

CHAPTER 2 – SECURITY **AND FORCE PROTECTION**

GENERAL. The purpose of this instruction is to establish policy; assign responsibility and accountability for the implementation of minimum mandatory physical security standards for the physical protection of personnel, facilities, operations for DRMS Field Activities worldwide.

a. Compliance with the provisions set forth herein is mandatory. The terms "shall" "will" and "must" are mandatory terms and any deviation from the standards, specifications, or requirements set forth in this chapter will be accompanied by an appropriate request for waiver or exception as required. The terms "should" and "may" are discretionary in scope and may reflect the best judgment of the responsible or accountable official.

b. Promulgation of this chapter is in accordance with and incorporates provisions of DOD Directive 5200.8, Security of DOD Installations and Resources; DOD **Directive** 2000.12, DOD **Antiterrorism/Force Protection (AT/FP) Program**; DOD 2000.12-H, **DoD Antiterrorism Handbook**; DOD Instruction 2000.16, DOD **Antiterrorism Standards**; applicable DLA Combating Terrorism directives, and DLAI 5710.1, DLA Physical Security Program. It applies to all DRMS Field Activities and assigned employees and supersedes DRMS-I 4160-14, Volume I, **Chapter 2**, updated **October 2001**. In case of conflicts with this chapter and higher headquarters (JCS/DoD/DLA) security policy, the higher headquarters policy will apply. In case of conflicts between this chapter and military service policy, notify the DRMS Command Security Office for assistance in resolution.

c. DLAI 5710.1 is the guiding directive for physical security at DLA Field Activities. DRMS field activities will comply with the applicable requirements of that instruction. This chapter is intended to support the requirements outlined in that instruction wherever possible. This chapter serves as the DRMS field activity's basic physical security plan as outlined in DLAI 5710.1, Paragraph E2c. DRMS Field Activities may supplement this directive as needed.

A. DEFINITIONS

1. Antiterrorism (AT): Force protection (FP) defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.
2. Clear Zone: An area on both sides of a perimeter barrier that provides an unobstructed view of the barrier and the ground adjacent to it.
3. Compensatory Measure: An alternate physical security measure employed to provide a degree of security equivalent to that provided by a required physical security measure. See also Waiver and Exception.
4. Controlled Area: A security area that contains information, matter, or materiel, which, while not vital to national security, requires special security measures to protect it from theft or damage because of its high value, vulnerability to pilferage or because of regulatory requirements.
5. Exception: Permanent relief from specific standards imposed within this instruction, based upon an individual determination that unique circumstances at a given activity are such that conformance to established standards is impossible, highly impractical, unnecessary due to measures exceeding those prescribed, or otherwise not in the best interest of the U.S. Government.
6. Exclusive Standoff Zone: A controlled area surrounding a facility into which only service and delivery vehicles operated by handicapped people are allowed. The perimeter of this area is defined by perimeter barriers and is set at a standoff distance sufficient to reduce the blast effects of a vehicle bomb detonation on the protected facility.
7. Force Protection (FP): Security program designed to protect military personnel, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and

DRMS-I 4160.14, Volume I, Chapter 2

integrated application of combating terrorism physical security, operations security, personal protective services, and support by intelligence, counterintelligence, and other security programs.

8. Host Security: Host installation agency having primary responsibility for physical security and law enforcement on the installation.

9. Key Custodian: The person designated to manage a key repository within the Key and Lock Control Program.

10. Restricted Area: A security area under DoD control into which persons may not enter without specific authorization. The area contains information, matter or materiel vital to national defense requiring special security measures to protect the resources contained therein from sabotage, espionage, or theft.

11. Official Visitor: Any DLA/DRMS command or staff member, Federal investigator, or DoD inspector on official business at the DRMS field activity.

12. Physical Barrier: Natural or man made obstruction to deter accidental or deliberate intrusion.

13. Physical Security: That portion of security concerned with the employment of physical measures such as barriers, protective lighting, and vehicle and personnel control measures. It also includes other functions such as loss prevention, security awareness training, and operational procedures designed to limit vulnerabilities.

14. Pilferable Item: Property in DRMS field activity custody which by virtue of its condition, intrinsic value, ready illicit market or resale potential, or widespread non-DoD usage, is highly desirable and therefore a primary target for theft.

15. Sensitive Item: Property requiring a high degree of protection and control due to statutory or regulatory requirements, such as drug abuse items; stock numbered precious metals, hazardous property; items which are of high value and small arms parts.

16. Small Arms: Category of weapons defined in DoD 5100.76-M, that have potential use in civil disturbances and are vulnerable to theft. Small arms are handguns, shoulder-fired weapons, light automatic weapons up to and including .50 caliber machine guns, recoilless rifles up to and including 106mm, mortars up to and including 81mm, man-portable rocket launchers, rifle and shoulder fired grenade launchers, and individually operated weapons which are portable and/or can be fired without special mounts or firing devices.

17. Standoff Distance: A distance maintained between a facility and the potential location for explosives detonation to reduce the explosives' blast effects on the facility. Standoff distances vary with building component construction. See also the definition for "Unobstructed Space".

18. Unobstructed Space: Space within 10 meters (33 feet) of and inhabited building that does not allow for concealment from observation of explosive devices 150mm (6 inches) or greater in height,

19. Visitor: Any individual, military or civilian, not assigned to or employed within an installation, activity, or area to which access is requested.

20. Vulnerability Assessment: An analysis of the compound probability of being hit by a terrorist attack and whether or not assigned responsibilities can be fulfilled as required if attacked. (One step in the preparation of an activity Terrorist Threat Estimate.)

21. Waiver: Temporary relief from specific standards imposed by this instruction pending accomplishment of actions or programs that will conform to established standards.

B. RESPONSIBILITIES

1. Commander, DRMS:

- a. Has command responsibility for the safety of personnel and protection of Federal property under his/her control.
- b. Has overall responsibility for implementing DoD Combating Terrorism programs at all DRMS activities worldwide. Ensures compliance by subordinate activities with applicable physical security directives.
- c. Assumes all risks involved with disapproval of all recommendations identified during Antiterrorism Vulnerability Assessments.
- d. Is responsible for the implementation of physical security measures designed to minimize the loss of supplies and equipment by natural or manmade hazards.
- e. Ensures that the functional organization of the activity includes a Command Security Officer and that the organizational placement of the Command Security Officer does not hinder accomplishments of the security mission.
- f. Implements the DOD/DLA Combating Terrorism Program as outlined in DoDD 2000.12 at all CONUS and OCONUS subordinate activities.
- g. Appoints an Antiterrorism/Force Protection Officer who meets the qualifications outlined in DLA Combating Terrorism directives and ensure that the AT/FP Officer has the tools, resources, and training necessary to successfully implement the DLA Combating Terrorism Program as outlined in this document.
- h. Ensures that all personnel under his/her control receive required Antiterrorism Awareness Training and Travel Briefings.
- i. Ensures that all personnel under his/her control who are duty-stationed OCONUS are provided adequate workplace and residential security that addresses the terrorist threat, in accordance with CINC standards.
- j. Ensures that funding or FTE shortfalls for DRMS and DRMS field activities are appropriately addressed at the HQ, and if necessary, forwarded to HQ DLA.
- k. Ensures that all disputes with facility hosts, the General Services Administration, the Chief of Mission, or the CINC, or other entities, regarding protection from terrorism for DRMS/DRMS field activity personnel, are appropriately addressed at the HQ level and, if necessary, forwarded to HQ DLA for resolution.

2. Director, Command Security:

- a. Functions as the technical subject matter expert and principal advisor to the Commander on all matters pertaining to physical security, antiterrorism, and force protection (AT/FP) issues.
- b. Provides oversight and management of the overall command security program; to include physical security, information security, personnel security, and [other duties as required].
- c. Conducts periodic reviews and inspections of DRMS field activities to ensure compliance with applicable regulations, directives, and instructions.
- d. Identifies shortfalls in the AT/FP program. Monitors budgetary needs to ensure compliance with applicable physical security and AT/FP goals. Submits and revises operating budget as needs arise.
- e. Serves as Command Security Representative on various boards and committees.
- f. Implements the DLA Loss Prevention Program.
- g. Provides security education and training material to DRMS field activities. Develops training modules for usage in security education program.

DRMS-I 4160.14, Volume I, Chapter 2

- h. Provides analysis of DRMS security deficiencies and recommendations.
- i. Formulates and administers command security education and training programs for all DRMS employees.
- j. Reviews all portions of this instruction at least annually.

3. AT/FP Officer:

- a. Implements the DOD/DLA Combating Terrorism Program at HQ DRMS and DRMS field activities as outlined in applicable Combating Terrorism directives.
- b. Provides oversight in the implementation of approved antiterrorism measures at HQ DRMS and DRMS field activities to include, where applicable, negotiation with facility hosts, the General Services Administration, or Chief of Mission to implement recommended Antiterrorism measures.
- c. Conducts Vulnerability Assessments at all DRMS field activities. Where responsibility for vulnerability assessments is assigned to another headquarters, will accompany the assigned assessment team and upon completion will provide oversight of and coordinate corrective action through close contact with the respective Forward Support Teams and facility heads.

4. DRMS Field Activity Leaders:

- a. Take responsibility for implementing security measures designed to minimize loss of supplies, equipment and material and to eliminate fraud, waste and mismanagement within their facilities.
- b. Ensure compliance with this chapter within their facilities.
- c. Ensure that individual employees safeguard government property in their charge and comply with the provisions of this chapter.
- d. Have responsibility for the safety of employees and protection of Federal property, to include subordinate operating locations.
- e. Execute the DLA Loss Prevention Program
- f. Ensure security requirements are identified in the activity budget.
- g. Implement physical security measures designed to minimize the loss of supplies and equipment by natural or manmade hazards.
- h. Act as incumbent or appoints a Security Coordinator (in writing).
- i. Provide the DRMS Command Security Office immediate notification of any terrorist incident discovered within or reported to the DRMS field activity.
- j. Ensure that the DRMS field activity is integrated into host security, antiterrorism and emergency reaction plans.
- k. Submit a DRMS situation report (SITREP) and an email “Security Notification” when host or other investigative agencies initiate security or criminal incidents, criminal investigations, security surveys involving the DRMS field activity *or any requests for information by any law enforcement agency. The “Security Notification” email address can be located in the Outlook Global Address List.***
- l. Be knowledgeable of installation resources and procedures as they relate to Workplace Violence issues. This will include procedures to respond to incidents or situations which fall short of criminal acts (i.e. assault, etc.).**

m. Maintain installation plans for antiterrorism, force protection, and emergency response/disaster preparedness. Be knowledgeable of DRMO taskings outlined in these plans.

n. At sites where a logistics contractor is present, any inspection or findings resulting from the inspection or corrective action required by the contractor will be forwarded to the contractor through the COTR.

5. DRMS Field Activity Security Coordinators:

a. Administer the activity's physical security program, in accordance with this chapter, and other appropriate security directives. Reports directly to DRMS field activity Chief for all security/antiterrorism matters.

b. Assist the DRMS field activity Chief in discharging their security responsibilities by analyzing security deficiencies and hazards and making recommendations for appropriate corrective action.

c. Maintain and supplement (as necessary) host physical security, antiterrorism and emergency plans. When the DRMS field activity is a not a tenant facility on a DoD installation and has no interservice support agreement for police services or force protection, the security coordinator will develop appropriate security and antiterrorism plans. Contact the DRMS Command Security Office for assistance as needed.

d. Develop and maintain a security file composed of copies of all documents of security interest to the DRMS field activity. Maintain the security file as an individual information file or incorporated into an existing DRMS field activity file system. It is recommended that a single file or binder be maintained. As a minimum, the security file must contain the following:

- Most recent physical security assessments conducted by DRMS Command Security Office and host security agency, with report of corrective actions.
- Approved **security** waivers and exceptions.
- Security coordinator and key control officer and other Security related appointment, as applicable.
- Host security/antiterrorism plan, supplemented as necessary.

NOTE: If host plans have been classified (Top Secret/Secret/Confidential), then maintain only appropriate unclassified portions or versions of the plans. The DRMS Field Activity only requires those portions of host plans that outline DRMS Field Activity taskings when the plan is implemented.

- Host emergency response/**disaster preparedness/consequence management** plan, supplemented as necessary.
- Training documentation and material.
- Documentation of emergency and security exercises.
- Miscellaneous other security correspondence.

e. Provide and document initial security indoctrination for all employees at the time of their assignment or employment and periodic security training more directly related to individual duties, at intervals not to exceed 1 year. Maintain a training folder reflecting dates of training, subject matter, and employees attending. Contact the host security office or DRMS Command Security Office for assistance.

DRMS-I 4160.14, Volume I, Chapter 2

f. Participate in, and communicate security-related information and concerns during DRMS field activity staff meetings.

g. Disseminate crime prevention information and encourage active participation by all DRMS field activity employees in observing and reporting criminal activities, and security deficiencies.

C. ADMINISTRATION

1. Exceptions and Waivers.

a. Although a positive effort is made to achieve the security standards established by this directive and DLAI 5710.1, unusual conditions or circumstances may exist at a DRMS field activity, which necessitate deviation from these requirements. Compliance with a particular requirement may be impractical considering such factors as host mission and resources available to the activity. **Requests for exceptions and waivers are to be submitted by the activity to DRMS-BA, which will in turn forward the request to the Command Security Office for evaluation. Refer to DRMS Instruction 4160.14, Volume I, Chapter 1, Paragraph A3 pertaining to requesting waivers and exceptions. Send requests to Waivers@mail.drms.dla.mil. Waivers and exceptions to security criteria that fall under the purview of DLA Instruction 5710.1, Physical Security Program, will be elevated to the DLA Command Security Office for evaluation and approval.** Both exception authority (permanent deviation) and waiver authority (specified period not to exceed 1 year) may be granted. DRMS field activities may request renewal of an approved waiver when justifying circumstances exist. An approved waiver may be renewed; the request, with justification for renewal, must be submitted to arrive at **DRMS-BA** not later than 90 days prior to expiration of the existing waiver.

2. Loss Prevention Program

a. General. This program provides for the protection of Government property from loss, theft, and damage. Elements of the Loss Prevention Program are prevention of losses through physical protection measures and education of employees and investigations of losses to identify criminal activity and recover material. DRMS field activity leaders will participate in host installation loss prevention and crime prevention programs. Leaders will also strive to identify and minimize crime-conducive conditions at their respective field agencies.

b. Functions. Required functions of the Loss Prevention Program are:

(1) Ensuring that vulnerable material is adequately protected and proper controls are in place and enforced to prevent losses.

(2) Collection of data lost. This information may be received from several sources but at a minimum will include reports of suspected theft or damage, and DD Forms 200, Financial Liability Investigation of Property Lost.

(3) Review of loss reports to determine necessity of immediate investigation by DRMS Command Security Office or host officials.

(4) Investigation of suspicious loss reports. All reports of suspected theft, fraud, or other criminal activity must be reported and investigated immediately upon discovery of the incident.

(5) Analysis to identify trends or suspicious activity at a DRMS field activity. Analysis may also be conducted at the zone or headquarters level to identify broader trends. An effective analysis of losses should include but not be limited to the following concerns:

- Losses of similar like items.
- Several losses occurring in a specific location or warehouse.
- Losses occurring during a specific time of year or time of day.

- Losses occurring under similar circumstances.

(6) Use of analysis to investigate suspicious persons or activities or improve protection for specific items.

(7) Attempts to recover property suspected to be lost.

(8) Use of data to provide justifications for security improvements or enhancements.

(9) Reporting of data to Forward Support Teams and HQ DRMS in accordance with current procedures.

c. Methods of Obtaining Data

(1) The DRMS field activity leader and/or Security Coordinator will ensure that all activity employees are periodically instructed in reporting requirements for thefts or suspicious losses of material. All suspected thefts or losses of items requiring the submission of DD Form 200 are to be immediately reported via DRMS SITREP.

(2) DD Forms 200 that are forwarded to DRMS HQ for closure will undergo review by the Command Security Office.

3. Security Awareness Training Program

a. General: DRMS field activity leaders/Security Coordinators will implement a Security Awareness Training Program. The purpose of the program is to educate activity employees on security policies and procedures, increase their awareness of security concerns, develop proficiency at responding to emergencies, and to enlist their assistance in the protection of activity resources.

b. Elements: A good Security Awareness Training Program will include at a minimum, the following elements:

- Regular briefings to activity employees on security procedures and current security concerns.
- Posting of procedures and policies near employee workstations.
- Use of posters, videos, emails and other media to increase awareness and interest in the security of the activity.
- Personal attention to employee's concerns and development of personal contacts.
- Regular reports on scheduled security improvements and enhancements to enlist the support of employees and limit resistance to such projects.
- Attention to local/host security concerns and directives.

c. Security awareness training should be constant and ongoing. All employees will receive an initial security indoctrination briefing during their first month of employment; all employees will receive refresher training at least once per year.

d. The DRMS field activity Leader/Security Coordinator will maintain records of security awareness training sessions for 2 years. The DRMS Command Security Office during physical security surveys and assessments will review these records

e. Training materials and information are available from a variety of sources. Host security offices, public affairs offices, audiovisual libraries, the DRMS Command Security Office and the Internet are good places to look.

DRMS-I 4160.14, Volume I, Chapter 2

4. Security Support Requirements for Interservice Support Agreements (ISA). The ISA with the host installation will set forth the specific police services and other security related support to be provided for the DRMS field activity. Each activity will try to secure the following services. In case the host declines to provide such service, contact the DRMS Command Security Office for guidance. ***The following services are to be requested, consistent with the activity mission.***

a. Non-reimbursable: The following security support should be requested on a non-reimbursable basis for all DRMS field activities as standard requirements at the time Interservice Support Agreements with host military installations are initiated or renewed:

(1) Police Patrol:

- Supplier will: Provide routine patrol services to maintain law and order on the same basis as support provided other host activities. Make at least one or more patrol checks per day during non-duty hours to ensure activity facilities are properly secured. Maintain a record such as a building checklist, radio log, etc, to document the checks. Protect and secure activity assets found unsecured and notify the designated activity personnel immediately upon discovery of any security incident of breach of security.
- Receiver will: Secure activity facilities when not attended. Promptly secure and inspect facilities when notified if found unsecured. Comply with host external security criteria.

(2) Traffic Enforcement:

- Supplier will: Provide traffic supervision and enforcement to include investigation of traffic mishaps/accidents.
- Receiver will: Comply with host criteria.

(3) Investigations:

- Supplier will: Investigate all security/criminal incidents involving DRMS field activity personnel, facilities, or assets not referred for investigation to a major DoD Investigative Organization, i.e., DCIS, AFOSI, USACIDC, NCIS. Secure evidence, document results of inquiry and provide copies of investigative reports to the DRMS Office of Command Security upon their completion.
- Receiver will: Promptly reports all security/criminal incidents to host security/military police. Protect crime scene and evidence until host security/military police respond to the scene.

(4) Identification:

- Supplier will: Provide activity employees with security badges, ID cards, and/or vehicle decals required to access the activity work site (s).
- Receiver will: Comply with host requirements.

(5) Funds Escort:

- Supplier will: Provide police escort to the designated financial activities for activity personnel to deposit sales proceeds as required. Escorts are requested for amounts in excess of \$10,000 in negotiable ***instruments, such as cashier checks, money orders, travelers' checks, etc., including cash.***
- Receiver will: Request escorts and coordinate request in advance if possible. Comply with host criteria on movement of funds.

(6) Weapons Storage:

- Supplier will: Provide in transit security for weapons and major small arms subparts received or shipped by tenant DRMS field activity or host installation and provide custody for weapons on DRMS activity accountable records in approved small arms storage facilities. Provide activity with monthly inventories of all weapons stored in host facilities. Provide armed security vigilance during demilitarization of weapons on the host installation.
- Receiver will: Request support and coordinate all such requests with the host installation in advance, if possible.

(7) Key Control:

- Supplier will:
 - Allow tenant DRMS field activity autonomous control of all keys and locks used to secure activity facilities and assets.
 - Receiver will: Maintain positive control of all keys and locks in accordance with DRMS security criteria.

(8) Information Security:

- Supplier will:
 - Provide tenant DRMS field activity personnel with security awareness training.
 - Secure any uncontrolled classified material discovered in activity assets and ensure that appropriate inquiries/investigations of all known and suspected security violations are conducted in accordance with DoD 5200.1-R.
- Receiver will comply with DoD/DLA/host criteria.

(9) Force Protection:

- Supplier will:
 - Provide a standard level of support for Force Protection (FP) in accordance with DoDD 2000.12, DoDI 2000.14, DoDI 2000.16, DoDI 2000.18 and DoD 2000.12-H. Responsibility to apply FP will be proactive and reactive to include the following:
 - **Provide** timely **unclassified** threat intelligence and information sharing.
 - Incorporate the Receiver into the installation physical security, resource protection and emergency preparedness plans.
 - Incorporate the Receiver into the installation's AT/FP plan/directives
 - Provide Receiver with copies of applicable installation plans and directives
 - Advise Receiver of changes in **FPCON** in a timely manner
 - Provide annual Antiterrorism/Force Protection Awareness Training, and Level I travel briefings
- Receiver will:

DRMS-I 4160.14, Volume I, Chapter 2

- Comply with host regulations, guidelines and directed actions.
- Provide the host FP officer with DRMS field activity points of contact, telephone numbers, and e-mail addresses. Reimburse the host for FP above and beyond the standard level.

b. Reimbursable: The following security support should be requested for all activities on a reimbursable basis at the time the Interservice Support Agreements are initiated or renewed:

(1) Security Reviews and Inspection.

- Supplier will: Conduct physical security inspections of DRMS field activity facilities and operations as requested by the activity or DRMS Command Security Office, using as a minimum, DRMS security criteria.
- Receiver Will: Schedule the inspection at a convenient time. Promptly respond to all findings noted.

(2) Alarm Monitoring/Armed Response: (for activities with IDS or duress alarms)

- Supplier Will: Include Receiver protected areas under an alarm monitoring system. Provide armed response within service-prescribed timeframes. Test alarms weekly.
- Receiver Will: Provide Supplier with names of employees authorized to activate/deactivate/test alarms. Comply with Supplier alarm activation and testing criteria.

(3) Security Lighting:

- Supplier will: Provide such area and exterior lighting commensurate with energy conservation measures and with environmental risk factors. Lighting will not be reduced to where Receiver activity security posture is in jeopardy.
- Receiver will: Request installation and maintenance of lighting fixtures as required. Ensure lighting is extinguished during hours of daylight.

(4) Emergency Repairs:

- Supplier will: Provide priority emergency repairs as required to maintain a satisfactory activity security posture, i.e., repair of cut/damages security barriers, re-keying compromised and defective locks, etc.
- Receiver will: Request support promptly when defect/deficiency is identified.

c. Contract Security Service. When adequate security service cannot be provided by the host installation, DRMS field activity Chiefs may, through DRMS Command Security Office coordination, contract protective services from commercial sources.

d. Receipt in place locations (RIPL). Physical Security and Force Protection Support at these locations will be requested based upon the "operating environment" at each location. Specific responsibilities for security and force protection must be specified in the Memorandum of Agreement. Support must be provided to DRMS activities and personnel, consistent with support provided to other DoD service providers and other DoD tenants on the installation. Contact the Command Security Office Force Protection team for assistance with verbiage. NOTE: At RIPL sites where a logistics contractor is present, any inspection or findings resulting from the inspection or corrective action required by the contractor will be forwarded to the contractor through the COTR.

D. PHYSICAL SECURITY

In order to protect and secure DRMS field activity property, uniform standards or criteria have been developed. Variations in physical layout of activity yards and in physical condition and configuration of buildings and display areas affect the degree of compliance obtainable at each individual yard. When full compliance with criteria set forth below cannot be achieved, the activity Leader will request either an exception or a waiver for those specific areas of noncompliance. Exceptions and waivers are detailed in DRMS-I 4160.14, Volume I, Chapter 1, paragraph A3. ***Commercial Venture partners who operate out of DRMS activity locations will comply will the requirements of this instruction and chapter.***

1. Barriers. Physical barriers may deter accidental or deliberate encroachment on DRMS field activity property. In addition to traditional fencing, masonry, pierced steel planking (PSP), and the walls of scrap bins and buildings at least seven feet high can serve as barriers. Certain barriers, such as those surrounding a pilferable storage area, and outside storage areas are required. Determine the need for other barriers by the DRMS Command Security Office based upon recommendation of the activity chief and local environmental risk factors.

a. General Requirements

(1) Walls of locked warehouses constitute physical barriers. Base the need for additional barriers on local conditions including the history of pilferage, forced entries and the strength and condition of the warehouse walls, doors and windows. Special attention will be given to remotely located activity warehouses outside the confines of a main activity yard.

(2) Protect property in an open display area, which has potential for theft or malicious damage due to its size or value by a barrier. The type of barrier selected should preclude easy access to the property and should eliminate pedestrian or vehicle traffic except through designated points of entry and exit.

(3) Open display of large, not easily pilfered items, either whole or in part, is permissible. When using open display areas without physical barriers, proper posting of warning signs is required.

(4) Inspect all barriers for damage and effectiveness at the beginning of each workday. Upon discovery of damage or evidence of forced entry, notify host security and submit a DRMS SITREP immediately. In the interim between discovery and arrival of responding host security force, detail an activity employee to secure and preserve the scene by denying access to all pedestrian, vehicle and equipment traffic. Make permanent repairs only after approval is received from the responding security force. All damage weaknesses or deficiencies must be promptly **reported** to the host facility engineer for correction.

(5) Maintain existing barriers until they are beyond economic repair and do not alter or destroy merely to conform to standards identified in this publication. When existing barriers are no longer serviceable, initiate actions to have a new barrier erected.

b. Walls and Other Structural Barriers. Where walls, floors, roofs, doors, windows, or combinations of these serve as barriers, they will be constructed and arranged to provide uniform protection equivalent to that provided by the chain link fencing specified below. Where a fence adjoins a building wall, it will extend to within 2-inches of the building wall. Miscellaneous openings requiring bar or grill protection include:

(1) Openings less than 18-feet above uncontrolled ground, roofs, or ledges.

(2) All openings having an area of 96 square inches or larger, and a minimum height or width dimension of 6-inches or greater.

(3) 9-gauge chainlink steel mesh or equivalent strength material will protect these openings.

NOTE: These requirements do not apply to DRMS field activity administrative areas, provided there are suitable barriers between the administrative areas and property display areas.

DRMS-I 4160.14, Volume I, Chapter 2

c. New Barrier Construction Standards. Use fencing to meet specifications prescribed in the Federal Specification RR-F-191 series, configured and constructed as follows:

(1) Fabric. For outer perimeter fence fabric use chain link, two-inch diamond mesh, nine-gauge woven steel, preferably painted or coated with a non-reflective substance to reduce glare.

(2) Vision Screening. Addition of vision screening material (e.g., metal or plastic slats woven into the mesh, or screening fabric installed over the mesh) is detrimental to security, as patrols cannot observe activity within the fenced area. When such screens are used, increased host security patrol of the activity must be requested.

(3) Mountings. Mount fence fabric on metal posts of appropriate height set in concrete with additional bracing at corners and gates. In areas where metal posts are not available, reinforced concrete posts may be used as a substitute. Make posts, bracings, ties and other structural accessories of equal or greater strength than the fabric and locate and secure on the inner side of the fence facing towards the interior of the activity. Do not use aluminum ties due to ease of removal.

(4) Height. Make minimum height of the mesh fabric above the ground seven feet.

(5) Top Guard. Install triple-strand barbed wire outrigger facing upward and outward at a 45-degree angle so as to increase the overall height of the fence at least 12 inches. Tack weld support arms holding the wire to the posts to prevent removal.

(6) Anchoring. Extend fence fabric bottom edges to within two inches of firm ground and anchor to prevent lifting of the fabric to create an opening more than five inches high. Weave horizontal lacing into the mesh at the top and bottom edges and pulled taut to prevent bowing of the fabric. Secure all such materials on the inner side of the fence.

(7) Stabilization. Stabilize surfaces in areas where loose sand, shifting soil, or surface waters cause erosion capable of providing means to penetrate the perimeter. Where stabilization is impractical or impossible, provide concrete curbs, sills, or other similar anchoring devices, which extend below ground level.

NOTE: New construction or modifications of existing fencing will be in accordance with these requirements. Existing fencing that does not meet the minimum height requirements outlined above need not be increased to the specified height provided the existing fence is in good repair and has an overall height to include barbed wire top guard of 7-feet.

d. Barrier Openings

(1) Keep the number of vehicle and pedestrian gates in barriers at a minimum, consistent with operational requirements and safety. Gates will be structurally comparable and provide the same penetration resistance as the adjacent fence. Remote-controlled vehicle gates may be required in order to provide positive control of vehicles entering and exiting the DRMS field activity. Gates will be designed so that all transiting traffic, vehicle or pedestrian inbound and outbound, will be monitored and controlled by activity employees. Gates will not be left open and unattended or unmonitored by activity employees.

(2) Bar culverts, drainage structures, water passages, or designed openings that underlie or breach the barrier to the extent that they afford access to the activity area with a material of equal or greater strength than the barrier. Openings to drainage structures having a cross-sectional area greater than 96 square inches and a smallest height or width dimension greater than 6-inches, will be protected by securely fastened, welded-bar grills.

2. Clear Zones

a. The purposes of clear zones are to:

- Deter intruders from undetected entry.

- Deter intruders from crossing barriers with the aid of material located against or adjacent the barrier.
- Minimize accidental barrier damage from property or vehicle movement.
- Facilitate inspection and repair of barriers.

b. An unobstructed area or clear zone will be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the adjacent ground.

c. An exterior clear zone of at least 20 feet will exist from the exterior barrier. A minimum five-foot internal clear zone will be maintained. For parking restrictions see paragraph E2b (1).

d. When it is not possible to have adequate clear zones because of property lines or natural or man-made features, an increase in the height of the perimeter barrier or other compensatory measures may be necessary.

e. Vegetation within clear zones will be maintained at a height not to exceed 8-inches.

f. Exemptions

(1) Interior clear zones are not required at locations where the sides of permanent structures or permanent scrap bins within the activity area constitute the perimeter barrier.

(2) If located within a clear zone, fire hydrants, power, telephone, light poles and any supporting cables, need not be removed. Foot rungs on poles and tree branches above a height of nine feet are permitted; remove rungs and branches below that level.

(3) DRMS field activities may request exemptions for permanent structures within the exterior clear zone upon request and submission of photographs; facility plans or sketches to the DRMS Command Security Office documenting the degree of encroachment on the clear zone. It is the responsibility of the activity Chief to convey clear zone requirements to appropriate host authorities to ensure that those requirements are considered prior to any new construction within the designated activity exterior clear zones. Similarly, the activity Chief must ensure that any proposed construction within the yard does not violate field activity interior clear zone requirements.

3. Warning Signs. Warning Signs are necessary but costly security devices requiring continual replacement because of theft, damage, or deterioration. Color schemes and print styles will comply with host policies. The following standards apply:

a. Display:

- Displayed at active entrances, and around perimeter boundaries, with at least one sign every 500 feet. Place at least one sign per boundary side, if the side is less than 500 feet in length.
- Employee and visitor parking lots, entrances to retail stores and administrative buildings outside perimeter barriers, and administrative offices with entrance on the perimeter barrier are excluded from warning sign requirements.
- Used in conjunction with tapes, ropes, chains or other cordon material to delineate areas within DRMS field activity boundaries where access is temporarily or permanently denied to all except DRMS field activity employees.
- Affixed to the perimeter barrier or staked in the ground if no barrier exists. When host installation perimeter coincides with a portion of DRMS field activity boundary, use host warning signs on that portion of the DRMS field activity perimeter.

DRMS-I 4160.14, Volume I, Chapter 2

b. Wording and construction: NOTE: Wording applies when purchase of replacement signs is required and after other potential sources of supply have been examined and found unproductive.

- Worded as "WARNING - AUTHORIZED PERSONNEL ONLY"
- Lettered to be easily readable from 50 feet. Use light reflective materials if available.
- Constructed of weather resistant materials. A uniform size of 12 inches high and 24 inches wide (12"x24") is recommended. Interior signs may be fabricated of wood, metal, plastic or cardboard.
- Worded bilingual where required by local laws in the U.S. and by international agreements in foreign countries. If bilingual signs are to be used, consider including locally accepted and understood danger-warning symbols on the signs. Do not post signs where a low profile of U.S. presence is preferred.
- DRMS Form 1988, DRMO Warning Sign, is suitable for this purpose.

c. When DRMS field activity boundaries form part of a military installation perimeter, installation-warning signs must be posted in accordance with service and host policy.

4. Pilferable Storage

a. Each DRMS field activity must set aside a room, locked enclosure, wire or steel mesh "cage", container, or building located inside the activity boundary, providing pilferable or sensitive property, additional protection against theft. This area must provide a delay factor requiring use of burglary tools by a potential intruder to gain entry. These areas are not mandatory if normal receipts of property requiring special safeguard do not exceed the volume that can be stored in a safe. In such situations, the safe itself becomes the pilferable area and access requirements identified in paragraph D4c this chapter, apply. Similarly, if additional security for unusually high value or extremely pilferable items is necessary, safes, lockable cabinets, or conex containers may be placed inside these areas. Again, access requirements of paragraphs D4c, this chapter, apply. Do not place any signs on the doors of such areas, which may draw attention to the fact that special access requirements apply, or sensitive assets are contained therein.

b. Construction Criteria

- Commercially procured prefabricated security cages constructed of not less than 10 gauge chain link material with a mesh of two inches or less (or its expanded steel equivalent) is recommended. When local commercial construction is preferred, identical strength requirements apply. When using chain link mesh material, the construction criteria outlined in paragraph D4c will apply.
- Cover windows and vents with a material that provides a deterrent equal to or greater than the rest of the structure.
- Install mortised deadbolts in doors where appropriate and lock whenever unattended. Door materials and locks must provide a delay factor equal to or greater than the rest of the structure.
- Only one active entrance/exit is permitted. When additional emergency exit doors are required by DRMS or host installation safety and health directives, they will open only from the inside and be equipped with audible alarms which sound when the doors are opened.
- Glass display cases must remain locked at all times if storing pilferable items.
- In the event the area is not topped with a ceiling panel, extend the walls to the ceiling of the room or roof of the building in which it is located. In such cases, pay particular attention to those overhead areas to ensure that crawl spaces, ducts and dropped ceilings do not provide unseen access into the area. Inspect the floor to ensure that similar access is not provided under the area. If either

ceiling or floor fail to provide required security, e.g., "delay factor requiring use of burglary tools", they must be reinforced to the point that the deficiency is corrected.

c. Access

- Only employees designated by the activity Leader, as access authorized will enter this area.
- List names of all access authorized employees in lock and key accountability records on DLA Form 1610b. **Separate access lists are not required.**
- Activity Leader or security coordinator: Notify access-authorized employees of their selection and brief immediately regarding their responsibilities involving the area.
- Restrict the number of access-authorized employees to a minimum commensurate with operational necessity.
- Access-authorized employees must escort visitors within the area at all times. While the number of escort employees required depends on the control capability of the escort, the behavior of the visitor, and the physical layout of the area, the primary concern is to ensure that all visitor activities are monitored. If escort employees feel they cannot adequately perform this duty, additional escorts must be detailed or the number of visitors allowed entry curtailed. In situations where numerous visitors require entry, either routinely or because special interest items are being safeguarded, give consideration to use of portable closed circuit television (CCTV) cameras to augment escort employee surveillance. Upon visitor entry into a these areas, responsibility for the safeguard of all items stored within, passes from the protection provided by the barrier, gate and locks to the awareness of the escort employee **Visitor registers are not required.**

5. **Locking Devices.** Care must be taken to select locks that are designed to provide the appropriate level of security, (i.e., delay factor equal to the barrier on which it is used) and that are constructed to withstand environmental conditions existing at the intended use site. Locks identified specifically for indoor use may not be suitable to be exposed to the elements and their continued use in outdoor applications will result in failure of the lock. When selection or serviceability of a particular locking device is in question, request DRMS Command Security Office assistance.

a. Key Operated Locks. The cost and complexity of locks varies widely according to the level of security provided. While any of the following pin-tumbler locking devices are suitable for DRMS field activity use, the indoor padlocks identified below are inadequate for prolonged use outdoors. However, any such serviceability becomes questionable. At that time they must be replaced with the outdoor use padlocks also identified below. Those padlocks are also suitable for pilferable area use. Padlocks selected for use indoors or outdoors should be with case hardened bodies. Shackles should also be case hardened, and a minimum of 5/16" wide.

NOTE: Padlocks listed here may no longer be available through military installation supply channels. For assistance and recommendations on locking devices, contact the DRMS Command Security Office.

- 5340-00-158-3805 - low security indoor use padlock, (MILSPEC MIL-P-17802).
- 5340-00-159-3807 - same as above with chain, (MILSPEC MIL-P-17802C).
- 5340-00-241-3670 - medium security outdoors use padlock, (MILSPEC MIL-P-43951).
- Mortise locks with minimum one inch throw deadbolts not visible or accessible in locked position.

b. Combination Locks

- If combination locks are required, GSA approved; three-position changeable combination padlocks are adequate for activity use in either indoor or outdoor applications.

DRMS-I 4160.14, Volume I, Chapter 2

- 5340-00-285-6522, 5340-01-119-3981 or 5340-00-285-6523 - combination padlock, (MILSPEC MIL-P-17257).
- Conventional three position "dial type" combination locks using numbers or other reference points to align tumblers into an unlocked position are not recommended for activity use.

c. Hasps and Staples

- Heavy steel hasps and staples are suitable for secondary locks when securely fastened to the structure with smooth headed bolts or rivets, or peened or welded to prevent removal.
- Use high security hasps, described in Amendment 1, MIL-P-43605 (CL), only in applications where lock of similar protection level are required.

d. Cipher Locks. This type of digital combination door lock is recommended for installation on high pedestrian traffic doors accessing areas limited to employees only. Cipher locks are not recommended for securing activity property.

e. Numerous sophisticated locking systems and automated access control systems are available which use neither keys nor combinations. Included are locks that open when a magnetic or punched card is inserted; others open when a fingerprint previously registered in computer memory is placed on a glass plate; still others open when a previously registered voice speaks into a microphone. Such systems may be suitable for activity use. Their intended use and installation must be coordinated with the DRMS Command Security Office.

6. PROTECTIVE SYSTEMS/FACTORS

a. Intrusion Detection Systems (IDS) provide an added degree of security, which may be cost effective in some facilities. IDS is designed to detect and announce an intrusion but is unable to prevent the intrusion or apprehend the intruder. Its use will enhance the efficiency of security forces. When used, IDS are usually installed on one or more warehouses where high value and highly pilferable items are stored. Do not enter into agreements for lease, purchase, or installation of IDS without written approval of the host security agency and coordination with the DRMS Command Security Office.

(1) The following factors must be considered in determining the necessity and feasibility for IDS:

- Mission, geographic location and critical importance of the host installation.
- Vulnerability, accessibility and value and potential threats against of activity property normally on hand at the location under consideration.
- Environmental risk factors including past history of pilferage and other criminal activity at the activity.
- Estimated initial and recurring cost of the IDS, their design and their salvage value.
- Response capability of host security personnel to an intrusion.

(2) The use of leased or purchased commercial security equipment may be authorized. Leasing arrangements will include a provision for Government retention of all wiring and cabling associated with the IDS after termination of the lease.

(3) It is important for planners to remember that any warning system is valueless unless it is supported by prompt security force action. All IDS alarms must prompt a security response. IDS alarms must provide direct and immediate alert to host security forces or commercial alarm monitoring facilities indicating that an unauthorized intrusion has been made into an area under alarm protection.

(4) The system must remain in continuous operation during the activity's non-operational hours. Each system must be capable of operating from an auxiliary power source. The time requirement for such operational capability must be evaluated in each case dependent upon such factors as alternate power supplies, maintenance support, and hours of active operation. Auxiliary power sources for IDS will be tested monthly. Records of such tests will be maintained.

(5) Plans and diagrams showing the location and technical data of installed systems, signal transmission lines, and control units will be marked "FOR OFFICIAL USE ONLY." Access to such plans and diagrams will be strictly limited to those with a "need to know."

(6) IDS and duress alarms will be tested weekly by the alarm monitoring response force to ensure component parts are operating properly. IDS tests may occur during normal duty opening or closing of the area under protection. Activities that have self-diagnosing alarm systems need not conduct the weekly tests, but will at a minimum, run the diagnostic program weekly.

(7) In case of alarm system failure, the DRMS field activity alarmed area must be manned until the system is repaired or other appropriate compensatory measures applied. Notify the DRMS Command Security Office whenever there is a catastrophic or complete alarm system failure.

b. Protective Lighting. Requirements for protective lighting at DRMS field activities depend upon the local situation and areas to be protected. Determine the need for such lighting and the specific type to be utilized by the activity Chief in coordination with the DRMS Command Security Office. If it is determined that new or additional protective lighting is required, consider the following guidelines:

(1) Use engineering services in the design and installation of the lighting system. High-sodium lights with an object illumination factor of a minimum of 0.2 foot-candles and 2 lux are the security industry standard.

(2) Use area lighting as opposed to boundary lighting. The outside storage area and building exteriors will be illuminated with sufficient intensity to enable visual surveillance by the security force.

(3) Protect switches, power lines and supporting equipment so as to deny an intruder the capability of neutralizing the system by merely turning off the switch or cutting the power supply.

(4) Alternate/emergency power sources for protective lighting is not required.

c. Communications. Each DRMS field activity will have at least one means of communication with host security. The regular telephone system (local exchange or commercial service) is adequate for this purpose. Alternate means of communication are not normally required but may be considered under unique circumstances.

d. Closed Circuit Television (CCTV). Potential applications for CCTV include:

(1) Control of vehicle/pedestrian gates from a remote location.

(2) Substitute for employee observers in activity areas open to the public, (i.e., RTD and sales screening, scrap yard, scales, etc.).

(3) Sustained monitoring for infrequent events (used with motion detection or time-lapse applications).

Do not enter into agreements for lease, purchase, or installation of CCTV without written coordination of the DRMS Command Security Office.

E. PROCEDURES

1. Lock and Key Control. Locking systems provide added security at DRMS field activity entry and exit points and on specialized cabinets, safes, rooms and areas used to store property. The effectiveness and adequacy of locking devices is only as good as the controls placed over it. Accomplish tight access control over all such

DRMS-I 4160.14, Volume I, Chapter 2

systems through uniform lock and key control systems of accountability. The activity Chief will determine what areas and containers are to be locked and which keys, if any will be issued for personal retention and/or removal from the facility. Keep issue of such keys to a minimum consistent with operational needs. Keys may not be duplicated without written approval of the activity Chief.

a. The activity Leader is the key custodian unless he/she delegates the authority to another employee in writing. The primary function of the key custodian is to implement and maintain the key control procedures outlined in this chapter. Alternate key custodians may be appointed by the DRMS field activity Leader as required. These designees will be concerned with the supply of locks and how they are stored, the handling of keys, record files, investigation of lost keys, maintenance and operation of key repositories, and the overall supervision of the Key and Lock Control Program

b. Depending on activity size and complexity, more than one key and lock control system may be required. Each system will have a designated key custodian and alternate, an active key repository with a listing of employees authorized to draw keys, and an additional repository, if required, for reserve locks and keys.

c. Affix keys normally used together or in sequence on key rings in sets. Identify each ring with a tag bearing a ring identification number. Keys normally issued and used, as a group will be affixed as a set on rings of at least 12-gauge wire or its equivalent that has been welded or brazed together. Each ring will include a metal or plastic tag stamped or imprinted with a ring identification code. Key rings will be signed out by their identification code.

d. On buildings or areas with several entrances, consideration should be given to securing all but one or two entrances from the inside. This effectively reduces the number of locks required to totally secure the building or area from unauthorized outside access.

e. Government keys and locks of an individual or personal nature, such as administrative offices, desk and locker keys, need not be included in the key control system.

f. Do not include keys of activity vehicles and material handling equipment (MHE) in the key control system. Do not leave keys in vehicles when unattended. Immobilize MHE without key ignition when not in use. Park MHE inside during non-duty hours, unless the size of the MHE makes that prohibitive.

g. Do not provide keys to the host installation without the DRMS Command Security Office approval based on receipt of a written request from host authorities.

h. Change keyed locks immediately when compromise of the lock is known or suspected. Key theft, loss, breakage, or unauthorized duplication is the most common causes of lock compromise.

i. To prevent theft or possible substitution, relock all padlocks, which have been unlocked to afford entry to an entrance or container on their staples immediately after opening. Do not leave keys in locks.

j. Standard Form 700, Security Container Information, and Standard Form 702, Security Container Check Sheet, will be used in conjunction with each combination lock or security container. **NOTE: This requirement only applies to safes that are used to store funds or fine precious metals.**

k. Physically inventory all keys and padlocks within a key control system, including keys issued for personal retention, at least every 6 months. Document the inventory reflecting total number of keys accounted for during the last inventory, number of keys in repositories (to include duplicate or reserve keys and locks), keys issued for permanent retention, keys added since last inventory, and keys removed since last inventory, and a total number of keys accounted for. Inventories are also to be conducted whenever a primary key custodian is assigned that duty.

l. Key and Lock Records and Accountability. Maintain control records for all key control systems.

m. Keep the number of individuals authorized to draw keys to the absolute minimum commensurate with security and operational requirements. Keep issued keys in the possession of the individuals to whom they

were issued at all times. Do not transfer to another person without being turned in to and reissued by a key custodian.

n. Use of master key systems is prohibited.

o. Operating keys to pilferable storage areas fine precious metals containers, and to cashier areas will not be issued for personal retention or removed from the DRMS field activity. **Keys that unlock key repositories may be permanently issued, but must not leave the activity. Security of key repositories with combination locks is encouraged. 9 May 2003**

p. When keys are not in use, secure in operating key repositories of at least 20-gauge steel or material of equivalent strength. During duty hours, secure key repositories in a manner to prevent unauthorized removal and located so they can be observed by operating personnel. After duty hours, key repositories will be secured in a safe unless they have been permanently anchored to the structure of a building or room designed to resist illegal entry. Keep repositories locked except to issue or return keys or to conduct inventories. Issue key(s) to the key repositories to the key custodian or alternate under appropriate receipt. Do not keep repository keys in unsecure desk drawers. Secure reserve padlocks and their keys as well as duplicate keys in a duplicate key repository or in a safe or locked metal container meeting the requirements of a key repository. Control access to the duplicate container and accountability in the same manner as for operating key repositories.

q. Keep all keys within the key and lock system under continuous accountability at all times. Accomplish as follows:

(1) Maintain DLA Form 1610 inside each repository reflecting a master inventory of all locks and keys in that particular repository. It will be used as the basis for inventories of keys controlled from the repository by individual key serial number. Prepare DLA Form 1610 for all reserve and duplicate keys.

(2) Use DLA Form 1610a to maintain accountability of each repository and its keys. Two inventories will be conducted each duty day. The key custodian will inventory the repository at the beginning and end of the day using the DLA Form 1610. Results of the inventory will be annotated on the DLA Form 1610a by completing the date and time blocks, indicating the number of keys in the repository in the "TOTAL NUMBER OF KEYS" block; stating "All keys accounted for" or annotating missing keys and actions taken in the block entitled "PRINTED NAME AND SIGNATURE OF INDIVIDUAL ASSUMING RESPONSIBILITY"; and signing in the block reserved for the signature of the individual receiving keys. All other blocks will be left blank. At the end of the day, the same procedures will be followed for the closing inventory. In the "REMARKS" blocks reflect keys that have been added, removed, or lost/stolen. Report losses or thefts immediately to the activity Chief.

(3) Use DLA Form 1610b, signed by the activity Chief, to authorize employees to sign for keys as well as to document withdrawal of that authorization. Several individuals may be listed on the same form provided each is authorized to sign for all keys listed on the form. The DLA Form 1610b will expire 1 year from signature date.

(4) Use DLA Form 1610c by all key custodians to record removal and return of keys. Maintain a separate DLA Form 1610c for each repository. Also, maintain a separate DLA Form 1610c for keys, which are permanently signed out to individuals (i.e., DRMS field activity chief, etc.). When not in use, DLA Form 1610c will be locked inside the repository to which it pertains. All keys removed from the repository will be recorded on the DLA Form 1610c. The DLA Form 1610c must reflect only signatures of designated key custodians and persons authorized to receive keys as designated on DLA Form 1610b.

(5) Keeping DLA Form 1610 current, with accurate inventories reflected on DLA Form 1610a achieves continuing accountability for operating keys, and all authorized key issues and returns properly reflected on DLA Form 1610c.

r. Automated Key Control Systems. An automated key control system may be used to store and control issue of security keys. The system should have sufficient controls built into it to provide the same or better security than the manual system described above. Completion of forms and reports mentioned above is not

DRMS-I 4160.14, Volume I, Chapter 2

necessary if the system can generate the same information. At a minimum, the system should have the following characteristics:

- (1) The capability to remove access for employees who have been terminated, resigned, transferred, or no longer have access to the areas that the keys unlock within 24 hours of notification.
- (2) Register an alarm after 3 unsuccessful attempts to retrieve a key.
- (3) Register an alarm upon attempts to tamper with or defeat the system.
- (4) Register an alarm upon attempts to retrieve or return a key outside of normal duty hours.
- (5) Have the capability to limit read/write authority to the database. Read/write authority should be limited to the minimum number necessary for efficient and effective operations.

NOTE: Do not enter into agreements for lease, purchase, or installation of automated key control systems without coordination by the DRMS Command Security Office

s. Change combinations at least annually, or when compromise is known or suspected, or when a person knowing the combination no longer requires that knowledge. Do not use anniversary dates, birth dates, multiples of 5 or 10 (e.g., 5-10-15; 20-30-40) or sequential numbers (e.g. 23-45-67; 98-76-54). Memorize combinations. Do not record for personal convenience and do not annotate in activity records. Recording of container combinations is optional at the activity Chief's discretion. If recording the combination is desired, annotate the combination on part 2a and enclose within Part 2 of Standard Form 700, Security Container Information, then forward to the Forward Support Team *or his/her designee*. Use certified mail for container combinations. Secure safe combinations in a locked drawer or container.

2. Entry and Movement Control. Control of visitors, vehicles and property moving in and out of an activity yard is a significant part of a total security program for any DRMS field activity. While standard or uniform procedures to effect this program are most desirable, variations in facility design influence the type of system needed that is best in terms of control, cost and convenience. The following are standard required procedures for entry and movement control. **NOTE: Requirements of the Logistics Partner are to maintain a Visitor Control Program.**

a. Visitor Control. The ability to enter a yard or building unchallenged and uncontrolled constitutes a serious breach of security resulting in increased pilferage and fraud. Therefore, continuous monitoring of visitors from entry through departure is required. Use the following practices:

(1) Registration. Register all persons, vehicle drivers included, desiring access to DRMS field activity for inspection, CV sales, screening, or property pick up, or property turn-in on DRMS Form 147. Prospective bidders complete DRMS Form 1581 and need not sign the DRMS Form 147. See paragraph I2a (1)(f) for additional registration requirements on sale days. Required visitor registration procedures are as follows:

- Maintain DRMS Forms 147 for visitor registration. If the activity has self-contained sites geographically separated from its central registration point, maintain separate registers at those sites.
- Visitors required to register need do so only once each day on their initial entry to the activity, or to any geographically separated site where a DRMS Form 147 is maintained. A requirement to sign out on the register at time of departure is mandatory.
- Required information on the DRMS Form 147. In addition to signature, limit to a legible rendering of the visitor's printed name; organization/firm represented, include address if not from the host installation; reason for accessing activity property, include the site location if it is geographically separated and a site register is not maintained; date and time of sign in. If an individual signing in has a vehicle that will be brought onto the activity yard, it must be listed by make, model and license/registration number. The activity Chief (or designated representative will conduct periodic

spot checks of the register to verify accuracy and completeness of entries made by visitors and to check their personal identification.

- Ensure visitors screening property are so authorized by verifying the individual's possession of valid identification. A picture ID is highly recommended, e.g., military/civilian ID, current driver's license, etc. In the case of direct removal by DoD or other transferee, review the appropriate authority designation document or letter of authorization (see DRMS-I 4160.14, Volume **III** for specific guidance for direct removal of property and Volume III for specific guidance on visitor identification.).
- In the event an individual known or suspected to be debarred from participation in surplus sales is identified within the activity, the activity Chief or representative will escort that person from the sale area and immediately contact the assigned counsel for guidance. If confirmation is received that debarment is current, remind the individual of the restrictions imposed by debarment and request the individual leave the facility. Should the individual fail to comply, contact installation security, brief on the situation, and request security to remove the person from the activity. Document the entire incident with signed statements by all activity employees having first hand knowledge of the events. Clip the statements, together with all pertinent disposal forms identifiable with the individual (i.e., DRMS Forms 147, 1581, etc.), and a photocopy, if obtained, of the identification used to gain entry. Forward to assigned counsel for consideration of debarment extension.
- Sale Days. All persons wishing to attend the sale must register by signing either the Bidder Registration Form or the Visitor/Vehicle Register as outlined in paragraph D5a (1), this chapter. Request all visitors provide valid identification, (e.g., photo ID cards issued by the Government or industry, driver licenses, passports, etc.). Following identity **verification and prior to award of successful bid, customers** will have their name checked against the Bidders Master File Extract (BMFE) to ensure that DRMS field activity access is authorized. (See DRMS-I 4160.14, Volume V, for specific listings and situations that may result in access denial.)
- Exemptions to Visitor Registration
 - Official visitors are exempt from registration based upon orders or other official credentials.
 - Visitors who enter only the DRMS field activity administrative area or otherwise have no access to DRMS field activity property.
 - Security, safety, medical and fire protection personnel responding to emergencies.
 - Contractor personnel (**such as CV**) with whom DRMS or the DRMS field activity have a contractual agreement, may be exempt from daily registration, provided the contractor agency has provided an official listing of personnel that will be doing business on the premises on a regular and continuing basis.

(2) Visitor Badges. Badge systems for visitors are mandatory if local conditions warrant increased visitor visibility. DRMS Forms 1960 (Sales), 1961 (RTD) and 1993 (Official Visitor) series are prescribed for identification for sales, RTD and official visitors. These forms are paper, adhesive-backed visitor badges that are designed to be disposed of at the end of the visit. Each form comes in 5 colors (blue, green, purple, red, and yellow). The activity Chief will prescribe different color forms for different days of the week, and inform the workforce of the color of the day in order to enhance visitor visibility and authorizations. Secure all unissued badges at all times.

b. Vehicle and Property Control

(1) Vehicle Control. Procedures used to control the movement of vehicles will be as follows:

- Vehicles will enter and exit through a single designated gate that is under continual visual observation by DRMS field activity employees. Employee and visitor parking within 50 feet of warehouse entrances or open storage areas or within the confines of the activity are prohibited. Activity chiefs will ensure appropriate signage and barriers are in place to enforce this restriction.

DRMS-I 4160.14, Volume I, Chapter 2

- All operators of vehicles having access to activity property or entering the activity to deliver or receive property will provide full, accurate and legible entries on the DRMS Form 147.
- After registration and inspection, drivers will proceed to and from appropriate receiving or shipping areas by designated routes. These vehicles will be escorted or monitored at all times. When business is completed, drivers will allow their vehicles to be inspected for unauthorized removal of property and will complete the sign out portion of the DRMS Form 147.
- Government, commercial and privately owned vehicles may enter the DRMS field activity only for the specific purpose of picking up or delivering property. Parking for extended periods of time is prohibited. Other government or commercial vehicles conducting official business may enter for that express purpose, by which the use of the vehicle is required, provided they comply with registration requirements.

(2) Inspection/Weighing Procedures

- Inspect all vehicles entering a DRMS field activity for the purpose of removing property by weight for extraneous cargo or suspicious items that could be used to inflate their weight. Re-inspect on departure, to ensure that all cargo and personnel in the vehicle at the time of weigh in are present on weigh out.
- Inspect each vehicle that accessed activity property prior to leaving the activity facility for unauthorized removal of property. Supplement the review of driver documents verifying removal authority by visual inspection of loaded material. Inspect vehicles that should be empty.
- Strictly enforce scale inspection requirements outlined in DoD 4160.21-M, Chapter 7, paragraph K3a, and activity weighing policy (also see DRMS-I 4160.14, Volume *II, Chapter 2, Para. F*).

c. Property Control. Use procedures to control the movement of property, material and packages as follows:

- Use activity employees and/or closed circuit TV to escort/monitor all visitors to preclude pilferage or improper handling of property.
- Establish single point entry/exit controls for each display location to preclude unauthorized movement of property.
- Do not remove Government property from the activity for personal use.
- Activity chief: Establish procedures to prevent employees and visitors from entering display areas with personal property items such as lunch boxes, handbags, briefcases and any other similar items which may be used to conceal pilferable property.
- Use Optional Form 7 or similar form used by the host installation, prepared in duplicate and signed by the activity Chief or his authorized representative, to authorize activity employees to remove property from activity facilities. Retain the original (by the activity Chief) and annotate when the property is returned. Use the pass for the following types of property:
 - Government property not covered by normal shipping documentation (DD Form 1348-1 and DRMS Form 1427).
 - Personal property not accompanied by a sales document and not readily identifiable as personal property.
- All property covered by a property pass is subject to inspection upon entry or departure from the activity.

- Property pick-up procedures for customers are fully discussed in DRMS-I 4160.14, Volume II.

d. Railroad Car Control

- Monitor movement of railroad cars in and out of DRMS field activity facilities by designated activity employees.
- Control all railroad entrances by locked gates when not in use. Activity employees will man gates, which are opened for passage of railroad cars.
- Control keys to railroad gates by the activity or provided to host security under proper receipt.

3. Pilferable Items

a. The designation of specific items or materials as pilferable or sensitive property is primarily by assigned Controlled Item Inventory Codes (CIIC) codes or pilferage codes. These codes may be reflected on turn-in documents and in DAISY or the FLIS. Activity Leaders are required to ensure that mandated protective requirements based on CIIC codes as reflected in DoD 4100.39-M, are met. Activity Leaders are required to effectively protect sensitive/pilferable assets by making effective use of available secure storage. Employees must declare "sensitive/pilferable" designations to certain categories of property that may not reflect a CIIC or pilferable code (i.e. property turned in under a local stock number). Conversely, items may be designated pilferable by NSN when condition, **obsolescence**, etc. may negate the designation. These designations should be consistent with military and commercial usage. Variables to be considered include quantity, size, weight, condition, and available storage facilities versus property on hand and current market conditions in the geographical area of the DRMS field activity. Special consideration must be given to the following types of items: Aircraft engines equipment and parts, communications and electronic equipment and parts, vehicular equipment and parts, photographic supplies and equipment, office machines, individual clothing and equipment, and hand tools and shop equipment. Inherently dangerous materials, i.e. swords, knives, police batons etc., will be placed in the designated pilferable storage area.

NOTE: Bolt cutters and similar cutting devices may not be left in open display areas. They must be secured as a "pilferable" item.

b. Store pilferable items in a safe or within the designated pilferable storage area. If this is not possible due to storage constraints or limitations, then use the next most secure available display location. The DRMS Command Security Office will provide guidance at any time an appropriate display area appears to be unavailable. DRMS field activity Leaders will ensure that:

- Employees are trained to recognize sensitive or "pilferable" property.
- DD Forms 1348-1A/2 accurately identify all pilferable items at time of receipt. (See DRMS-I 4160.14, Volume IV, batches for additional guidance.)
- Pilferable property is immediately processed and secured in the designated pilferable storage area on receipt.
- Movement of pilferable items is controlled to, from and within the most secure display location in the DRMS field activity.
- Status changes of pilferable items are processed on accountable records in a timely manner.

4. Safeguarding Funds. The following minimum physical security practices for funds protection are required at all DRMS field activities where funds are collected; for specific cashier responsibilities in this area (see DRMS-I 4160.14, Volume VI, Chapter 3). All references to "cashier" in this section pertain equally to both primary and alternate cashiers.

DRMS-I 4160.14, Volume I, Chapter 2

a. Safes. When negotiable instruments are retained overnight, a cashier safe independent of the activity safe must be furnished for exclusive use and access by the cashier. Place the funds into the cashier's cash box; lock the box then place in the safe. Safes must be GSA approved or be a UL certified burglary resistant safe, with a minimum protection factor of TL-15. Contact host security or the DRMS Command Security Office for guidance. Safes will, when possible, be located so that it may be seen from outside the building.

- Cash Boxes. When the safe storing funds does not contain lockable compartments, issue each cashier a cash box for their exclusive use. Keep boxes closed and locked except when funds transactions are being made. Do not leave cash boxes or funds unattended. During cashier operations, position money drawers and cash boxes out of public view and reach, placed so as to deny funds access to anyone but the cashier. Most commercial cash boxes are little more than temporary funds containers equipped with cash drawers from which to make change and are not intended to be used as security containers or strongboxes. They are typically constructed of extremely light metal, which can be easily distorted or damaged in order to access their contents. Under attack, their locking devices provide insignificant protection.
- Cash Box Modification. The activity chief should examine all cashier cash boxes for the inherent defects identified above. Modify those containers having weaknesses by riveting a hasp and staple to the box. When locked with a padlock, cash boxes so modified are generally immune to undetected pilferage or tampering of funds stored therein. Secure hinges on cash box covers by peening, crimping, or reinforcing with rivets. When heavy duty, entry-resistant, industrial cash boxes are utilized, the foregoing modifications are not required.
- Cash Box Padlocks. Issue each cashier a new cash box padlock and, in order to maintain exclusive access to cashier funds, issue all keys for that lock. Retain one key permanently for daily use; maintain duplicates outside the facility or destroy duplicate keys and record such destruction. Replace cash box locks when cashiers are changed.
- Initiate Standard Form 700 and affix Part 1 to an interior wall or drawer of the container. Recording of container combinations will be at the activity chief's discretion. If recording is desired, forward Parts 2 and 2a to the Forward Support Team by certified mail. Under this arrangement should a lock out occur, the Forward Support Team will provide the cashier, or if circumstances warrant, the sales or activity Chief, the combination by telephone. Once the safe is opened, change the compromised combination and re-accomplish the Standard Form 700. Change the safe combination at least annually or whenever persons with access to the combination no longer have or require access, or when compromise of the combination is known or suspected. Protect container combinations in a secure container.
- Affix Standard Form 702 to the exterior of each safe. Each time the safe is opened or closed, complete entries in the "Opened By" and "Closed By" columns. A disinterested person other than the individual who closed the safe must complete the "Checked By" column at the close of business daily. Each duty day that the safe is not opened, check the safe with time and initials of the person checking the safe entered in the "Checked By" column and "not opened" annotated through the "Opened By" and "Closed By" columns. Retain these forms for 90 days. ***When the safe is empty, daily checks and subsequent documentation are not required. 24 April 2004***
- If cash and negotiable instruments are stored in a safe weighing less than 500 pounds, anchor the safe to the structure in which it is located by bolts, heavy metal straps or protected in an equivalent manner. Remove wheels, if present.

b. Funds Storage Limitations: DRMS field activities will not store negotiable instruments overnight in excess of the authorized change fund, or as limited by host officials, whichever is the lesser amount. Under no circumstances will over \$2000 be stored. If deposit in a designated night depository is not possible, one time overnight storage of funds for exigent purposes may be authorized by the Forward Support Team, provided there is a suitable container (GSA Class 5, or equivalent) available, and coordination is obtained from host security. Cash reconciliation and verification as outlined in DRMS Instruction 4160.14, Volume VI, Chapter 3

must be accomplished before the end of the duty, and a cash count and verification must also be performed immediately after the safe is opened on the next duty day.

c. Permanent Cashier Facilities. Activities need not have a permanent "cage" for cashier use. If construction is desired, cashier cages will conform to requirements defined in paragraph D4b, this chapter, with the following addition: limit access to the cashier cage to the primary/alternate cashier, cashier supervisors, cash verifiers and auditors, and disinterested witnesses for purposes of locking the safe. Visitors, other than official visitors in the conduct of their duties, are not authorized in cashier cages. List names of all access authorized employees in lock and key accountability records on DLA Form 1610b.

d. Temporary Cashier Areas. At activities that do not have permanent cashier cages, set aside a temporary room or otherwise enclosed area for the exclusive use of the cashier. Because the cashier operation should be observable to management and co-workers at all times, take care in selection of the site. It should be sufficiently removed from the noise and commotion of the sales area to allow business to be conducted accurately and efficiently; it cannot be so remote as to encourage a robbery attempt. Ideally, the room or selected area will have only a single entrance. If such location is unavailable, lock all windows and doors providing access to the site from the cashier's side of the wall or barrier. An office table or desk moved into the doorway of the room bars public entry and normally provides both adequate customer-to-funds distance as well as a convenient work surface on which to conduct business. When rooms are unavailable, construct a makeshift area by moving furniture and files to create the necessary customer barrier.

e. Duress Alarms. Duress alarms are required at activities where their installation is prescribed by host directive or unique and specific local threats. Duress alarms must provide direct and immediate alert to host security forces or a commercial alarm monitoring facilities indicating that a cashier is undergoing, or has just experienced, a robbery or other threatening situation.

- Locate activating controls to allow covert operation by cashiers.
- Test the alarm weekly or as prescribed by host asset control/crime prevention authorities and also, in coordination with those authorities, prior to each sale date. Document all duress alarm tests and retain that documentation for 2 years.
- Govern activation of direct duress, local, or radio alarms by local installation security procedures. On most installations, cashiers are instructed not to activate robbery alarms until after the robber has left the facility. This procedure reduces the potential for cashier, employee, or customer injury and greatly decreases the possibility of having the robbery escalate into a hostage situation.
- Do not enter into agreements for lease, purchase, or installation of duress alarms without written approval of the host security office and coordination with the DRMS Command Security Office.

f. Funds Escort. Request armed escort from the host for amounts of greater than \$10,000 in negotiable instruments, including cashier's checks, money orders and cash. Host and military service thresholds may differ than this amount. Fund escort requirements for DRMS field activities tenant on military installations will be in accordance with the criteria established by the host.

- At locations where the movement of funds through an area is not under military jurisdiction, request host security support with armed escort. Request armed escort by the host based upon local threat, and upon host support to other installation funds handling activities. Coordinate with local security or investigative agencies for information on threat assessment. Should the host be unable to provide the funds escort support due to jurisdictional constraints, other armed escort service may be appropriate. Contract armed courier service for funds escort will be determined in coordination with the DRMS Office of Command Security on a case by case basis.
- Procedures. In addition to instructions provided by the host security agency, activities will comply with the following procedures when transporting funds without armed escort, both on and off the installation. If these procedures conflict with host policy, then the host policy will prevail.

DRMS-I 4160.14, Volume I, Chapter 2

- Routes To Facility:
 - Plan a primary and one or more alternate routes if possible.
 - Avoid routes/times where congestion or delays may occur.
 - Avoid routes that are remote and away from the "beaten path".
 - Vary the routes used.
- Times of Movement: Vary the times of day the funds are transported.
- Preparation
 - Ensure the transport vehicle is in good working condition.
 - Have two employees escort the funds, one to drive, one to act as observer.
 - Have a cellular telephone or radio to communicate with the DRMS field activity office or host security Desk Sergeant in case of trouble or emergency.
 - Notify activity management and the host security Desk Sergeant of the movement of the funds. Provide a description of the employees, transport vehicle, and the route used. Do not tell police exactly how much money is being transported.
 - Be observant for persons who may be watching the departure. If employees are uncomfortable, do not transport money and request police assistance.
 - Don't carry funds in a bank envelope. Use a briefcase or some other bag that will not draw attention.
- Enroute
 - Store money out of sight, i.e., trunk, glove compartment, etc. The trunk is preferable.
 - Be observant to problems.
 - Avoid congestion or anything that may cause delay, adjust the route if necessary but inform the activity or Desk Sergeant via radio if route is altered.
 - Stop only for traffic signals or police instructions.
 - In case of actual robbery attempt, comply completely with robber's instructions and follow host anti-robbery protocol.
- At Financial Activity
 - Be observant for suspicious person(s). If uncomfortable, do not stop. Go to a police station or other safe place. Plan ahead for such an eventuality.
 - Notify the DRMS field activity office and Desk Sergeant when funds have been transferred successfully (accepted at the financial activity).

g. Robbery Prevention Planning

- Ensure that all cashiers (primary and alternate) are thoroughly familiar with host installation anti-robbery plans. Specifically, they must know:
 - Actions to be taken by fund handling activity employees
 - Actions to be taken by the security force.
 - Actions to be taken by the supporting law enforcement agency or agencies.
 - Agencies and officials to be notified and the individual, by position, responsible for the notification.
 - All required reports.
- All needed supplements to host-antirobbery procedures will be coordinated with host security officials.
- DRMS field activity participation in host installation robbery response exercises is strongly encouraged.
- Take the following preventive measures at the DRMS field activity:
 - Be alert for and carefully observe any persons loitering in the vicinity of the cashier area. Challenge unidentified personnel.
 - Keep cash on hand to the minimum required to conduct efficient business.
 - Remove and secure all cash, checks and negotiable instruments from counters, desks and tables whenever you leave your work area.
 - Prior to departure at the close of business each day, inspect the area to ensure that safes, windows, doors and other access points to the cashier area are locked.
 - Post Suspect Height Chart, DRMS Form 1992, and anti-robbery checklists and visual aids inside the cashier area. Post a copy of the host anti-robbery plan or checklist within the cashier area.
 - Request annual training on host anti-robbery procedures for all cashiers.
- Employee Conduct During and After a Robbery. Employees during and after a robbery should take the following actions. If any of these procedures conflict with host procedures, the host procedures will apply:
 - Avoid actions that might increase danger to you or others.
 - Activate the robbery duress alarm system if it appears that such activation can be accomplished safely.
 - Observe the robber's physical features; voice, accent, mannerism, dress, the kind of weapon he has, and any other characteristics that would be useful for identification purposes.
 - If the robber leaves evidence (such as a note), try to put it aside and out of sight if it appears that this can be done safely. Retain and protect the evidence, do not handle it, and give it to the security police when they arrive.
 - Refrain from touching, and assist in preventing others from touching articles or places the robber may have touched or evidence he may have left, to preserve fingerprints of the robber. Protect the scene from disturbance.

DRMS-I 4160.14, Volume I, Chapter 2

- Give the robber no more money than the amount he demands and include "bait" money in the amount given ("bait money" consists of a serially recorded packet of paper money inconspicuously banded or clipped for identification purposes).
- If it can be done safely, observe the direction of the robber's escape and the description and license plate number of the vehicle used, if any.
- Telephone the security office or inform a designated officer or other employee who has this responsibility that a robbery has been committed. Give the security force dispatcher all available information; i.e., your location, description of the robbers and the vehicle, and the escape route.
- If the robber leaves before the security police arrive, assure that a designated officer or other employee waits outside the office to inform the security police.
- Attempt to determine the names and addresses of persons who witnessed the robbery or the escape and request them to record their observations or to assist a designated officer or other employee to record their observations.
- Refrain from discussing the details of the robbery with others before recording the observations. This will assist in keeping the memory clear of distractions.

5. Precious Metals

a. Display. Provide security for precious metals bearing materials consistent with the value of the expected precious metals recovery. See DRMS-I 4160.14, Volume VIII, Chapter 5 for requirements for storage of specific precious metals SCLs. Whenever possible, store all precious metals in inside display areas. Store all fine precious metals in a pilferable storage area within a safe, locked metal container, or locked conex container. All prescribed key control procedures apply to safe combinations; combination and/or key operated locks used to secure precious metals containers.

b. Employee Access. Limit entry to the locked container where fine precious metals are stored to the precious metals monitors (primary and alternate) designated by the DRMS field activity Chief. List monitor names as such in lock and key accountability records and on Standard Form 700 if a safe is used. Restrict entry to precious metals processing areas to employees with assigned duties in that area.

c. Fine Precious Metals. Weigh all fine precious metals (V-coded SCLs) on receipt in the presence of the generating activity's representative. Annotate the receiving document with the date, printed names and signatures of the parties involved. Accomplish all further handling of fine precious metals by the precious metals monitors in the presence of one witness. Annotate any additional documentation with the date, printed names and signatures of all parties involved.

d. Reports of Discrepancy (RODs). If the activity receives a ROD concerning a precious metals shipment of any kind, respond within 21 calendar days. Information copies of the activity response will be provided the DRMS Command Security Office.

6. Small Arms

a. Store complete weapons, weapon receivers, and barrels when attached to receiver assemblies, which contain the weapon's serial number in approved arms room facilities according to DoD 5100.76-M, Chapter 4. These facilities require the designation of "Restricted Area" by the host installation commander. Refer to DLA I 5710.1, Paragraph E3n (1)(h) for security procedural guidance.

b. Inventory. If the DRMS field activity has accountability of small arms conduct a monthly inventory, by serial number, of all small arms not in bulk or crated display. Inventory weapons, which remain in inventory in bulk display for more than 1 year annually by type and number based on count of sealed containers. Open five percent of the bulk stored containers annually and check 100 percent of the arms stored in the opened

containers by serial number. Both monthly and annual inventories may be accomplished by the host activity, if stored in host activity facilities, when such inventory requirements are included in the ISA or other local agreements. Any evidence of tampering or attempted entry into the sealed container is cause for a complete serial number verification of weapons in that container and notification of the DRMS Command Security Office. A written record of the most recent monthly or annual inventory will be maintained by the DRMS field activity for a minimum of 2 years, and in accordance with DLAR 7510.3, Control of Small Arms by Number. Military Assistance Program (MAP) small arms not stored on an U.S. installation are exempt from the provisions of this paragraph.

c. Small Arms Parts. All undemilitarized bolts, trigger assemblies, and barrels not attached to a receiver assembly, which contains a weapon's serial number, will be stored in the DRMO security cage. When a DRMO security cage is inadequate, the host will store those parts.

d. Demilitarization Security. Transportation of small arms and subparts will be in accordance with DoD 5100.76M, Chapter 7. Similarly, the DRMO Chief is responsible for assurance that small arms parts removed from the DRMO security cage are under constant DRMO surveillance until DEMILLED and any UNDEMILLED parts are returned to the DRMO security cage at the close of the business day.

7. Security Surveys/Vulnerability Assessments/Periodic Security Review (PSR). Purpose of the PSR is to evaluate compliance with the minimum physical security standards identified in this chapter, to identify conditions in DRMS field activity operations potentially subject to criminal exploitation, and to observe existing crime prevention practices utilized by the DRMS field activity staff. DRMS Office of Command Security personnel will conduct PSRs once every 3 years. When funding, scheduling, or other operational problems preclude accomplishment of the mandatory 3-year visits, DRMS Office of Command Security personnel will request the assistance of host asset protection officials in conducting physical security reviews of the affected facilities. To ensure uniformity in the reviews, DRMS Office of Command Security personnel will provide reviewing officials with checklists identifying the minimum physical security requirements of this chapter. Office of Command Security personnel will perform antiterrorism vulnerability assessments (VAs) of the DRMS field activity in conjunction with the PSR.

8. Classified Materials. DRMS field activities are not authorized to receive, process, or store classified material. Discovery of classified documents, usable property, or scrap in activity custody creates a security incident because of the potential for compromise of classified information/technology once the document or item left authorized channels. Consequently, each security incident requires immediate attention and continued follow-up until custody is regained by properly cleared authority and the material is removed from the DRMS field activity. Corrective action is initiated by protecting further potential for compromise and concluded by return of the material to the generator or to the temporary control of the host installation security manager. For detailed procedures to be followed when classified or possible classified material is identified or discovered within the disposal system are found (see DRMS-I 4160.14, Volume VII, Chapter 2).

9. ADP Security. DRMS Field activities will ensure that all ADP and information systems receive proper protection. Comply with the provisions of DLAR 5200.17, DRMS-D 5210.1, and other DRMS 5200/5210 series publications.

10. Security Force Protection. Should the DRMS field activity require a continuing armed or unarmed security force presence, refer to DLA I 5710.1, Paragraph E5.

F. FORCE PROTECTION

1. Department of Defense employees, military and civilian, physical assets, and facilities have been attacked before, and will continue to be targeted by terrorists and criminals. During the past 30 years, over **600** DoD personnel have been killed, and many more injured as the result of terrorist activities. Terrorists have used a wide variety of tactics in order to achieve their goals; tactics that have proven to kill, maim, intimidate. ***The events of September 11, 2001 indicate that terrorists can and will aggressively attack U.S. commercial and military targets, with high "body counts" as their goal. Non-traditional methods or attack such as chemical-biological or cyber-attacks are also likely in the future.*** Terrorists attack targets of opportunity as well as "soft" targets. They don't always target critical military or government assets to achieve their goals.

DRMS-I 4160.14, Volume I, Chapter 2

DLA and DRMS field activity employees and assets are not immune from terrorist activity, either domestic or foreign.

2. DRMS activities tenant on DoD facilities, in GSA-leased spaces, or in other facilities not under their control, whether CONUS or OCONUS, receive their antiterrorism protection from their host. DRMS field activities that are tenants must meet the requirements outlined in this instruction to the maximum extent possible and activity chiefs remain responsible for ensuring that the support provided by their host is adequate to protect the personnel, facilities, and resources under his/her control from acts of terrorism. Activities that are not a tenant on military installations will receive necessary support in coordination with the DRMS Command Security Office. All disputes with the host must be promptly elevated up the chain of command for resolution.

3. In order to carry out these responsibilities, activity Chiefs will as a minimum, accomplish the following:

a. Maintain a current threat statement. This will include the DRMS Threat Statement; unclassified host threat statements, and internally developed threat data. This information will be applied to the protection of human and physical assets at the DRMS field activity. Review threat statements annually or when the threat changes.

b. Establish and maintain a close liaison with host officials to ensure timely receipt of intelligence information as it applies to the protection of the DRMS field activity. When information is received, take appropriate measures in coordination with host force protection officials and the DRMS Command Security Office. NOTE: Only unclassified intelligence information may be provided to the activity. Refer providers of classified intelligence information to the DRMS Command Security Office. Ensure that the DRMO is incorporated in the installation **FPCON** notification matrix and that DRMO employees are aware of actions mandated by host installation **FPCON** protocols.

c. Continually identify activity assets, and vulnerabilities of those assets against terrorist tactics. This is accomplished by close communication with host antiterrorism/force protection (AT/FP) officials, review of previously conducted vulnerability assessments, and emergency drills and exercises.

d. Ensure that Antiterrorism/ Force Protection needs and requirements are addressed in the activity budget.

e. Maintain necessary physical protective measures for activity infrastructure and facilities.

f. Ensure appropriate emergency reaction plans are in place. These normally are host installation plans; however, they may be supplemented as necessary by the activity.

g. Train activity employees on responsibilities during emergencies. Exercise emergency plans routinely.

h. Ensure the DRMS field activity is integrated in host antiterrorism plans. Train employees on activity and owner/user responsibilities as outlined in the plan.

i. Participate in host antiterrorism working groups, committees, and other formal activities. Provide the host AT/FP officer with the name of an activity point of contact for antiterrorism matters.

j. Ensure that formal agreements are in effect with the host for all required antiterrorism/force protection support. Notify the DRMS Command Security Office promptly of shortfalls or disputes with host over requirements or activity needs.

k. Implement the DLA Combating Terrorism Program at the respective DRMS field activity and subordinate units.

4. Emergency Plans and Exercises.

a. Each DRMS field activity must possess current working plans (usually host plans) that address as a minimum, the following scenarios:

- Fire

- Armed Assault (robbery, workplace violence, etc.)
- Bomb Threats
- Bomb Detonation
- Hostage Situations
- Chemical/Biological agent dispersal
- Mass Casualty
- Natural Disasters (common to the locality)
- Country Noncombatant Evacuations (OCONUS Only)

b. Plans should provide for:

- Notification of emergency response personnel.
- Notification of activity employees and visitors.
- Evacuation procedures. Gathering/Rally Points.
- Response to incident by security and emergency personnel.
- Employee roles and responsibilities.
- Isolation of incident.
- Reporting requirements.

c. Plans do little good if they are not effectively and routinely exercised. Activities must exercise their fire plan and two other scenarios yearly. Mass-casualty exercises and response to terrorist activity are highly desired. Make every effort to get involved in the planning and conduct of exercises that are the purview of the host installation. It is not necessary to always have an "installation-wide" exercise involving the activity. Smaller scale exercises involving host security fire response, and medical services are in many ways just as effective. Involve all employees in exercises.

d. Exercises should be as realistic as possible. It is not always possible to have 100% response and participation from all host agencies tasked under the variety of plans; however, observers and controllers from those agencies may be available to assist in the conduct of activity emergency exercises and in documenting lessons to be learned. DLA Form 1827 is available for this purpose. Records of exercises must be maintained for a minimum of 3 years. Safety must be a primary concern. When exercising, do nothing to jeopardize the safety of activity employees or visitors. A strict element of control must be present over all exercises.

e. Actual (real-world) activation of any emergency plan requires SITREP initiation as soon as time allows. If computer information systems are effected, telephonic or facsimile reporting is mandated.

5. Standards. In addition to security standards as listed previously in this chapter and in DLA I 5710.1, the following prescriptive standards are established to specifically address the threat of terrorism at DLA and DRMS activities.

a. Maintain positive access control measures to prevent intrusion by unauthorized personnel.

DRMS-I 4160.14, Volume I, Chapter 2

b. If the DRMS field activity has been determined to be vulnerable to vehicle bombs, comply with the following in order to provide at least a "low level of protection" against the potential effects of a vehicle bomb.

(1) Use Army TM 5-853, Volumes I (Security Engineering Concept Design) and 2 (Security Engineering Project Development) in order to determine required standoff distances or facility hardening techniques. These documents also provide "engineering solutions" to a wide variety of terrorist tactics.

(2) Keep all unsearched vehicles at a minimum distance as prescribed by the design-based threat; consistent with the manuals listed in the preceding paragraph. NOTE: This will normally be determined during the vulnerability assessment performed at the DRMS activity. If this distance is not possible due to a wide variety of factors, apply appropriate and reasonable compensatory measures.

(3) Activities unable to meet standoff distance requirements due to facility location, adjacent streets, parking areas not under their control, etc., will implement compensatory measures to mitigate the threat of a vehicle bomb. Some actions include:

- Conduct random searches of vehicles entering the area with mandatory searches of all vehicles when the threat rises.
- Monitoring of the standoff zone via CCTV.
- Where adequate standoff distance cannot be gained, blast resistance must be provided for glazed surfaces on buildings housing DRMS employees. For new construction, use laminated glass. For existing structures, install a minimum of 4-mil fragment retention film.

(4) Negotiate with host officials to achieve the appropriate standoff zone around DRMS buildings/areas. Unresolved disputes will be elevated to HQ DLA Command Security Office through command channels.

c. Placed Explosives. Apply protective measures to protect against the explosive effects of a 50 lb. explosive device.

(1) Create an **unobstructed space** around occupied facilities of at least 33 feet.

(2) Move all trash receptacles and ashtrays out of the exclusion zone.

(3) Remove landscaping and other objects that may be used to conceal explosives.

(4) Allow no obstacles within the exclusive standoff zone that would conceal an explosive device. Ensure that gutters, windowsills, doorways, sewer grates, etc. are considered and modified to prevent concealment of a device.

(5) Train employees to be alert for suspicious items, conditions, persons, vehicles, and what to do if they encounter something.

d. Train employees who receive mail and packages to recognize characteristics of mail bombs. Training should be conducted annually. Host mailroom or US Postal Service officials are available to provide this training.

e. Develop procedures covering the visual inspections of mail and package. Discourage or prohibit the receipt of personal mail.

f. Ensure that the host installation has the capability to x-ray mail and packages that are destined for the DRMS field activity.

g. All DRMS field activities will employ separate notification systems and evacuation procedures for fire evacuations, bomb threat evacuations and chemical or biological threats. Each event must be addressed

separately. A primary and at least one alternate gathering area/rally point will be established. These points must be alternately used in order to reduce the vulnerability to secondary explosions.

6. New Construction/Renovations/Relocation

a. All new construction and renovation plans must be reviewed for antiterrorism concerns. DoD directives and HQ DLA policy requires a security review of all such plans at all design phases. The DRMS Command Security Office will review such plans by preparing a threat assessment IAW with the Army TM 5-853 Volumes 1 and 2 and determining appropriate construction standards to deter and prevent damage from a terrorist attack. All recommendations will be made in writing. **DRMS Facilities and Engineering (DRMS-RW) will secure Command Security coordination on all construction projects.**

b. The DRMS AT/FP Officer will develop a prioritized list of AT/FP factors to be considered by site-selection teams prior to the relocation of any DRMS activity. The site-selection team to determine if the proposed facility provides adequate protection against terrorist attacks will use these criteria.

7. Training. All employees must be trained on a regular basis concerning self-protective measures against terrorists.

a. All employees must receive Level I Antiterrorism Awareness Training from a qualified AT/FP officer, **at the intervals and the content as prescribed in DoD Instruction 2000.16, DoD Standard 22..** For those employees assigned outside the continental United States, Level I training will also include Area of Responsibility (AOR) specific training requirements established by the theater Commander in Chief.

b. **In addition to the requirement listed in the previous paragraph,** employees selected for OCONUS duty (TDY or PCS) must receive an **AOR-specific** update from qualified host AT/FP or intelligence officials within **three (3)** months prior to travel. Adult family members accompanying employees PCS must also receive this briefing. The briefing must meet the content requirements as outlined in **DoD Instruction 2000.16, DoD Standard 22..**

c. Employees must also be trained on local antiterrorism and emergency policies and procedures.

d. **Provisions for the above training must be included within the ISSA or MOU/MOA's with host installations.**

8. **FORCE PROTECTION CONDITIONS (FPCONS).** The DoD **Force Protection** Condition System (**FPCONS**) describes the progressive level of protective measures implemented by all DoD components in response to terrorist threats. The local installation commander or higher headquarters direct the implementation of specific **FPCONS** in response to intelligence or information received, indicating a threat against installation facilities or personnel. The DRMS field activity will comply with **all tasked host installation FPCON measures,** when responding to threats against installation facilities, assets and personnel. **Notify DRMS HQ via SITREP of FPCON elevation. When FPCON is reduced by order of installation commander or other authority, make a follow-up SITREP.**

a. **FPCON** NORMAL: This **FPCON** exists when a general threat of terrorist activity exists, but warrants only a routine security posture. These are measures taken on a normal, day-to-day basis, and provide the necessary foundation for expanding into increased threat conditions.

- b. **FPCON** ALPHA: This **FPCON** applies when there is a general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable, and circumstances do not warrant full implementation of FPCON BRAVO measures. The measures in this FPCON must be capable of being maintained indefinitely.

c. **FPCON** BRAVO: This **FPCON** is implemented when an increased and more predictable threat of terrorist activities exists. These measures must be capable of being maintained for weeks without causing undue hardships, without affecting operational capability, and without aggravating relations with local authorities.

d. **FPCON CHARLIE**: This **FPCON** is declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations or personnel is imminent. Implementation of this FPCON for more than a short period of time will probably cause hardships and affect the peacetime activities of the organization and its personnel.

e. **FPCON DELTA**: This condition applies in the immediate area when a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this condition is declared as a localized condition.

9. Vulnerability Assessment Protocols

a. Each DRMS field activity will receive an antiterrorism vulnerability assessment (VA) at least once every three years. Representatives from the DLA or DRMS Command Security Office and US Army Corps of Engineers will conduct the VA. **Normally, the DLA Command Security Office will conduct assessments for all OCONUS sites, and the DRMS Command Security will assess CONUS sites. The DRMS Command Security Office will conduct a compliance-oriented security review in conjunction with the VA.**

b. The VA's will review the following areas:

- Physical Security
- Electronic Security Systems, as applicable
- Law Enforcement Liaison and Intelligence Support
- Disaster Preparedness and Vulnerability to a Threat
- Force Protection Plans and Programs
- Plans and Support
- Resources
- Training
- Site-Specific Issues and Concerns

c. The activity Chief will be required to assemble pertinent documents and/or obtain information necessary to conduct the VA. The following tasks should be completed prior to the arrival of the VA Team.

(1) Develop a Prioritized Asset List, with a brief description of each asset. Prioritization should be based upon critically to the military mission and activity's mission. Generally this list will include activity employees and information systems.

(2) Communicate with host AT/FP officials to determine aggressor likelihood for each asset on the Prioritized Asset Listing by determining the following for each of these aggressors:

- Criminals
- Vandals
- Extremist protectors
- Saboteurs

- Terrorists.

(3) This information is to be used to determine asset vulnerabilities and subsequent recommend courses of action to mitigate those vulnerabilities. This information will include:

- Profile of asset to the aggressor (how well known is the presence of the asset to the aggressor).
- Usefulness of the asset to the aggressor.
- Availability of the asset outside the activity.
- Past incident involving attempts to compromise similar assets both locally and nearby.
- Potential for future incidents.
- Accessibility to the asset (stored in open, inside buildings, in a vault, etc.).
- Effectiveness of responsible law enforcement agency.
- Any site specific threat information.

(4) Communicate with host AT/FP officials concerning asset vulnerability against the following terrorist tactics.

(a) Vehicle bombs.

(b) Explosive devices placed either inside a building containing assets or placed on the exterior of buildings containing assets.

(b) Ballistics attack.

(c) Mail or supplies bombs.

(d) Forced entry.

(e) Covert entry.

(f) Insider compromise.

(5) Assemble or create the following documents:

(a) Activity budget

(b) Mail and Package screening procedures.

(c) Current installation threat statement(s) (unclassified).

(d) Procedures for vehicle and pedestrian access control procedures for gaining access to the DRMS field activity and installation.

(e) Host procedures for Intelligence information dissemination to the activity.

(f) Procedures for activity and/or host response to emergencies.

(g) As applicable, listing of internal guard posts and security patrols for each shift. (Activity internal only)

DRMS-I 4160.14, Volume I, Chapter 2

(h) Host AT/FP Plan, as supplemented

(i) Host Security Plan, as supplemented

(j) Host Emergency/Disaster Preparedness Plan, as supplemented

(k) Copies of all agreements for police services, force protection, fire protection, emergency services, and civil engineering/public works.

(l) Records of exercises of emergency procedures for the past three years.

(m) Records of funding levels and requests for funding for the past two years.

(n) Records of staffing levels and requests for additional staffing for the past two years.

(o) Current activity COOP, as prescribed by DRMS National (CONUS sites only)

(p) Three copies of the following engineer documents: (available through public works/civil engineering.

- Vicinity map showing the location of the activity with respect to the surrounding area.
- Scalable site plan of the installation or activity buildings, roads, parking, entrances, etc.
- Aerial photos (if available).
- Architectural floor plans showing space utilization, elevations, and sections of buildings housing assets.
- Structural floor plans, elevations, and sections of buildings housing assets showing typical construction.
- Drawings showing any electronic security systems (IDS, CCTV, access control, duress alarms, monitoring stations, etc.) related to the identified assets.
- Drawings showing any alternate power sources for security related equipment (UPS).

(q) Names/phone numbers of the following individuals.

- Installation AT/FP Officer
- Installation Law Enforcement Officer
- Installation Officer responsible for providing intelligence information concerning terrorist threats.
- Installation Disaster Preparedness/Emergency Services officer
- Installation Physical Security/Resource Protection Program Manager

d. Identify points of contact in the responsible civil engineering or public works organization that can provide additional engineering information.

e. Make all appropriate courtesy notifications to host and tenant agencies, (Installation Commander, AFOSI, USACIDC, NCIS, Security Forces/Security Police/Military Police, etc....)

f. Arrange for any necessary camera, vehicle or security passes for each VA team member.

10. Assessment Report Processing.

- a. The respective force protection officer will provide the activity chief/site manager with a written and oral outbrief at the conclusion of the assessment.
- b. Upon finalization of the report, it will be transmitted electronically in a secure means (PKI) to the DRMS National Support office, with a 60-day suspense. Reports on DRMS International activities will be provided in hardcopy.
- c. Activity chiefs will completely justify any non-acceptance of an assessment recommendation, with the understanding that the DRMS Commander decide whether or not the risk of non-acceptance will be taken.

d. At sites where a logistics contractor is present, any findings resulting from the VA or corrective action required by the contractor will be forwarded to the contractor through the COTR. The VA will be coordinated with the Logistics contractor management through the COR.