Tobacco, and Firearms

BCU
battery coolant unit

BRDEC
Belvior Research & Development Engineering Center

CB
close boundary

CBT/T
combatting terrorism

CCI
controlled cryptographic items

CCP
circulation control point

CCTV
closed circuit television

CDR
commander

CE
U.S. Army Corps of Engineers

CECOM
U.S. Army Communications-Electronics Command

C-E
communications-electronics

CFM
cubic feet per minute

CG
commanding general

CL
carload

CMP
Civilian Marksmanship Program

COA
Comptroller of the Army

COCO
contractor-owned, contractor-operated

COE
Chief of Engineers

COFC
container-on-flatcar

COMDT
commandant

COMSEC
communications security

CONEX
container express

CONUS
continental United States

CONUSA
the numbered armies in the Continental United States

CPA
Chief of Public Affairs

CPCO
Central Port Call Office

CPR
civilian personnel regulation

CQ
charge of quarters

CRC
U.S. Army Crime Records Center

CSS
Constant Surveillance Service

CT
counterterrorism

CUCV
commercial utility and cargo vehicle

DA
Department of the Army

DAPSRB
Department of the Army Physical Security Review Board

DCSINT
Deputy Chief of Staff for Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations

DCSPER
Deputy Chief of Staff for Personnel

DDPS
Dual Driver Protective Service

DEA
Drug Enforcement Administration

DEFCON
defense readiness condition

DEH
Director of Engineering and Housing

DLA
Defense Logistics Agency

DNA
Defense Nuclear Agency

DOD
Department of Defense

DODD
Department of Defense directive

DOL
Director of Logistics

DPDO
Defense Property Disposal Office

DRMO
Defense Reutilization Marketing Offices

DTS
Defense Transportation System

DUSD(P)
Deputy Under Secretary of Defense for Policy

EDD
explosives detector dog

ENTNAC
Entrance National Agency Check

EOC
Emergency Operations Center

EOD
explosive ordnance disposal

FAA
Federal Aviation Administration

FBI
Federal Bureau of Investigation

FISO
Force Integration Staff Officer

FM
field manual

FMS
foreign military sales

FOA
field operating agency

FOB
free on board

FSC
Federal supply classification

FY
fiscal year

GBL
Government bill of lading

GOCO
Government-owned, contractor-operated

GOGO
Government-owned, Government-operated

GS
greater security

GSA
General Services Administration

GT
general technical aptitude area

GTR
Government transportation request

HQDA
Headquarters, Department of the Army

HQMC
Headquarters, United States Marine Corps

HSP
high security padlock

HUMINT
human intelligence

ID
identification

IDS
intrusion detection system

IED
improvised explosive device

IES
Illuminating Engineering Society

ILS
integrated logistic support

INSCOM
U.S. Army Intelligence and Security Command

ITO
installation transportation office(r)

JCS
Joint Chiefs of Staff

JMSNS
Justification for Major System New Start

JROTC
Junior Reserve Officers' Training Corps

JRWG
Joint Requirements Working Group

J-SIIDS
Joint-Service Interior Intrusion Detection System

JTAG
Joint Test Advisory Group

LAW
light antitank weapon

LCC
life cycle cost

LEA
law enforcement activity

LEC
law enforcement command

LIN
line item number

LOA
letter of agreement

LOI
Letter of Instruction

LR
letter requirement

LTC
lieutenant colonel

LTL
less than truckload

MAC
Military Airlift Command

MACOM
major Army command

MAJ
major

MATCU
military air traffic coordinating unit

MCA
major construction, Army

MEDCEN
U.S. Army Medical Center

MEDDAC
medical department activity

MEVA
mission essential or vulnerable area

MHE
materials handling equipment

MI
military intelligence

MILPO
military personnel office

MILSPEC
military specification

MILSTRIP
military standard requisitioning and issue procedures

MILVAN
military-owned demountable container

MIPR
military interdepartmental purchase request

MOS
military occupational specialty

MP
military police

MPA
military personnel, Army

MPI
Military Police Investigator

MSC
major subordinate command; Military Sealift Command

MSD
maximum stress diet

MSR
main supply route

MTOE/TDA
modified table of organization and equipment/table of distribution and allowances

MTMC
Military Traffic Management Command

MTX
Military Traffic Expediting Service

MUSAREC
major U.S. Army Reserve command

MWD
military working dog

NAF
non-appropriated fund

NATO
North Atlantic Treaty Organization

NBC
nuclear, biological, and chemical

NBS
National Bureau of Standards

NCDD
narcotics/contraband detector dog

NCEL
Naval Civil Engineering Laboratory

NCIC
National Crime Information Center

NCO
noncommissioned officer

NCOIC
noncommissioned officer in charge

NDA
National Defense Area

NDI
nondevelopmental item

NGR
National Guard regulation

NIS
Naval Investigative Service

NSN
national stock number

OACSI
Office of the Assistant Chief of Staff for Intelligence

OCE
Office of the Chief of Engineers

OCIE
organizational clothing and individual equipment

OCONUS
outside continental United States

OCPA
Office of the Chief of Public Affairs

ODCSLOG
Office of the Deputy Chief of Staff for Logistics

ODCSOPS
Office of the Deputy Chief of Staff for Operations

ODCSPER
Office of the Deputy Chief of Staff for Personnel

ODUSDP
Office of the Deputy Under Secretary of Defense for Policy

OJT
on-the-job training

OMA
Operation and Maintenance, Army

OMAR
Operation and Maintenance, Army Reserve

OPA
Other Procurement, Army

OPLAN
operation plan

OPM
Office of Personnel Management

OPSEC
operations security

OSD
Office of the Secretary of Defense

pam
pamphlet

PAO
public affairs officer

PAP
personnel assistance point

PARR
Program Analysis Resource Review

PCP
phencyclidine

PCS
permanent change of station

PDIP
Program Development Increment Package

PECIP
Productivity Enhancing Capitol Investment Program

PERSCOM
U.S. Total Army Personnel Command

PIF
productivity investment funding

PM
product manager; program manager; project manager; provost marshal

POC
point of contact

POD
port of debarkation

POE
port of embarkation

POL
petroleum, oils, and lubricants

POV
privately-owned vehicle

PPBES
Planning, Programming, Budgeting, and Execution System

PS
physical security

psi
pounds per square inch

PSC
physical security councils

PSE
physical security equipment

PSEAG
Physical Security Equipment Action Group

PSI
physical security inspector

PSS
Protective Security Service

PT
physical training

QPL
qualified products list

QRIP
Quick Return on Investment Program

RAM
reliability, availability, and maintainability

RAM-D
reliability, availability, maintainability, and durability

RC
Reserve component

RCS
reports control symbol

RDA
research, development, and acquisition

RDT&E
research, development, test, and evaluation

RDX
research department explosive

RESHIP
report of shipment

RF
radio frequency, response forces

RFP
request for proposal

ROC
required operational capability

ROTC
Reserve Officers' Training Corps

RSS
Rail Surveillance System

SCIF
sensitive compartmented information facilities

SECDEF
Secretary of Defense

SF
standard form

SFC
sergeant first class

SGA
standards of grade authorization

SJA
Staff Judge Advocate

SIR
serious incident report

SOFA
Status of Forces Agreement

SOP
standing operating procedure

SQT
skills qualification test

SRT
special reaction team

SSG
staff sergeant

SSN
social security number

SSS
Signature Security Service

SSSC
self-service supply center

TAADS
The Army Authorization Documents System

TAG
The Adjutant General

TASA
television audio support activity

TASC
training and audiovisual support center

TB
technical bulletin

TC
training circular

TCE
Technical Center of Expertise

TCP
traffic control point

TDA
tables of distribution and allowances

TDP
technical data package

TDY
temporary duty

THC
tetrahydrocannabinol

THREATCON
terrorist threat condition

TISA
Troop Issue Subsistence Activity

tl
truckload

TM
technical manual

TMDE
test, measurement, and diagnostic equipment

TMF
threat management force

TNT
trinitrotoluene

TOFC
trailer-on-flatcar

TOVEX
water gel (explosive)

TRADOC
U.S. Army Training and Doctrine Command

TSG
The Surgeon General

TSRWG
Tri-Service Requirements Working Group

TTS
technical training squadron

TTG
technical training group

TTW
technical training wing

UCMJ
Uniform Code of Military Justice

UL
Underwriter Laboratories

USACE
U.S. Army Corps of Engineering

USACIDC
United States Army Criminal Investigation Command

USAF
United States Air Force

USAISC
U.S. Army Information Systems Command

USAMPS
U.S. Army Military Police School

USAR
U.S. Army Reserve

USAREUR
U.S. Army, Europe, and Seventh Army

USC
United States Code

USMA
United States Military Academy

USS
United States standard

WSM-PSE
Weapons Systems Manager-Physical Security Equipment

WSN
weapon serial number

WTCA
Water Terminal Clearance Authority

Section II
Terms

Access (when pertaining to a restricted area or CCI)
Personnel movement within a restricted area that allows the chance for visual observation of, or physical proximity to, either classified or protected materiel. It is also the ability and opportunity to obtain detailed knowledge of CCI through uncontrolled physical possession. External viewing or escorted proximity to CCI does not constitute access.

Aggressor
Any person seeking to compromise an asset. Aggressor categories include criminals, terrorists and protestors.

Ammunition
A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame, for use in connection with defense or offense, including demolition. Excluded from this definition are devices charged with chemical agents defined in JCS Pub. 1 and nuclear or biological materiel. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition and caliber .22 ammunition are excluded.

Antiterrorism
Defensive measure used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by military forces.

Armed Guard Surveillance
A service that provides armed guards to maintain constant and specific surveillance of shipments for which the service is requested. “Armed” is defined as having a firearm and appropriate ammunition readily available for immediate use. (DOD 5100.76–M)

Arms
A weapon included in AR 190–11, appendix A, that will or is designated to expel a projectile or flame by the action of the explosive, and the frame or receiver of any such weapon.

Asset
Any resource requiring protection.

Aviation Facility
A department of the Army activity or area collocated with facilities for the takeoff and landing of aircraft. The facility has the mission of command and control of administrative, operational, training, and/or logistical support of Army aviation.

Badge
A security credential that is worn on the possessor's outer garment and validates (his or her) authority for access to a restricted area.

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 lockpoint from the lockbody will strengthen its connection. (DOD 5100.76–M)

Carrier Custodian
An employee who has been assigned responsibility for controlled shipments containing SECRET material by the carrier and who has been issued a personnel security clearance by the Government. (DOD 5100.76–M)

Certification
The process whereby a patrol or detector dog's and handler's proficiency is verified to be in compliance with minimum training standards.

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 low security 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 intrusion detection systems (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.

Closed post
An army installation or activity to which ground and water access is controlled at all times by perimeter barriers with limited, manned entry control points.

Closed vehicle or equipment
A conveyance that is fully enclosed with permanent sides and a permanent top, with installed doors that can be locked and sealed. (DOD 5100.76–M)

Combatting Terrorism
Actions, including AT and CT, taken to oppose terrorism throughout the entire threat spectrum.

Commercial-type vehicle
A vehicle designed to meet civilian requirements, and used without major modifications, for routine purposes in connection with the transportation of supplies, personnel, or equipment.

Constant Surveillance Service
A service that is an integral part of the provisions of 49 CFR 397 (reference (b)) that a carrier must apply when transporting hazardous or Class A and B explosive materials. It provides constant surveillance over a shipment. The transporting conveyance containing the shipment must be attended at all times by a qualified representative of the carrier. A motor vehicle is "attended" when the person in charge of the vehicle is awake and not in a sleeper berth and

is within 100 feet of the vehicle, provided the vehicle is within the person's obstructed field of vision. The qualified representative "attending" the vehicle must:

a. Be aware of the nature of the material contained in the vehicle.
b. Have been instructed on procedures to follow in case of emergency.
c. Be authorized to move the vehicle and have the means and capability to do so.

Note. CSS does not include a signature and tally service as provided under Signature Security Service (SSS). (DOD 5100.76–M)

Container Express
A reusable container for shipment of troop support cargo, quasi-military cargo, household goods, and personal baggage.

Containerization
A box or other device in which a number of packages are stored, protected, and handled as a unit in transit; for example, CONEX, MILVAN, and SEAVAN. This term also refers to the shipping system based on large cargo-carrying containers that can be easily interchanged between trucks, trains, and ships, without rehandling of contents. (DOD 5100.76–M)

Container on a flat car
A large box-like demountable body without undercarriage used to transport cargo that is mounted on a railroad flat car. (DOD 5100.76–M)

Constant Surveillance
Observing or protecting a storage facility containing AA&E by a human, intrusion detection system, closed circuit television, or combination, to prevent unobserved access, or make known any unauthorized access to the protected facility.

Continuous Surveillance
Constant unobstructed observance of items or an area to prevent unauthorized access. Continuous surveillance may be maintained by dedicated guards, other on-duty personnel, or intrusion detection systems and those enhanced by closed-circuit television.

Controlled Area
See restricted area.

Controlled cryptographic item
A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but is controlled.

Controlled medical substance
A drug or other substance, or its immediate precursor, listed in current schedules of 21 USC 812 in medical facilities for the purpose of military treatment, therapy, or research. Categories listed in this section are narcotics, amphetamines, barbiturates, and hallucinogens.

Counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism.

Crime analysis
The process used to determine the essential features of a criminal act. It is a mandatory part of any crime prevention program.

Crime prevention
The anticipation, recognition, and appraisal of a crime risk, and initiation of some action to remove or reduce it. Crime prevention is a direct crime control method that applies to before-the-fact efforts to reduce criminal opportunity, protect potential human victims, and prevent property loss.

Crime prevention inspection
An on-site evaluation of the crime prevention program of a unit, section, office, or other facility.

Crime risk management
The development of systematic approaches to reduce crime risks.

Crisis management team
A team found at a major command or installation level. A crisis management team is concerned with plan, procedures, techniques, policies, and controls for dealing with terrorism, special threats, or other major disruptions occurring on Government installations and facilities. A crisis management team considers all aspects of the incident and establishes contact with the AOC.

Critical communications facility
A communications facility that is essential to the continuity of operations of the National Command Authority during the initial phases of national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

Cryptographic component
The embodiment of a cryptographic logic in either hardware or firmware form, such as a modular assembly, a printed circuit board, a microcircuit, or any combination of these.

Cryptographic equipment
Any equipment employing a cryptographic logic.

Cryptographic logic
A deterministic logic by which information may be converted to an unintelligible form and reconverted to an intelligible form. Logic may take the form of engineering drawings, schematics, hardware, or firmware circuitry.

Day gate
Any barriers, used in a doorway or entrance to pharmacy or medically sensitive item storage areas, that prevents unauthorized personnel access during operating hours. Such barriers normally are not the sole protection afforded the entrance during nonoperating hours; however, during operating hours, the barrier ensures positive entry control by on-duty personnel (for example, electronic buzzer control entry to the area after positive identification by receptionist or on-duty personnel).

Dedicated guards
Individuals charged with performing the primary task of safeguarding designated facilities, material, and personnel within a defined area during a tour of duty. A dedicated guard may perform this function as a static post. He or she remains within or on the perimeter of a protected area and maintains continuous surveillance over that which is being protected during the tour of duty.

Defense Transportation System
Consists of military controlled terminal facilities, Military Airlift Command (MAC) controlled airlift, Military Sealift Command (MSC) controlled or arranged sealift, and Government controlled air or land transportation. (DOD 5100. 76–M)

Demilitarization
The act of destroying the offensive or defensive characteristics inherent in certain types of equipment and materiel. The term comprehends mutilation, scrapping, burning, or alteration designed so as to prevent the further use of such equipment and materiel for its originally intended military or lethal purpose.

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.

Dromedary
A freight box carried on and securely fastened to the chassis of the tractor or on a flat-bed trailer. The dromedary is demountable by the use of a forklift truck, is protected by a plymetal shield, and is equipped with doors on each side that may be locked with seals or padlocks. All explosive items carried in the dromedary must be compatible and in compliance with 49 CFR 177 (ref (c)) or host nation regulations. (DOD 5100.76–M)

Dual Driver Protective Service
A service requiring SSS plus continuous attendance and surveillance of the shipment through the use of two drivers.
a. The vehicle containing the shipment must be attended at all times by one of the drivers. A vehicle is attended

when at least one of the drivers is in the cab of the vehicle, awake, and not in a sleeper berth or is within 10 feet of the vehicle.

b. SSS signature and tally requirements are not required between the same pair of drivers for a particular movement. (DOD 5100.76–M)

Duress alarm system
A method by which authorized personnel can covertly communicate a situation of duress to a security control center or to other personnel in a position to notify a security control center. (DOD 5100.76–M)

Duress or holdup alarms
Devices which allow personnel on duty to transmit a signal to the alarm monitoring station from which an armed response force can be dispatched if a holdup or a duress situation occurs.

Emergency Aircraft
An aircraft designated by the commander to respond to emergency situations and provide life-saving and property-saving services. Normally, such aircraft has special equipment and markings. Air Ambulances and firefighting aircraft are examples.

Emergency vehicle
A vehicle designated by the commander to respond to emergency situations and provide life-saving and property-saving services. Normally, the vehicle has special equipment and markings. Ambulances and firefighting and military or security police vehicles are examples.

Enclosed vehicle or equipment
A conveyance that is fully enclosed with permanent sides and permanent top, with installed doors that can be locked and sealed.

Entry control (when pertaining to a restricted area)
Security actions, procedures, equipment, and techniques, employed within restricted areas to ensure that persons who are present in the areas at any time have authority and official reason for being there.

Escorted personnel (when pertaining to a restricted area)
Those persons authorized access to a restricted areas who are escorted at all times by a designated person.

Escorts and couriers
Military members, U.S. civilian employees, or DOD contractor employees responsible for the continuous surveillance and control over movements of classified material. Individuals designated as escorts and couriers must possess a Government-issued security clearance at least equal to that of the material being transported.

Exception
An approved permanent exclusion from specific requirements of this regulation. Exceptions will be based on a case-by-case determination and involve unique circumstances which make conformance to security standards impossible or highly impractical. An exception can also be an approved permanent deviation from the provisions of this regulation. There are two types of exceptions:

a. Compensatory Measures Exception. This is a deviation in which the standards are not being met, but the DOD component (HQDA(DAMO–ODL–S) concerned determines it is appropriate, because of physical factors and operational requirements. Compensatory measures are normally required.

b. Equivalent Protection Exception. This is a deviation in which nonstandard conditions exist, but the totality of protection afforded is equivalent to or better than that provided under standard criteria.

Exclusion area
See restricted area.

Exclusive use
A conveyance unit or vehicle that is used only for a shipment from origin to destination without transfer of lading, and that permits locking of the unit and use of seals. (DOD 5100.76–M)

Explosives
Any chemical compound, mixture or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives (dynamite,

trinitrotoluene (TNT), C–4, and other high explosives), and other explosives consisting of 10 pounds or more; for example, gunpowder or nitroguanidine.

Facility
Any single building, project, or site.

Force Protection
Security program developed to protect soldiers, civilian employees and family members, facilities and equipment, in all locations and situations. This is accomplished through the planned integration of combatting terrorism, physical security, operations security, protective services and law enforcement operations, all supported by foreign intelligence, counterintelligence and other security programs.

Greater security (GS)
A seal tracing and inspection rail service for unclassified sensitive cargo that includes a military traffic expending (MTX) service and provides:

a. Inspection of railcars at major terminals by railroad personnel for evidence of forced entry or tampering with seals or security devices.

b. Name of carrier reporting.

c. Time of inspection; that is, a.m. or p.m.

d. Actual arrival and actual departure time from inspection terminal. (DOD 5100.76–M)

Handler
A military police person or DOD civilian guard or police person who has been qualified by training and certification to care for, train, and employ a military working dog.

Handling
Controlled physical possession without access.

High risk personnel
Personnel who, by their grade, assignment, value, location, or specific threat, are more likely to be attractive or accessible terrorist targets.

Independent power source
A power source, normally battery, independent of any other source (DOD 5100.76–M)

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.

In flight
The condition of an aircraft from the moment when all external doors are closed following embarkation until the moment when one such door is opened for disembarkation.

Installations
Such real properties as reserve centers, depots, arsenals, ammunition plants (both contractor- and Government-operated, hospitals, terminals, and other special mission facilities, as well as those used primarily by troops. (See also JCS Pub. 1)

Internal controls (when pertaining to a restricted area)
Security actions, procedures, and techniques employed within restricted areas to ensure persons who are present in these areas at any time have authority and official reason.

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. The IDS will be an approved DOD standardized system, such as the Joint Service Interior Intrusion Detection System or MACOM-approved commercial equipment.

Justification for Major System New Start
A requirement document that the combat developer prepares with the material developer, training developer, manpower

and personnel planner, and logistician. A JMSNS is prepared to describe the mission need and justifies the acquisition of a major new system at program initiation in the acquisition cycle.

Kennel facilities

The buildings, the kennels, the runs, and the exercise and training areas which are used to house, care for, and train military working dogs.

Key and lock control system

A system of identifying both locks and their locations and personnel in possession of keys and/or combinations.

Keying

The process of establishing a sequence of random binary digits used to initially set up and periodically change permutations in cryptographic equipment for purpose of encrypting or decrypting electronic signals, for controlling transmission security processes, or for producing other keys.

King Tut block

A King Tut block is a specially designed large concrete block. It is placed in front of an igloo or magazine entrance with a fork lift. Access to the igloo or magazine therefore requires a fork lift to move the block. The King Tut block is of sufficient weight to prevent removal without a fork lift.

Letter of agreement

A document jointly prepared and signed by the combat and materiel developers when a potential materiel system need has been identified and it has been determined that one or more technological approaches may satisfy the need. Even though it may be in an early stage of development, the LOA will address the materiel system from the Total System Management standpoint. The LOA describes operational, technical, training, personnel, and logistical system unique events that must be undertaken to produce the total system.

Letter requirement

An abbreviated procedure for acquisition of low-unit cost, low-risk developmental, or commercial items. It will be used instead of the ROC when applicable. The total system definitive requirements for training, personnel, and logistics requirements are the same for the LR as for the ROC. The LR is jointly prepared by TRADOC and AMC.

Lightweight construction

Building construction other than reinforced concrete or masonry (concrete block or clay brick) such as wood or metal siding.

Limited access post

An Army installation or activity that meets one of the criteria below:

a. No permanent fences or other physical barriers exist, but entry can be temporarily closed to vehicular traffic and other movements using roads and other conventional points of entry.

b. Permanent perimeter barriers exist and access is controlled only after normal duty hours; for example, gates are secured or manned with guards after dark.

c. No permanent perimeter barriers exist, but vehicular traffic and other movements using roads and other conventional points of entry are continuously controlled.

Limited area

See restricted area.

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.

Locking devices

a. Padlocks, military specifications MIL–P–43607 (High Security Padlock); shrouded shackle, NSN

5340–01–217–5068 or horizontal sliding bolt, NSN 5340–00–799–8248) or MIL–P–43951 (medium security padlock; regular shackle, NSN 5340–00–799–8016).

b. Padlocks, Commercial Item Description A–A–1927 (low security padlock) having a hardened steel shackle and body; NSN 5340–00–158–3807 (with chain), NSN 5340–00–158–3805 (without chain).

c. GSA-approved changeable three-position padlock, Federal Specification FF–P–110.

d. High security hasps. Military Specifications MIL–H–43905 or MIL–H–29181A.

e. Hasps and staples for low-security padlocks which are of heavy pattern steel, securely fastened to the structure with smooth-headed bolts, rivets, or welding to prevent removal.

Locks

Locks should be considered as delay devices only, not as positive bars to unauthorized entry, since any lock can be defeated by expert manipulation or force.

a. Padlocks

High security padlocks: Military Specification MIL–P–43607, shrouded shackle with clevis and chain, NSN 5340–01–217–5068 or NSN 5340–00–188–1560; horizontal sliding bolt with clevis and chain, NSN 5340–00–799–8248.

Medium security padlocks: Military Specification MIL–P–43951, open shackle with clevis and chain, NSN 5340–00–799–8016. Authorized for continued use to secure Categories III and IV AA&E only until stocks are depleted or replaced.

Low security padlocks: Commercial Item Description A–A–1927, hardened steel shackle and case, without chain: NSN 5340–00–158–3805; with chain: NSN 5340–00–158–3807.

(Any questions regarding the above specifications will be addressed to the DOD Lock Program Technical Manager, Naval Facilities Engineering Service Center, Code C66, 560 Center Drive, Port Hueneme, CA 93043–4328 (DSN 551–1567 or –1212).

b. Certain locks, such as high or medium security padlocks, provide excellent protection when used in conjunction with a high security hasp. Hasps installed for protection of AA&E will provide protection comparable to that given by the lock used. Determination of "comparable protection" will be addressed to the DOD Lock Program Technical Manager, Naval Civil Engineering Laboratory, Code L56, 560 Center Drive, Port Hueneme, CA 93043–4328 (DSN 551–1567 or –1212).

NAPEC high security shrouded hasp (MIL–H–29181A) is approved for use with the high security padlock to secure all categories of AA&E. The hasp has a cover that protects the lock from cutting or hammer tools and inclement weather. It should be used to secure Category I and II AA&E storage facilities. When replacement of a hasp on Category III, IV or uncategorized AA&E is necessary, this hasp should also be used. The Natick high security hasp (MIL–H–43905) is a high security hasp that also is approved for protection of Category III and IV AA&E when used with an approved high security padlock.

Hasp, pin-type, locking "T" is a hasp that was authorized previously to secure ammunition storage magazines. Magazines were secured using the installed locking bar in conjunction with a "T" pin and high security padlock. The locking "T" hasp does not provide adequate security for sensitive AA&E. It must be replaced with a high security hasp to enhance security. It will not be used to secure Category I and II ammunition storage facilities.

c. Another lock is the cable seal lock. Once locked, any force exerted to separate the lockpoint from the lockbody strengthens the connection. Such locks are not approved for use in securing storage facilities containing AA&E. The same restriction applies to d below.

d. A complementary device to locks is the No. 5 American Wire Gauge wire twist. This is a U-shaped wire place in the hasp along with the shackle and twisted tightly in place. Another device is a wire cable of a thickness equivalent to or larger than No. 5 wire. This is placed through the hasp, a metal sleeve slipped over it, and crimped into place.

e. Built-in combination locks, meeting Underwriters Laboratories Standard 768, Group 1 (NSN 5340–01–375–7593) are approved for use on GSA-approved Class 5 vault doors and GSA-approved Class 5 weapons containers storing unclassified material and unclassified AA&E.

LOGAIR

Long-term contract airlift service within the continental United States for the movement of cargo in support of the logistics system of the Military Services (primarily the Army and Air Force) and Defense Agencies. (DOD 5100.76–M)

Major disruption on installations

Acts. Threats, or attempts to commit such acts as kidnapping, extortion, bombings, hijackings, ambushing, major weapons thefts, arson, assassination, and hostage taking on a military installation. These acts that have potential for widespread publicity require special response, tactics, and management.

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 and/or misuse such as needles and syringes.

Military Traffic Expediting (MTX) Service
A service providing for movement from origin to destination in the shortest time possible for specifically identified rail shipments, and which is required for the shipment of firearms and other sensitive shipments. This service uses electrical communications between members of the Association of American Railroads, is available for either single line haul or jointline movements, and provides progress reports as required. (DOD 5100.76–M)

Military van (MILVAN)
Military-owned demountable container, conforming to U.S. and international standards, operated in a centrally controlled fleet for movement of military cargo. (DOD 5100.76–M)

Military working dog
Dogs required by the using DOD component for a specific purpose, mission, or combat capability. MWDs include patrol, patrol and narcotic/contraband, and patrol and explosive detector dogs.

Military working dog team
The MWD and its appropriately qualified, assigned handler.

Mission-critical personnel
Personnel who are essential to the operation of an organization of function.

Mission essential and vulnerable areas
Facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful accomplishment of the installation's State National Guard, or MUSARC mission. This includes areas nonessential to the installation's/facility's operational mission but which, by nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.

Motor pool
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 nontenant Army activity with 10 or less assigned commercial-type vehicles but no local organizational maintenance support does not have a motor pool, under this regulation, even though the vehicles are parked together.

Motor vehicle
A self-propelled, boosted, or towed conveyance used to transport a burden on land. This includes all Army wheeled and track vehicles, trailers, and semitrailers, but not railroad locomotives and rolling stock.

National Defense Area
An area set up on non-Federal lands located within the United States, its possessions or territories, to safeguard classified defense information or DOD equipment or materiel. Establishment of a National Defense Area temporarily places such non-Federal lands under the effective control of DOD and results only from an emergency event.

Negotiations
A dialogue between authorities and offenders which has as the ultimate goal for the safe release of hostages and the surrender of the offenders.

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, 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.

One dog-one handler
The concept that each MWD will have only one handler. Personnel shortages may necessitate assigning a handler responsibility for more than one dog. However, two or more handlers cannot handle the same dog.

Open post
Installations or activities that do not qualify as closed or limited access posts. Access to the installation or activity is not controlled during or after normal duty hours.

Perimeter fence
Fences for the security of unclassified, non-sensitive items that meet the requirements of U.S. Army Corps of Engineers Drawing Code 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 protective 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
That part of the Army security system, based on threat analysis, concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, materiel, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft. Operations security (OPSEC) and security targeted against traditional criminal activity are included.

a. Physical security procedures 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 procedures and measures during the exercise of these plans; the interface of installation OPSEC, 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 procedures employed to protect security interests from possible threats and include, but are not limited to, security guards; military working dogs; lights and physical barriers; explosives and bomb detection equipment; protective vests and similar equipment; badging systems; electronic entry control systems and access control devices; security containers; locking devices; electronic intrusion detection systems; standardized command, control, and display subsystems; radio frequency data links used for physical security; security lighting; delay devices; artificial intelligence (robotics); and assessment and/or surveillance systems to include closed-circuit television. Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans.

Physical security 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.

c. Intrusion detection system. See previous definition.

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

Physical security measures
See physical security.

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 combatting terrorism committees and fusion cells; and a continuing assessment of the installation's physical security posture.

Physical security resource plan
Plan developed by the physical security officer that identifies physical security needs, and shows proposed programmed procurement of those needs.

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

Physical security system architecture
A system ensuring that IDS components designed by the various services are compatible when used together. The Air Force is responsible for systems architecture.

Pier service
Ocean carrier booking is restricted over ocean movement from port of embarkation (POE) to port of debarkation (POD). It precludes prearranged-through-booking employing surface transportation to inland destinations. (DOD 5100. 76–M)

Pilferable assets
Any asset which can be stolen and which does not fall under the other asset 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 (45.34 kilograms) is considered portable.

Primary electrical power source
That source of power, either external (commercial) or internal, that provides power to site facilities on a daily basis. (DOD 5100.76–M)

Protection in depth
A system providing several supplementary security barriers. For example, a perimeter fence, a secure building, a vault, and a locked container provide four layers of protection. (DOD 5100.76–M)

Protective layer
Any envelope of building components which surrounds an asset and delays or prevents aggressor movement toward the asset or which shields the asset from weapons and explosives effects.

Protective Security Service
A service to protect shipments. PSS involves a transporting carrier that must be a "cleared carrier" under provisions of DOD 5220.22–R, paragraph 1–702.a (ref (d)). A shipment must be under the constant surveillance of designated carrier employees, unless it is stored in containers or an area approved by the cognizant Defense Investigative Service regional

office. The designated carrier employees providing constant surveillance when PSS is required must possess a Government-issued SECRET clearance and a carrier-issued identification. (DOD 5100.76–M)

QUICKTRANS
Long-term contract airlift service within the continental United States (CONUS) for the movement of cargo in support of the logistic system for the Military Services (primarily the Navy and Marine Corps) and Defense agencies. (DOD 5100.76–M)

Rail Surveillance Service
An inspection service of rail shipments. An inspection is made within one hour after each stop, if the trailer containing a shipment remains at a halt. Reinspection is made a minimum of once each hour, as long as the railcar containing the shipment remains at a halt. (DOD 5100.76–M)

Report of Shipment
An advanced report furnished by message or telephone immediately upon dispatch of a shipment within CONUS for domestic shipments. A report goes to both Water Terminal Clearance Authority (WTCA) and the water port transshipping facility for surface export shipments, or to the Military Air Traffic Coordinating Officer (MATCO) for air export shipments. The advance notice of shipments shall include the following applicable data:

a. For domestic shipments, see AR 55–355/NAVSUPINST 4600.70/AFM 75–2/MCO P4600.14A/DLAR 4500.3, Routing Instruction Note (RIN) 146, Appendix L (reference (e)).

b. For export shipments, see chapter 4, DOD 4500.32–R (reference (f)). (DOD 5100.76–M)

Required operational capability
A requirements document that the combat developer prepares with input from the training developer in coordination with the material developer, logistician, and manpower and personnel planner. The ROC is a concise statement of the minimum essential operational, RAM, technical, personnel and manpower, training, safety, health, human factors engineering, logistical, and cost information to start full scale development or procurement of a material system.

Restricted area
Any area to which entry is subject to special restrictions or control for security reasons or to safeguard property or material. This does not include those designated areas over which aircraft flight is restricted. Restricted areas may be of different types. The type depends on the nature and varying degree of importance, from a security standpoint, of the security interest or other matter contained therein.

a. Exclusion area. A restricted area containing—

(1) A security interest or other matter of such nature that access to the area constitutes, for all practical purposes, access to such security interests or matter; or—

(2) A security interest or other matter of such vital importance that proximity resulting from access to the area is treated equal to (1) above.

b. Limited area. A restricted area containing a security interest or other matter, in which uncontrolled movement will permit access to such security interest or matter; access within limited areas may be prevented by escort and other internal restrictions and controls.

c. Controlled area. That portion of a restricted area usually near or surrounding an exclusion or limited area. Entry to the controlled area is restricted to authorized personnel. However, movement of authorized personnel within this area is not necessarily controlled. Mere entry to the area does not provide access to the security interest or other matter within the exclusion or limited area. The controlled area is provided for administrative control, safety, or as a buffer zone for security in depth for the exclusion or limited area. The proper commander establishes the degree of control of movement.

Ride awhile-walk awhile method
A law enforcement or security patrolling technique. The MWD team patrols for a period of time in a vehicle and then dismounts for an appropriate period of time to patrol an area on foot. This method increases the potential area the team can cover, as well as allowing the team to concentrate their foot patrols in especially critical areas.

Risk
The degree or likelihood of loss of an asset. Factors that determine risk are the value of the asset to its user in terms of mission criticality, replaceability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the asset to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the asset.

Risk analysis
Method of examining various risk factors to determine the risk value of likelihood of resource loss. This analysis will be used to decide the level of security warranted for protection of resources.

Risk factors
Elements that make up the total degree of resource loss liability. Factors to be considered in a risk analysis include the importance of the resource to mission accomplishment; the cost, volume, criticality and vulnerabilities of the resources; and the severity of threats to the resources.

Risk level
An indication of the degree of risk associated with an asset 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.

Safe
A GSA Class 5 Map and Plans Security Container, Class 6 Security Filing Cabinet or refrigerator or freezer, secured with an approved locking device and weighing 500 pounds or more, or secured to the structure to prevent removal.

Schedule I drug
Any drug or substance by whatever official name (common, usual, or brand name) listed by the DEA in Title 21 of the Code of Federal Regulations, chapter II, Section 308.11, intended for clinical or non-clinical use. A list of Schedule I drugs and substances is contained in AR 40-7, appendix A.

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 shall be shown on Government Bills of Lading (GBL). A cable seal lock provides both a seal and locking device.

Sealed containers
Wooden boxes, crates, metal containers, and fiber containers sealed in a way to show when the containers are tampered with after sealing. The method of sealing depends of the type of construction of the containers. Sealing may be by metal banding, nailing, airtight sealing, or wax dripping (for fiber containers). In key control, a sealed container is also a locked key container or a sealed envelope containing the key or combination to the key container.

Sealed protection
A container or an area enclosed by a plastic or soft metal device which is opened easily without the use of a key or combination.

SEAVAN
A commercial, Government-owned or leased shipping container and without bogey wheels attached that is moved by ocean transportation and must be lifted on and off the ship. (DOD 5100.76–M)

Security card
An official distinctive identification (pass or card) that identifies and authorizes the possessor to be physically present in a U.S. Army designated restricted area.

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

Security lighting
The amount of lighting necessary to permit visual surveillance by security police or by supervisory personnel.

Security procedural measures
Physical security measures to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. The procedures can usually be changed within a short amount of time and involve manpower.

Sensitive conventional arms, ammunition, and explosives
See categorization of such items in appendix A, AR 190–11.

Sensitive items
Material requiring a high degree of protection to prevent unauthorized acquisition. This includes arms, ammunition, explosives, drugs, precious metals, or other substances determined by the Administrator, Drug Enforcement Administration to be designated Schedule Symbol II, III, IV, or V under the Controlled Substance Act of 1970.

Signal intelligence
Intelligence derived from communications means (such as telephone, telegraph, radio), electronic signal emitters (such as navigation radar, identification friend or foe, and weapons guidance devices) and instrumentation signals (such as telemetry and beaconry).

Signature Security Service
A service designed to provide continuous responsibility for the custody of shipments in transit. A signature and tally record is required from each person responsible for the proper handling of the shipment at specified stages of its transit from origin to destination.

a. The initial signature on the signature and tally record should be the same as that of the carrier's agent on the GBL. When SSS is used in conjunction with DDPS, both drivers in each pair of drivers shall sign the signature and tally record when that pair assumes responsibility for the shipment.

b. Commercial carriers offering SSS must be able to trace a shipment in less than 24 hours. The following forms shall be used to obtain SSS:

(1) *Surface shipments.* DD Form 1907 (Signature and Tally Record) shall accompany every surface shipment of classified or protected material accorded a signature and tally service by surface commercial carriers. Carrier tariffs and tenders may describe this type of service under different titles for example, Hand-to-Hand Signature Service or Signature Service.

(2) *Commercial air shipments.* The air industry internal Form AC–10 (Airlines Signature Service Record) shall be used by regulated and nonscheduled airlines to obtain the signature and tally record. Air taxi operators and air freight forwarders providing SSS may use DD Form 1907 instead of AC–10. No receipt is required from the flight crew or attendants while the aircraft is in flight. A signature and tally record is required; however, from air carrier personnel whenever the aircraft is on the ground and access to the cargo compartment containing the sensitive arms, ammunition, and explosives (AA&E) is available for any purpose. A signature and tally record is also required from pickup and delivery carriers used by the airlines for such purposes.

(3) *Military air shipments.* The AF Form 127 (Traffic Transfer Receipt) or similar document, will be used to provide hand-to-hand receipt control for sensitive and classified shipments being transferred in the DTS. (DOD 5100. 76–M)

Steel bar
A flat bar, 3/8 inch by one inch minimum; or round bar 1/2 inch diameter minimum.

Steel mesh
High carbon, manganese steel not less than 15/100 inch (8-gauge) in thickness, and a grid of not more than two inches center to center.

Storage
Any area where AA&E are kept. Storage does not include items in process of manufacture, in use, or being transported to a place of storage or use.

Survivability
The ability to withstand or repel an attack, or other hostile action, to the extent that essential functions can continue or be resumed after the hostile action.

Tactics
The specific methods of achieving the aggressor's goals to injure personnel, destroy Army assets, or steal Army materiel.

Tactical vehicle
A vehicle with military characteristics designed primarily for use by forces in the field in direct connection with, or support of, combat or tactical operations, or the training of troops for such operations.

Tenant activity
A unit or activity of one Government agency, military department, or command that occupies facilities on an installation of another military department or command and that receives supplies or other support services from that installation.

Terrorism
The calculated use of violence or the threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals, that are generally political, religious, or ideological.

Terrorism counteraction measures
Term used previously for combatting terrorism (see definition of this term).

Terrorist group
A politically, religious, or ideologically oriented group which uses terrorism as its prime mode of operations.

Threat management force
An action force from the installation that responds to major disruptions on installations. The TMF should be of sufficient size to manage the disruption and will usually involve a command element, security element, negotiation team, SRT, and logistical element.

TOW
A tube-launched, optically traced, wire-command missile designed as an antitank weapon system. (DOD 5100.76–M)

Upper rail loc
A set screw operated variation of a "C" clamp designed for gripping the upper sliding rail which supports or guides the weight of some styles of railroad boxcar doors. Gripping the upper sliding rail, the "loc" blocks and prevents the door's roller hangers or carriers from sliding past, thereby effectively preventing the door from being moved. (DOD 5100. 76–M)

Waiver
Temporary relief from specific standards imposed by this manual (regulation) pending actions accomplishment of actions that will conform to the standards required. Compensatory measures are required.

Section III
Special Abbreviations and Terms
There are no entries in this section.

Index

This index is organized alphabetically by topic and by subtopic within topic. Topics and subtopics are identified by paragraph number.