

**C4. SECURITY AND FORCE PROTECTION****TABLE OF CONTENTS**

C4. SECURITY AND FORCE PROTECTION .....	4-3
C4.1. General. ....	4-3
C4.1.1. Purpose. ....	4-3
C4.2. Definitions. ....	4-4
C4.3. Responsibilities. ....	4-4
C4.3.1. Director, DLA Disposition Services.....	4-4
C4.3.2. Site Director, DLA Installation Support at Battle Creek.....	4-5
C4.3.3. Chief, Security and Emergency Services, DLA Installation Support at Battle Creek Public Safety Branch.....	4-5
C4.3.4. AT/FP Officer (assigned to DLA Installation Support at Battle Creek, Security and Emergency Services.....	4-6
C4.3.5. DLA Disposition Services Area Managers/Field Activity Leaders.....	4-6
C4.3.6. DLA Disposition Services Area Manager/Field Activity Security Representatives .....	4-7
C4.4. Security Administration. ....	4-8
C4.4.1. Exceptions and Waivers.....	4-8
C4.4.2. Loss Prevention Program.....	4-9
C4.4.3. Security Awareness Training Program.....	4-9
C4.4.4. Security Support Requirements for Interservice Support Agreements (ISA)....	4-9
C4.5. Physical Security. ....	4-14
C4.5.1. Discussion.....	4-14
C4.5.2. Barriers.....	4-14
C4.5.3. Clear Zones.....	4-15
C4.5.4. Warning Signs.....	4-16
C4.5.5. Pilferable Storage.....	4-17
C4.5.6. Locking Devices. ....	4-19
C4.5.7. Protective Systems/Factors.....	4-20
C4.6. Procedures.....	4-21
C4.6.1. Lock and Key Control. ....	4-21
C4.6.2. Entry and Movement Control.....	4-24
C4.6.3. Pilferable Items. ....	4-30
C4.6.4. Safeguarding Funds.....	4-32
C4.6.5. Precious Metals.....	4-35
C4.6.6. Small Arms.....	4-36
C4.6.7. Classified Materials (edited Sep 2012) .....	4-37
C4.6.8. ADP (Information Technology) Security (edited Sep 2012).....	4-37
C4.6.9. Security of Hazardous Material / Hazardous Waste (edited Sep 2012) .....	4-37
C4.7. Force Protection.....	4-38
C4.7.1. Scope.....	4-38
C4.7.2. DLA Disposition Services Area Manager/Field Activity Leader Responsibilities (edited Sep 2012).....	4-38
C4.7.3. Emergency Plans and Exercises.....	4-40
C4.7.4. Antiterrorism Prescriptive Standards.....	4-41

C4.7.5. New Construction/Renovations/Relocation. .... 4-44

C4.7.6. Training. .... 4-44

C4.7.7. Force Protection Conditions (FPCONS)..... 4-45

C4.7.8. Security Program Review (SPR)/Vulnerability Assessment (edited Sep 2012). 4-45

C4.7.9. Security Program Review/Vulnerability Assessment Protocols  
(edited Sep 2012) ..... 4-46

C4.7.10. Assessment Report Processing (edited Sep 2012)..... 4-49

## SECTION 1 - ADMINISTRATIVE PROCESSING

### C4. SECURITY AND FORCE PROTECTION

#### C4.1. General.

**NOTE:** How To Notify The **DLA Disposition Services** Director About Urgent Incidents.

<<https://www.drms.dla.mil/gov/publications/suppdocs/urgentincidepdf>>

<https://dispositionservices.dla.mil/gov/publications/suppdocs/urgentincidents.pdf>

#### C4.1.1. Purpose.

C4.1.1.1. 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 **DLA Disposition Services** Field Activities worldwide.

C4.1.1.2. 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.

C4.1.1.3. 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 O-2000.12-H, DoD Antiterrorism Handbook; DOD Instruction 2000.16, DOD Antiterrorism Standards; applicable DLA Combating Terrorism directives, and the **most current** DLA Physical Security Guidebook **Manual**, undated. It applies to all **DLA Disposition Services** Field Activities and assigned employees and supersedes DRMS-I 4160.14, Section 1, Chapter 4, updated **October, 2010**. In case of conflicts with this chapter and higher headquarters (JCS/DoD/DLA) security policy, the higher headquarters policy will apply. **To the greatest extent possible, DLA Disposition Services sites in contingency areas will meet the requirements of this manual. However, field activity directors/site chiefs/supervisors in contingency areas must ensure that their facilities/operations are integrated into the host base' defense and force protection plans. In situations where the base command force protection or base defense guidance differ or contradict the DRMS-I 4160.14, the local security/force protection guidance will supersede DRMS-I 4160.14.** In case of conflicts between this chapter and military service policy, notify the **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** for assistance in resolution.

C4.1.1.4. The DLA Physical Security Guidebook **Manual** is the guiding directive for physical security at DLA Field Activities. **DLA Disposition Services** field activities will comply with the applicable requirements of that instruction **manual**. This chapter is intended to support the requirements outlined in that instruction **manual** wherever possible. ~~This chapter serves as the~~

~~DRMS field activity's basic physical security plan as outlined in DLA Physical Security Guidebook, Paragraph D2c DRMS Field Activities may supplement this directive as needed.~~

C4.1.1.5. Although procedures and protocols may need to vary from location to location based upon unique operating environments, the standards in this chapter must be applied

appropriately to each **DLA Disposition Services** field activity wherever **DLA Disposition Services** maintains physical custody of excess/surplus property or has personnel (government employees or contract employees) physically present. This may include locations where the operations is by OCONUS **DLA Disposition Services sites** or Receipt-In-Place locations (RIPLs), as well as Centralized Demilitarization ~~Centers~~ **Divisions** or Controlled Property ~~Centers~~ **Branches and Cross Docks**.

#### C4.2. Definitions.

See ~~Section 4, Supplement 1, Security, Enclosure 1~~ **DLA Physical Security Manual Appendix B for Security Definitions.**

#### C4.3. Responsibilities.

##### C4.3.1. ~~Commander, DRMS~~ **Director, DLA Disposition Services:**

C4.3.1.1. Has command responsibility for the safety of personnel and protection of Federal property under his/her control.

C4.3.1.2. Has overall responsibility for implementing DoD Combating Terrorism programs at all **DLA Disposition Services** activities worldwide. Ensures compliance by subordinate activities with applicable physical security directives.

C4.3.1.3. Assumes all risks involved with disapproval of all recommendations identified during Antiterrorism Vulnerability Assessments.

C4.3.1.4. Is responsible for the implementation of physical security measures designed to minimize the loss of supplies and equipment by natural or manmade hazards.

C4.3.1.5. Implements the DoD/DLA Combating Terrorism Program as outlined in DoD D 2000.12 at all CONUS and OCONUS subordinate activities.

C4.3.1.6. Ensures that all personnel under his/her control receive required Antiterrorism Awareness Training and Travel Briefings.

C4.3.1.7. 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 Combatant Command (COCOM) standards.

C4.3.1.8. Ensures that funding or FTE shortfalls for all ~~DRMS and DRMS field activities~~

**DLA Disposition Services** are appropriately addressed at the HQ, and if necessary, forwarded to HQ DLA.

C4.3.1.9. Ensures that all disputes with facility hosts, the General Services Administration (**GSA**), the Chief of Mission, or the COCOM, or other entities, regarding protection from terrorism for **DLA Disposition Services** personnel, are appropriately addressed at the HQ level and, if necessary, forwarded to HQ DLA for resolution.

C4.3.2. Site Director, **DLA Installation Support at Battle Creek.**

C4.3.2.1. Ensures that the functional organization of the activity includes a Security Manager and that the organizational placement of the Security Manager does not hinder accomplishments of the security mission.

C4.3.2.2. 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.

C4.3.2.3. Administers the DoD Antiterrorism Program on behalf of the **DLA Disposition Services Director**.

C4.3.3. Chief, Security and Emergency Services, **DLA Installation Support at Battle Creek.**

C4.3.3.1. Functions as the technical subject matter expert and principal advisor to the ~~Commander~~ **Site Director** on all matters pertaining to physical security, antiterrorism, and force protection (AT/FP) issues.

C4.3.3.2. Provides oversight and management of the overall command security program; to include physical security, ~~information security, personnel security,~~ and other duties as required.

C4.3.3.3. Conducts periodic reviews and inspections of **DLA Disposition Services** field activities to ensure compliance with applicable regulations, directives, and instructions.

C4.3.3.4. 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.

C4.3.3.5. Serves as DLA Disposition Services, Security and Emergency Services ~~DES-  
Public Safety Division~~ Representative on various boards and committees.

C4.3.3.6. Implements the DLA Loss Prevention Program.

C4.3.3.7. Provides security education and training material to **DLA Disposition Services field activities**. Develops training modules for usage in security education program.

C4.3.3.8. Provides analysis of **DLA Disposition Services** security deficiencies and recommendations.

~~C4.3.3.9. Formulates and administers security education and training programs for all DRMS employees.~~

C4.3.3.9. Reviews all portions of this instruction at least annually.

C4.3.4. AT/FP Officers **DLA Installation Support at Battle Creek, Security and Emergency Services Branch**: (assigned to ~~DES Battle Creek, Public Safety Branch~~):

C4.3.4.1. Implements the Combating Terrorism Program at HQ **DLA Disposition Services and DLA Disposition Services** field activities as outlined in applicable Combating Terrorism directives.

C4.3.4.2. Provides oversight in the implementation of approved antiterrorism measures at HQ **DLA Disposition Services and DLA Disposition Services** field activities to include, where applicable, negotiation with facility hosts, the General Services Administration (**GSA**), or Chief of Mission to implement recommended Antiterrorism measures.

C4.3.4.3. Conducts **Security Program Reviews Vulnerability Assessments** at all **DLA Disposition Services CONUS** 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 **DSD FST** and facility heads.

C4.3.5. **DLA Disposition Services Area Manager/Field Activity Leaders**:

C4.3.5.1. 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.

C4.3.5.2. Ensure compliance with this chapter within their facilities.

C4.3.5.3. Ensure that individual employees safeguard government property in their charge and comply with the provisions of this chapter.

C4.3.5.4. Have responsibility for the safety of employees and protection of Federal property, to include subordinate operating locations.

C4.3.5.5. Execute the DLA Loss Prevention Program.

C4.3.5.6. Ensure security requirements are identified in the activity budget.

C4.3.5.7. Implement physical security measures designed to minimize the loss of supplies and equipment by natural or manmade hazards.

C4.3.5.8. Act as incumbent or appoints a Security Coordinator (in writing).

C4.3.5.9. Provide **DLA Installation Support at Battle Creek** Public Safety Branch immediate notification of any terrorist incident discovered within or reported to the **DLA Disposition Services** field activity.

C4.3.5.10. Ensure that the **DLA Disposition Services** field activity is integrated into host security, antiterrorism and emergency reaction plans.

C4.3.5.11. Submit a **DLA Disposition Services** situation report (SITREP) when host or other investigative agencies initiate security or criminal incidents, criminal investigations, and security surveys involving the **DLA Disposition Services** field activity or any requests for information by any law enforcement agency.

C4.3.5.12. 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.).

C4.3.5.13. Maintain installation plans for antiterrorism, force protection, and emergency response/disaster preparedness. Be knowledgeable of DLA Disposition Services taskings outlined in these plans.

C4.3.5.14. At sites where a 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 Contracting Officer's Technical Representative (COTR).

C4.3.5.15. Ensure **DLA Disposition Services** Inspection Log CAMS Version is completed as required.

C4.3.6. **DLA Disposition Services** Field Activity Security **Representatives** Coordinators:

C4.3.6.1. Administer the activity's antiterrorism and physical security programs, in accordance with this chapter, and other appropriate directives. Reports directly to **DLA Disposition Services Area Manager**/field activity leader for all security/antiterrorism matters.

C4.3.6.2. Assist the **DLA Disposition Services Area Manager**/field activity leader in discharging their security responsibilities by analyzing security deficiencies and hazards and making recommendations for appropriate corrective action.

C4.3.6.3. Maintain and supplement (as necessary) host physical security, antiterrorism and emergency plans. When the **DLA Disposition Services** 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** for assistance as needed.

C4.3.6.4. Develop and maintain a security file composed of copies of all documents of

security interest to the **DLA Disposition Services** field activity. Maintain the security file as an individual information file or incorporated into an existing **DLA Disposition Services** 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:

C4.3.6.4.1. Most recent physical security assessments conducted by **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** and host security agency, with report of corrective actions and **supporting documents**.

C4.3.6.4.2. Approved security waivers and exceptions.

C4.3.6.4.3. Security **Representative** coordinator and key control officer and other Security related appointments, as applicable.

C4.3.6.4.4. 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 **DLA Disposition Services** field activity only requires those portions of host plans that outline **DLA Disposition Services** field activity taskings when the plan is implemented.

C4.3.6.4.5. Host emergency response/disaster preparedness/consequence management plan, supplemented as necessary.

C4.3.6.4.6. Training documentation and material.

C4.3.6.4.7. Documentation of emergency and security exercises.

C4.3.6.4.8. Miscellaneous other security correspondence.

C4.3.6.5. 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** for assistance.

C4.3.6.6. Participate in, and communicate security-related information and concerns during **DLA Disposition Services** field activity staff meetings.

C4.3.6.7. Disseminate crime prevention information and encourage active participation by all **DLA Disposition Services** field activity employees in observing and reporting criminal activities, and security deficiencies.

#### C4.4. **Security Administration.**

C4.4.1. Security Exceptions and Waivers.

C4.4.1.1. See DLA Physical Security Manual, Chapter 16.

C4.4.1.2. ~~Established by this procedure and the DLA Physical Security Guide,~~ Unusual conditions or circumstances may exist at a DLA Disposition Services field activity, which necessitate deviation from ~~meeting regulatory security~~ these requirements. Compliance with a particular requirement may be impractical considering such factors as host mission and resources available to the activity. Each PLFA will use the DLA Form 1885 (May 2008) "Request for Deviation from Security Criteria" IAW with the DLA Physical Security Manual. This form is available on eWorkplace and is a .pdf, fillable form.  
<http://www.dla.mil/dss/forms/fillables/DL1885.pdf>

C4.4.1.2.1. Requests will be submitted to DLA Installation Support at Battle Creek, Security and Emergency Services Branch (DS-FBS) which will coordinate the request with DLA Disposition Services Command Office and DLA Installation Support via the PLFA Area Manager and Regional Disposition Services Director. Send completed requests to [BattleCreekForceProtection@dlamail.mil](mailto:BattleCreekForceProtection@dlamail.mil).

C4.4.2. Loss Prevention Program.

See DLA Physical Security ~~Guide~~ Manual, Chapter 4.

C4.4.2.1. ~~Methods of Obtaining Data:~~

C4.4.2.1.4. The DLA Disposition Services 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 the new system, which is web based, at <http://drmsweb.drms.dla.mil/SitRep>

C4.4.2.4.2. DD Forms 200 that is forwarded to DLA Disposition Services HQ for closure will undergo review by DLA Disposition Services J322.

C4.4.3. Security Awareness Training Program. See DLA Physical Security ~~Guide~~ Manual, Chapter 18.

C4.4.3.1. The DLA Disposition Services Area Manager/field activity Leader/Security Coordinator will maintain records of security awareness training sessions for 2 years. The DLA Installation Support at Battle Creek, Security and Emergency Services Branch during physical security program reviews ~~surveys~~ and assessments will review these records.

C4.4.3.2. Training materials and information are available from a variety of sources. Host security offices, public affairs offices, audiovisual libraries, the DLA Installation Support at Battle Creek, Security and Emergency Services Branch and the Internet are good places to look.

C4.4.4. Security Support Requirements for Interservice Support Agreements (ISA).

C4.4.4.1. The ISA with the host installation will set forth the specific police services and

other security related support to be provided for the **DLA Disposition Services** field activity. Each activity will try to secure the following services. In case the host declines to provide such service, contact the **DLA Installation Support at Battle Creek, Security and Emergency Services** Branch for guidance. Refer to **Section 4 – Supplements, Supplement 1-Administrative Processing, Enclosure 8 MOA for Disposal Services** section of the instruction for **ISA Security Support Requirements** following services are to be requested, consistent with the activity mission.

~~C4.4.4.2. Non-reimbursable: The following security support should be requested on a non-reimbursable basis for all **DLA Disposition Services** field activities as standard requirements at the time Inter-service Support Agreements with host military installations are initiated or renewed:~~

~~C4.4.4.2.1. Police Patrol:~~

~~C4.4.4.2.1.1 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 or breach of security.~~

~~C4.4.4.2.1.2 Receiver will: Secure activity facilities when not attended. Promptly secure and inspect facilities when notified if found unsecured. Comply with host external security criteria.~~

~~C4.4.4.2.2. Traffic Enforcement:~~

~~C4.4.4.2.2.1 Supplier will: Provide traffic supervision and enforcement to include investigation of traffic mishaps/accidents.~~

~~C4.4.4.2.2.2 Receiver will: Comply with host criteria.~~

~~C4.4.4.2.3. Investigations:~~

~~C4.4.4.2.3.1 Supplier will: Investigate all security/criminal incidents involving **DLA Disposition Services** 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 **DLA Disposition Services** Office of Compliance upon their completion.~~

~~C4.4.4.2.3.2 Receiver will: Promptly report all security/criminal incidents to host security/military police. Protect crime scene and evidence until host security/military police respond to the scene.~~

~~C4.4.4.2.4. Identification:~~

~~C4.4.4.2.4.1 Supplier will: Provide **DLA Disposition Services** field activity employees with security badges, ID cards, and/or vehicle decals required to access the activity work site(s).~~

~~C4.4.4.2.4.2 Receiver will: Comply with host requirements.~~

~~C4.4.4.2.5. Funds Escort:~~

~~C4.4.4.2.5.1 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.~~

~~C4.4.4.2.5.2 Receiver will: Request escorts and coordinate request in advance if possible. Comply with host criteria on movement of funds.~~

~~C4.4.4.2.6. Weapons Storage:~~

~~C4.4.4.2.6.1 Supplier will: Provide in transit security for weapons and major small arms subparts received or shipped by **DLA Disposition Services** field activity or host installation and provide custody for weapons on **DLA Disposition Services** 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.~~

~~C4.4.4.2.6.2 Receiver will: Request support and coordinate all such requests with the host installation in advance, if possible.~~

~~C4.4.4.2.7. Key Control:~~

~~C4.4.4.2.7.1 Supplier will: allow tenant **DLA Disposition Services** field activity autonomous control of all keys and locks used to secure activity facilities and assets.~~

~~C4.4.4.2.7.2 Receiver will: Maintain positive control of all keys and locks in accordance with **DLA Disposition Services** security criteria.~~

~~C4.4.4.2.8. Information Security:~~

~~C4.4.4.2.8.1 Supplier will:~~

~~C4.4.4.2.8.1.1 Provide tenant **DLA Disposition Services** field activity personnel with security awareness training.~~

~~C4.4.4.2.8.1.2 Secure any uncontrolled classified material discovered in **DLA Disposition Services** field activity assets and ensure that appropriate inquiries/investigations of all known and suspected security violations are conducted in accordance with DoD 5200.1-R.~~

~~C4.4.4.2.8.1.3 As needed, ship (at DLA Disposition Services cost) back to the generating activity. C4.4.4.2.8.2 Receiver will:~~

~~C4.4.4.2.8.2.1 Receiver will comply with DoD/DLA/host criteria.~~

~~C4.4.4.2.8.2.2 Assist host agency by providing all information needed for required inquiries/investigations.~~

~~C4.4.4.2.9. Force Protection:~~

~~C4.4.4.2.9.1 Supplier will:~~

~~C4.4.4.2.9.1.1 Provide a standard level of support for Force Protection (FP) in accordance with DoD D 2000.12, DoD I 2000.14, DoD I 2000.16, DoD I 2000.18 and O-DoD 2000.12-H. Responsibility to apply FP will be proactive and reactive to include the following:~~

~~C4.4.4.2.9.1.2 Provide timely unclassified threat intelligence and information sharing.~~

~~C4.4.4.2.9.1.3 Incorporate the receiver into the installation physical security, resource protection and emergency preparedness plans.~~

~~C4.4.4.2.9.1.4 Incorporate the receiver into the installation's AT/FP plan/directives.~~

~~C4.4.4.2.9.1.5 Provide with copies of applicable installation plans and directives.~~

~~C4.4.4.2.9.1.6 Advise of changes in FPCON in a timely manner.~~

~~C4.4.4.2.9.1.7 Provide annual Antiterrorism/Force Protection Awareness Training, and Level I travel briefings.~~

~~C4.4.4.2.9.2 Receiver will:~~

~~C4.4.4.2.9.2.1 Comply with host regulations, guidelines and directed actions.~~

~~C4.4.4.2.9.2.2 Provide the host FP officer with DLA Disposition Services field activity points of contact, telephone numbers, and e-mail addresses.~~

~~Reimburse the host for FP above and beyond the standard level.~~

~~C4.4.4.3. Reimbursable: The following security support should be requested for DLA-  
Disposition Services field activities on a reimbursable basis at the time the Interservice Support  
Agreements are initiated or renewed:~~

~~C4.4.4.3.1. Security Reviews and Inspection.~~

~~C4.4.4.3.1.1 Supplier will: Conduct physical security inspections of DLA-  
Disposition Services field activity facilities and operations as requested by the activity or DES-  
Battle Creek Public Safety Branch using as a minimum, DLA Disposition Services security  
criteria.~~

~~C4.4.4.3.1.2 Receiver will: Schedule the inspection at a convenient time.  
Promptly respond to all findings noted.~~

**C4.4.4.2. Additional Reimbursable ISA requirements not contained in Section 4-  
Supplements; Supplement 1-Administrative Processing, Enclosure 8-MOA for Disposal Services  
section are:**

**C4.4.4.2.1. Alarm Monitoring/Armed Response: (for activities with IDS or duress  
alarms).**

**C4.4.4.2.1.1. Supplier will: Include DLA Disposition Services field activity  
protected areas under an alarm monitoring system. Provide armed response within service-  
prescribed timeframes. Test alarms weekly.**

**C4.4.4.2.1.2. Receiver will: Provide Supplier with names of employees  
authorized to activate/deactivate/test alarms. Comply with Supplier alarm activation and testing  
criteria.**

**C4.4.4.2.2. Security Lighting:**

**C4.4.4.2.2.1. 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 activity security posture is in jeopardy.**

**C4.4.4.2.2.2. Receiver will: Request installation and maintenance of  
lighting fixtures as required. Ensure lighting is extinguished during hours of daylight.**

**C4.4.4.2.3. Emergency Repairs:**

**C4.4.4.2.3.1. 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.**

**C4.4.4.2.3.2. Receiver will: Request support promptly when defect/deficiency is  
identified.**

**C4.4.4.3. Contract Security Service. When adequate security service cannot be**  
Section 1, Chapter 4

provided by the host installation, **DLA Disposition Services Area Managers**/field activity leaders may, through **DLA Installation Support at Battle Creek, Security and Emergency Services** Branch coordination, contract protective services from commercial sources.

C4.4.4.4. 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 **DLA Disposition Services** activities

and personnel, consistent with support provided to other DoD service providers and other DoD tenants on the installation. **Refer to Section 4-Supplements, Supplement 1-Administrative**

**Processing, Enclosure 8-MOA for Disposal Services** section of this instruction or contact the **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** for assistance with verbiage.

**NOTE:** At RIPL sites where a 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.

## C4.5. Physical Security.

### C4.5.1. Discussion.

C4.5.1.1. In order to protect and secure **DLA Disposition Services** 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 will request either an exception or a waiver for those specific areas of noncompliance. Exceptions and waivers are detailed in Section 1, Chapter 1 – Administration, this instruction. Commercial Venture partners who operate out of **DLA Disposition Services** activity locations will comply with the requirements of this instruction and chapter.

### C4.5.2. Barriers.

C4.5.2.1. See DLA Physical Security Guide, **Manual, Chapter 3.**

~~C4.5.2.2. Physical barriers may deter accidental or deliberate encroachment on DLA Disposition Services 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 DES Battle Creek Public Safety Branch based upon recommendation of the activity chief and local environmental risk factors.~~

#### ~~C4.5.2.3. General Requirements.~~

~~C4.5.2.3.1. Inspect 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 DLA Disposition Services SITREP immediately. In 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. Damage weaknesses or deficiencies must be promptly reported to the host facility engineer for correction.~~

~~C4.5.2.3.2. 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.~~

#### ~~C4.5.2.4. Barrier Openings.~~

~~C4.5.2.4.1. 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 DLA Disposition Services 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.~~

#### C4.5.3. Clear Zones.

See DLA Physical Security **Manual, Chapter 3. Guide, Paragraph D3a(8).**

C4.5.3.1. 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, a 20-foot clear zone is desired. For parking restrictions see paragraphs C4.6.2.3.1.1 and C4.7.4.3.1.1 below. **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. As a minimum, the clear zone shall extend 20 feet on the outside and between 5 and 30 feet on the inside of the perimeter barrier.**

**C4.5.3.1.1. Trash receptacles located within the clear zone shall be a minimum of 12 feet from buildings and storage areas to provide a low level of protection. Standoff distances will be met based on the conventional construction standoff distance (Table B-2-UFC 4-010-01) based on the specific construction of the walls and whether they are load bearing or not of the facility.**

#### C4.5.3.2. Exemptions.

C4.5.3.2.1. 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.

C4.5.3.2.2. 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.

C4.5.3.2.3. **DLA Disposition Services** field activities may request exemptions for permanent structures within the exterior clear zone **by submitting photographs upon request and submission of photographs**; facility plans or sketches to the **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** documenting the degree of

**encroachment on the clear zone**. See this chapter; paragraph C4.4.1 for procedures pertaining to waiver submission.

C4.5.3.2.4. It is the responsibility of the **Area Manager/field** activity leader 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 **Area Manager/field** activity leader must ensure that any proposed construction within the yard does not violate field activity interior clear zone requirements.

#### C4.5.4. Warning Signs.

**Refer to DLA Physical Security Manual, Chapter 10, Paragraph G.**

C4.5.4.1. 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. **In addition to the requirements identified in the DLA Physical Security Manual, the following standards apply:**

##### C4.5.4.2. Display:

C4.5.4.2.1. 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.

C4.5.4.2.2. 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.

C4.5.4.2.3. Used in conjunction with tapes, ropes, chains or other cordon material to delineate areas within **DLA Disposition Services** field activity boundaries where access is temporarily or permanently denied to all except **DLA Disposition Services** field activity employees.

C4.5.4.2.4. Affixed to the perimeter barrier or staked in the ground if no barrier exists. When host installation perimeter coincides with a portion of **DLA Disposition Services** field

activity boundary, use host warning signs on that portion of the **DLA Disposition Services** field activity perimeter.

C4.5.4.3. 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.~~

~~C4.5.4.3.1. Worded as "WARNING - AUTHORIZED PERSONNEL ONLY"~~

~~C4.5.4.3.2. Lettered to be easily readable from 50 feet. Use light reflective materials if available.~~

~~C4.5.4.3.3. 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.~~

C4.5.4.3.1. Worded bilingually 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.

~~C4.5.4.3.5. DRMS Form 1988, DRMO Warning Sign, is suitable for this purpose.~~

~~C4.5.4.4. When **DLA Disposition Services** field activity boundaries form part of a military installation perimeter, installation warning signs must be posted in accordance with service and host policy.~~

C4.5.4.3.2. For areas officially designated by an installation commander as "restricted" or "controlled", refer to the DLA Physical Security **Manual Guide**, Paragraph D3b G for proper signage requirements.

C4.5.5. Pilferable Storage.

**Refer to DLA Physical Security Manual, Chapter 4.**

C4.5.5.1. Each **DLA Disposition Services** 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 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 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.~~

#### C4.5.5.2. Construction Criteria.

C4.5.5.2.1. 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 above will apply.

C4.5.5.2.2. Cage panel mounting hardware (screws, nuts, bolts, etc.) should not be exposed to the exterior of the facility. If mounting hardware is exposed and/or accessible, they will be security hardware which requires special tools, spot welded, peened, covered, or filled with material in a way to prevent easy removal and provide a delay factor requiring use of special burglary tools.

C4.5.5.2.3. Cover windows and vents with a material that provides a deterrent equal to or greater than the rest of the structure.

C4.5.5.2.4. 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.

C4.5.5.2.5. Only one active entrance/exit is permitted. When additional emergency exit doors are required by **DLA Disposition Services** 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.

C4.5.5.2.6. Glass display cases are not suitable for protecting pilferable items.

C4.5.5.2.7. 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.

#### C4.5.5.3. Access.

C4.5.5.3.1. Only employees designated by the activity leader, as access authorized will enter this area.

C4.5.5.3.2. List names of access authorized employees in lock and key accountability records on DLA Form 1610b. Separate access lists are not required.

C4.5.5.3.3. Activity or **Security Representative** coordinator: Notify ~~access-~~ **and appoint in writing authorized employees that have been identified as having authorized access and brief immediately regarding their responsibilities involving the area.**

C4.5.5.3.4. Restrict the number of ~~access-authorized~~ **authorized access** employees to a minimum commensurate with operational necessity.

C4.5.5.3.5. ~~Access-authorized~~ **Employees with authorized access** 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 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 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.

C4.5.5.3.6. Visitors are not permitted to enter the pilferable storage area with items such as purses, backpacks, etc. which could be used to conceal pilferable items.

#### C4.5.6. Locking Devices.

**Refer to DLA Physical Security Manual, Chapter 8, Paragraph E.**

C4.5.6.1. 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 **assistance from DLA Installation Support at Battle Creek, Security and Emergency Services Branch.**

##### C4.5.6.1.1. Key Operated Locks.

C4.5.6.1.1.1. 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 **DLA Disposition Services** field activity use, the indoor padlocks identified below are inadequate for prolonged use outdoors; but 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch.**

C4.5.6.1.1.2. 5340-00-158-3805 - low security indoor use padlock, (MILSPEC MI P-17802).

C4.5.6.1.1.3. 5340-00-1595340-3807 - same as above with chain, (MILSPEC MIL-P-17802C).

C4.5.6.1.1.4. 5340-00-241-3670 - medium security outdoors use padlock, (MILSPEC MIL-P-43951).

C4.5.6.1.1.5 Mortise locks with minimum one inch throw deadbolts not visible or accessible in locked position.

#### C4.5.6.1.2. Combination Locks.

C4.5.6.1.2.1. If combination locks are required, GSA approved; three-position changeable combination padlocks are adequate for activity use in either indoor or outdoor applications. Padlocks selected for indoor and outdoor use should be with case-hardened bodies. Shackles should also be case-hardened, and a minimum of 5/16" wide.

C4.5.6.1.2.2. 5340-00-285-6522, 5340-01-119-3981 or 5340-00-285-6523 - combination padlock, (MILSPEC MIL-P-17257).

C4.5.6.1.2.3. 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.

#### C4.5.6.1.3. Hasps and Staples.

C4.5.6.1.3.1. Heavy steel hasps and staples are suitable for secondary locks when they are securely fastened to the structure with smooth headed bolts or rivets, or peened or welded to prevent removal.

C4.5.6.1.3.2. Use high security hasps, described in Amendment 1, MIL-P-43605 (CL), only in applications where lock of similar protection level are required.

#### C4.5.6.1.4. Cipher Locks.

C4.5.6.1.4.1. 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.

C4.5.6.1.5. 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 [DLA Installation Support at Battle Creek, Security and Emergency Services Branch](#).

#### C4.5.7. Protective Systems/Factors.

Refer to the DLA Physical Security [Manual Guide, Chapter 6](#).

C4.5.7.1. 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 [DLA Installation Support at Battle Creek, Security and Emergency Services Branch](#).

~~C4.5.7.1.1. 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.~~

~~C4.5.7.1.2. It is important for planners to remember that any warning system is valueless unless it is supported by prompt security force action. 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.~~

C4.5.7.1.1. In case of alarm system failure, the [DLA Disposition Services](#) field activity alarmed area must be manned until the system is repaired or other appropriate compensatory measures applied. Notify the [DLA Installation Support at Battle Creek, Security and Emergency Services](#) Branch whenever there is a catastrophic or complete alarm system failure.

#### C4.5.7.2. Communications.

C4.5.7.2.1. Each [DLA Disposition Services](#) 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.

C4.5.7.2.2. Each [DLA Disposition Services](#) field activity must possess an adequate system of internal communication, in order to notify all employees and visitors of emergencies. This could be a public address system, cell phones, or some other suitable means.

## C4.6. Procedures.

### C4.6.1. Lock and Key Control.

C4.6.1.1. See the DLA Physical Security **Manual, Chapter 7. Guide**, paragraph D3f.

C4.6.1.2. Locking systems provide added security at **DLA Disposition Services** 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 systems through uniform lock and key control systems of accountability. The **Area Manager/field** activity leader 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 **Area Manager/field** activity leader.

C4.6.1.3. The **Area Manager/field** 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 **DLA Disposition Services** field activity 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.

C4.6.1.4. 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.

C4.6.1.5. 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.

C4.6.1.6. 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.

**C4.6.1.6.1. Field Activity sites using automated key security systems (key watch, key tracer, etc.) may co-locate keys within the same system provided that there is a 100% accountability of facility keys through automated reports provided by the system.**

C4.6.1.7. Do not provide keys to the host installation without the **DLA Installation Support at Battle Creek, Security and Emergency Services** Branch approval based on receipt of a written request from host authorities.

C4.6.1.8. 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.

C4.6.1.9. To prevent theft or possible substitution, relock 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.

C4.6.1.10. 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.

C4.6.1.11. Key and Lock Records and Accountability. Maintain control records for key control systems.

C4.6.1.12. Use of master key systems is prohibited.

C4.6.1.12.1. 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 **DLA Disposition Services** field activity. Keys that unlock key repositories may be permanently issued, but must not leave the activity. Securing of key repositories with combinations locks is encouraged.

C4.6.1.12.2. Keep all keys within the key and lock system under continuous accountability at all times. Accomplish as follows:

C4.6.1.12.2.1. The number of individuals authorized to draw keys will be kept to the absolute minimum commensurate with security and operational requirements. Flexi time will not be the sole justification for key issuance.

C4.6.1.12.2.2. Master keys and operating keys to security areas will not be issued for personal retention or removal from the activity. This restriction also applies to keys that unlock repositories that contain keys to security areas.

C4.6.1.12.2.3. When keys are not in use, they will be secured in containers of at least 20-gauge steel or material of equivalent strength. Key repositories will be attached to the structure to prevent easy removal and located in buildings or rooms with structural features that forestall illegal entry. During off duty hours, the building will be locked with an approved locking device. Key repositories will be so located that they are under the surveillance of operating personnel during duty hours. Repositories will be kept locked except to issue or return keys or to conduct inventories. Separate key repositories will be maintained for operating and duplicate keys.

C4.6.1.12.2.4. Operating and duplicate keys that control access to repositories containing keys to security areas (less utility areas), will be controlled from, and when not in use, stored in central key repositories under 24 hour control of the activity.

C4.6.1.12.2.5. DLA Form 1610 *Key Repository Index*, will be maintained for each repository within the key and lock control system. The Index will be kept inside the repository to which it pertains and will be used as the basis for inventories of keys and controlled from the repository by individual key serial number.

C4.6.1.12.2.6. Use DLA Form 1610a *Key Repository Accountability Record*, will be used to maintain accountability of the keys in each repository to maintain accountability of each repository and its keys.

C4.6.1.12.2.6.1. 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 *Area Manager/field* activity leader.

C4.6.1.12.2.7. DLA Form 1610b *Delegation of Authority-Key Control*, will be used to authorize personnel to sign for keys. Designations of individuals authorized to sign for repository keys will be signed by an individual at the division level or higher. Several individuals may be listed on the same form provided they are all authorized to sign for all keys listed on the form. The DLA Form 1610b will expire one year from signature date.

C4.6.1.12.2.8. DLA Form 1610c. *Key Control Register*, will be used by all repository custodians to record the issue and turn-in of keys. A separate DLA Form 1610c will be maintained for each repository. 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.

C4.6.1.12.2.8.1. 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.

C4.6.1.12.2.8.2. All keys and padlocks within the key control system, to included keys issued for personal retention, will be physically inventoried by serial number, at least once every six months. A record of the inventory will be maintained by the Key Control Officer until completion of the next scheduled inventory.

C4.6.1.12.2.8.3. Retain key control forms in accordance with the DLA Records Schedule.

C4.6.1.12.3. 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 **Area Manager/field** activity Leader'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 **DLA Disposition Services DSD Forward-Support Team** or his/her designee. Use certified mail for container combinations. Secure safe combinations in a locked drawer or container.

#### C4.6.2. Entry and Movement Control

C4.6.2.1. Control of visitors, vehicles and property moving in and out of an activity is a significant part of a total security program for any **DLA Disposition Services** field activity. While standard or uniform procedures to affect 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.

**C.4.6.2.1.1. The DLA Disposition Services field activity will develop local standard operating procedures for entry and movement control operations to include processes, procedures, and/or checklists outlining visitor control and identification protocols.**

**NOTE:** Requirements of the Logistics Partner are to maintain a Visitor Control Program, consistent with the standards in this chapter and with local **DLA** protocols. The sales partner must use the same type of visitor badges and registration logs as the **DLA Disposition Services field activity**.

C4.6.2.2. Visitor Control. **See DLA Physical Security Manual, Chapter 2, subparagraph G.** 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:

C4.6.2.2.1. Registration. Legibly register all persons, vehicle drivers included, desiring access to **DLA Disposition Services** field activity for inspection, CV sales, screening, or property pick up, or property turn-in on **DLA Form 584**. Required visitor registration procedures are as follows:

C4.6.2.2.1.1. Maintain **DLA Form 584** for visitor registration. If the activity has self-contained sites geographically separated from its central registration point, maintain separate registers at those sites. Retain visitor registers in accordance with the DLA Records Schedule. A single entry point and single **DLA Form 584** is most desirable, and should be enforced if possible and practical.

C4.6.2.2.1.2. Required information on the **DLA Form 584**: Date; Time; Printed Name of visitor; Signature; Badge or Pass number; Their organization office, company or DoDAAC; Destination or Purpose of visit; and Printed Name of Government POC or Entry control officer. The Area Manager/field activity leader (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. (updated Feb 2012)

~~C4.6.2.2.1.2.1 Visitors must complete each applicable section of the DLA Form 584 completely and legibly at the time of entry into the DRMO.~~

~~C4.6.2.2.1.2.1.1 Printed Name, Signature, DODAAC, Company Name.~~

~~C4.6.2.2.1.2.1.2 Purpose of Visit (i.e. screening, etc.).~~

For Visitors: A legible rendering of the visitor's printed name, DODAAC, organization/firm/unit represented, including address (city and state- minimum) 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.

For Transporters: A legible rendering of the visitor's printed name, license number, DODAAC, organization/firm/unit represented, including address (city and state- minimum) if not from the host installation; reason for accessing activity (either picking up or dropping property off), type of conveyance (tractor trailer, panel truck, van, etc.) and license plate.

~~NOTE: This information is required only when the vehicle physically enters a DLA Disposition Services yard or warehouse. It is not required for vehicles parked on public streets or in designated visitor parking areas.~~

C4.6.2.2.1.3. The **DLA Disposition Services** or Sales Partner employee will physically check the visitor's identification, compare the identification data and features listed on the identification media, with those of the visitor, and legibly complete the appropriate sections of the **DLA Form 584**.

~~C4.6.2.2.1.2.2.1 Badge Number and Type (i.e. Badge #3, DRMS Form 1961/RTD).~~

~~C4.6.2.2.1.2.2.2 Date of Entry.~~

~~C4.6.2.2.1.2.2.3 Time of Entry.~~

~~C4.6.2.2.1.2.2.4 ID Verification. Print legibly and sign.~~

C4.6.2.2.1.4. 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 **DLA Form 584** is maintained. A requirement to sign out on the register at time of departure is mandatory.

When the visitor leaves the **DLA Disposition Services field activity**, the **DLA Disposition Services** or Sales partner employee will physically retrieve the visitor badge and annotate the time of departure on the **DLA Form 584**.

C4.6.2.2.1.5. Ensure visitors screening property are so authorized by verifying the individual's possession of valid identification. A picture ID is required, 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 Section 2, Chapter 5) for specific guidance for direct removal of property and Section 4 2, Chapter 4 5 for specific guidance on visitor identification.).

C4.6.2.2.1.6. **Debarment**. In the event an individual known or suspected to be debarred from participation in surplus sales is identified within the activity, the **Area Manager/field** activity leader 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., **DLA Form 584**, 1581, etc.), and a photocopy, if obtained, of the identification used to gain entry. Forward to assigned counsel for consideration of debarment extension.

C4.6.2.2.1.7. If the sales partner is not within the main **DLA Disposition Services** compound, the sales partner will be responsible for maintaining the **DLA Form 584**, and for issuance of visitor badges. The Sales Partner is responsible for securing all unused or unissued visitor badges.

#### C4.6.2.2.1.8. Exemptions to Visitor Registration.

~~C4.6.2.2.1.8.1 Official visitors, such as personnel from HQ DLA, DLA Disposition Services Battle Creek, or DLA Enterprise Support (DES), are exempt from registration based upon orders or other official credentials.~~

C4.6.2.2.1.8.1. Visitors who enter only the **DLA Disposition Services** field activity administrative area or otherwise have no access to **DLA Disposition Services** field activity property.

C4.6.2.2.1.8.2. Security, safety, medical and fire protection personnel responding to emergencies.

C4.6.2.2.1.8.3. Contractor personnel (such as CV) with whom **DLA Disposition Services** or the **DLA Disposition Services** 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.

#### C4.6.2.2.2. Visitor Badges.

C4.6.2.2.2.1. Visitor badges are to be issued to all **DLA Disposition Services** visitors (except as reflected in paragraph C4.6.2.2.1.7 above) using DRMS Forms 1960 (Sales), 1961 (RTD), 1962 (Turn-In), and 1965 (Other – Special). The activity Area Manager will inform the workforce of badging requirements.

C4.6.2.2.2.2. The Sales Partner will provide badge requirements (quantity) to the **DLA Disposition Services field activity**. The **DLA Disposition Services field activity** will provide a sufficient number of blank **DLA Form 584** and 1960 to the Sales partner. The Sales partner will provide completed **DLA Form 584** to the **DLA Disposition Services field activity** for filing when the form has been completely filled out.

C4.6.2.2.2.3. Visitor badges will be issued to visitors after they register. The **DLA Disposition Services personnel** will retrieve these badges prior to visitor departure. The **DLA Disposition Services field activity leader** will take steps to retrieve visitor badges from visitors who depart the premises without returning their visitor badges.

C4.6.2.2.2.4. Unissued visitor badges will be secured at all times.

C4.6.2.2.2.5. Templates of official visitor badges can be obtained through **DLA Disposition Services, J-321**. The template will not be posted on the Internal Web Page for security purposes.

C4.6.2.2.2.6. Future requests for the Visitor Badges template must be made by Area Managers in encrypted email format to help prevent impersonation and tampering.

#### C4.6.2.3. Vehicle and Property Control.

C4.6.2.3.1. Vehicle Control. Procedures used to control the movement of vehicles will be as follows:

C4.6.2.3.1.1. Vehicles will enter and exit through a single designated gate that is under continual visual observation by **DLA Disposition Services** 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. **Area Managers/field activity leaders** will ensure appropriate signage and barriers are in place to enforce this restriction.

C4.6.2.3.1.2. 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, unless the Disposition Services regional Director determines that the facility has gate and other security to prevent pilferage of property. The provided security must include the inspection of trucks prior to departure from the Disposition Services site. This determination must be approved by the Regional Disposition Services Director. This exception and determination may apply to any Disposition Services field activity, worldwide. 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 **DLA Form 584**. (Updated Feb 2012)

C4.6.2.3.1.3. Government, commercial and privately owned vehicles may enter the **DLA Disposition Services** 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.

#### C4.6.2.3.2. Inspection/Weighing Procedures.

C4.6.2.3.2.1. Inspect vehicles entering a **DLA Disposition Services** 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.

C4.6.2.3.2.2. 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.

C4.6.2.3.2.3. Strictly enforce scale inspection requirements outlined in DoD 4160.21-M, Chapter 7, paragraph K3a, and activity weighing policy (also see paragraph C2.15.5.1.3. ~~above~~). ~~Discussed previously above in scales.~~

**C4.6.2.3.2.4. The DLA Disposition Services field activity is responsible for the inspections of platform, truck, and railroad scales at a frequency not less than annually and more often if required by State or local laws. A record shall be maintained of visits by qualified inspectors showing the date of the visit, and where appropriate, action taken to correct the accuracy of the scales. It is the responsibility of the DLA Disposition Services field activity to initiate the action to obtain the services of a qualified scale inspector, and to request repair action when needed.**

C4.6.2.3.3. Property Control. Use procedures to control the movement of property, material and packages as follows:

C4.6.2.3.3.1. Use activity employees and/or closed circuit TV to escort/monitor visitors to preclude pilferage or improper handling of property.

C4.6.2.3.3.2. Establish single point entry/exit controls for each display location to preclude unauthorized movement of property.

C4.6.2.3.3.3. Do not remove Government property from the activity for personal use.

C4.6.2.3.3.4. **Area Manager/field** activity leader: Establish procedures to prevent employees and visitors from entering display areas with personal property items such as lunch

boxes, handbags, briefcases and other similar items which may be used to conceal pilferable property.

C4.6.2.3.3.5. Use Optional Form 7 or similar form used by the host installation, prepared in duplicate and signed by the **Area Manager/field** activity leader or his authorized representative, to authorize activity employees to remove property from facilities. Retain the original (by the activity leader) and annotate when the property is returned. Use the pass for the following types of property:

C4.6.2.3.3.5.1. Government property not covered by normal shipping documentation (DD Form 1348-1 and DRMS Form 1427).

C4.6.2.3.3.5.2. Personal property not accompanied by a sales document and not readily identifiable as personal property.

C4.6.2.3.3.6. All property covered by a property pass is subject to inspection upon entry or departure from the activity.

C4.6.2.3.3.7. Property pick-up procedures for customers are fully discussed in Chapter 2 – General Operations, this instruction.

C4.6.2.3.4. Railroad Car Control.

**C4.6.2.3.4.1. Locally developed procedures for the control of railroad cars will, at a minimum, include the following requirements.**

~~C4.6.2.3.4.1 Monitor movement of railroad cars in and out of DLA Disposition Services field activity facilities by designated employees.~~

**C4.6.2.3.4.1.1. The movement of railroad cars in and out of DLA Disposition Services Field Activities (as applicable) will be supervised by field activity personnel and observed by security forces.**

**C4.6.2.3.4.1.2. All railroad entrances will be secured when not in use. Field activity employees and security forces will provide access control during passage of railroad cars.**

**C4.6.2.3.4.1.3. Keys to active railroad gates will be controlled by host security forces.**

**C4.6.2.3.4.1.4. Security personnel will inspect the cargo seals on all incoming and outgoing railroad cars at the entry control point. Empty railroad cars will be inspected for contraband, hazardous items, and unauthorized personnel. Local procedures will be established which provide guidance to security force personnel when discrepancies are found during this inspection. Whenever railroad cars are staged at warehouse locations, partially loaded cars will be sealed at the close of loading operations and will be checked by security patrols.**

**C4.6.2.3.4.1.5. Railroad seals will be affixed and verified in the same manner as that prescribed for truck control.**

~~C4.6.2.3.4.2 Control railroad entrances by locked gates when not in use. Activity employees will man gates, which are opened for passage of railroad cars.~~

~~C4.6.2.3.4.3 Control keys to railroad gates by the activity or provided to host security under proper receipt.~~

C4.6.2.3.5. Tamper Seals. Refer to DLA Physical Security **Manual, Chapter 4, Paragraph E.**

### C4.6.3. Pilferable Items.

C4.6.3.1. 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. Activities are required to ensure that mandated protective requirements based on CIIC codes as reflected in DoD 4100.39-M, are met. Activities 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 **DLA Disposition Services** field activity.

C4.6.3.2. As a minimum, store the following items within the designated pilferable storage area:

C4.6.3.2.1. Small arms (1005 stock class) undemilitarized bolts, barrels and trigger assemblies.

**NOTE:** This policy pertains only to items within the 1005 stock class, and only refers to bolts, barrels and trigger assemblies. For further guidance on the storage of weapons parts, refer to paragraph C4.6.3.2.5.

C4.6.3.2.2. Inherently dangerous items such as knives, bayonets, and swords.

C4.6.3.2.3. Crowbars, bolt cutters and other similar cutting devices.

C4.6.3.2.4. Smaller musical instruments.

C4.6.3.2.5. All of the following items as identified by the Controlled Item Inventory Code (CIIC).

C4.6.3.2.5.1. 0 – Naval nuclear propulsion items.

C4.6.3.2.5.2. 2 – High Sensitivity (Category II) arms, ammunition and explosives (parts only – do not store complete weapons).

C4.6.3.2.5.3. 3 – Moderate Sensitivity (Category III) arms, ammunition and explosives (parts only – do not store complete weapons).

C4.6.3.2.5.4. 4 – Low Sensitivity (Category IV) arms, ammunition and explosives (parts only – do not store complete weapons).

C4.6.3.2.5.5. N – Firearms (parts only – do not store complete weapons).

~~C4.6.3.2.5.6. R – Precious Metals.~~

C4.6.3.2.5.6. J – Pilferable (smaller items – one cubic foot or less)

~~C4.6.3.2.5.7. R - Precious metals in SCLs PSC, P8A, P8B, P8C, P81, P83, P84 and P87, and (all "V" coded SCLs).~~

C4.6.3.3. Consider items in the following CIIC codes. Store in the designated pilferable storage area consistent with size of item and with available secured storage space. As a minimum, all items in these CIIC codes must be stored within locked warehouses (rolling stock excluded).

C4.6.3.3.1. I – Aircraft engine equipment and parts.

C4.6.3.3.2. M - Hand tools and shop equipment.

C4.6.3.3.3. V- Individual Clothing and Equipment.

C4.6.3.3.4. W – Office Machines.

C4.6.3.3.5. X – Photographic equipment and supplies.

C4.6.3.3.6. Y – Communications/Electronic equipment and parts.

C4.6.3.3.7. Z – Vehicular equipment and parts.

C4.6.3.4. 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** will provide guidance at any time an appropriate display area appears to be unavailable. **DLA Disposition Services** field activity will ensure that:

C4.6.3.4.1. Employees are trained to recognize sensitive or "pilferable" property.

C4.6.3.4.2. DD Forms 1348-1A/2 accurately identifies pilferable items at time of receipt. (See Section 2, Chapter 2 – Property Accounting or Section 2, Chapter 3 – Process Disposition, batches for additional guidance.)

C4.6.3.4.3. Pilferable property is immediately processed and secured in the designated pilferable storage area on receipt.

C4.6.3.4.4. Movement of pilferable items is controlled to, from and within the most secure display location in the **DLA Disposition Services** field activity.

C4.6.3.4.5. Status changes of pilferable items are processed on accountable records in a timely manner.

#### C4.6.4. Safeguarding Funds.

See DLA Physical Security **Manual, Chapter 11. Guide, Paragraph D3p(6)**. (Currently applicable only in OCONUS locations as **DLA Disposition Services** does not conduct sales directly in CONUS).

C4.6.4.1. The following minimum physical security practices for funds protection are required at all **DLA Disposition Services** field activities where funds are collected; for specific cashier responsibilities in this area see Section 2, Chapter 2 – Property Accounting or Chapter 3 – Process Disposition. References to "cashier" in this section pertain equally to both primary and alternate cashiers.

C4.6.4.2. 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** for guidance. Safes will, when possible, be located so that it may **NOT** be seen from outside the building.

C4.6.4.2.1. Cash Boxes. When the safe storing funds do 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.

C4.6.4.2.2. Cash Box Modification. The activity leader 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.

C4.6.4.2.3. 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 padlocks when cashiers are changed.

C4.6.4.2.4. 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 leader's discretion. If recording is desired, forward Parts 2 and 2a to the **Disposition Service Director** by certified mail. Under this arrangement should a lock out occur, the **Disposition Service Director** will provide the cashier, or if circumstances warrant, the sales or activity leader, 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.

C4.6.4.2.5. 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.

C4.6.4.3. Funds Storage Limitations: **DLA Disposition Services** 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 **Disposition Service Director Forward-Support Team (FST) Operations Chief**, 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 Section 2, Chapter 2 or 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.

C4.6.4.4. 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 this chapter and in the ~~DLA Physical Security Guide, Paragraph D3n(6)(f)~~, 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.

C4.6.4.5. 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. Since 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.

C4.6.4.6. 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.

C4.6.4.6.1. Locate activating controls to allow covert operation by cashiers.

C4.6.4.6.2. 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 two (2) years.

C4.6.4.6.3. 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.

C4.6.4.6.4. 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch**.

C4.6.4.7. Funds Escort. See DLA Physical Security **Manual, Chapter 11, Paragraph D. Guide, Paragraph D3o(6)(h)**. 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 **DLA Disposition Services** field activities tenant on military installations will be in accordance with the criteria established by the host.

C4.6.4.7.1. 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 **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** on a case by case basis.

#### C4.6.5. Precious Metals.

C4.6.5.1. Display. Provide security for precious metals bearing materials consistent with the value of the expected precious metals recovery. See Precious Metals in Section 2, Chapter 1 – Logistics and Chapter 7 - Scrap 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.

C4.6.5.2. 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 **DLA Disposition Services Area Manager**/field activity leader. 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.

C4.6.5.3. 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.

C4.6.5.4. 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 to the **DLA Disposition Services J311 Office of Compliance**.

#### C4.6.6. Small Arms.

C4.6.6.1. 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 the DLA Physical Security **Manual, Chapter 10, Paragraph C** ~~Guide Paragraph D3n(1)(e)~~ for security procedural guidance.

C4.6.6.2. Inventory. If the **DLA Disposition Services** 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 **DLA Disposition Services** Office of Compliance. A written record of the most recent monthly or annual inventory will be maintained by the **DLA Disposition Services** field activity for a minimum of 2 years. Military Assistance Program (MAP) small arms not stored on an U.S. installation are exempt from the provisions of this paragraph.

C4.6.6.3. 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 **DLA Disposition Services** site security cage. In addition, items with a CIIC of 2, 3, 4, and N (parts only – not complete weapons) will be stored in the **DLA Disposition Services** sites pilferable storage area. When a **DLA Disposition Services** security cage is inadequate, the host will store those parts.

C4.6.6.4. Demilitarization Security. Transportation of small arms and subparts will be in accordance with DoD 5100.76M, Chapter 7. Similarly, the **DLA Disposition Services Area Manager**/field activity Leader is responsible for assurance that small arms parts removed from the **DLA Disposition Services** security cage are under constant **DLA Disposition Services** surveillance until DEMILLED and any UNDEMILLED parts are returned to the **DLA Disposition Services** security cage at the close of the business day.

#### C4.6.7. Periodic Security Review (PSR)/Vulnerability Assessments.

~~C4.6.7.1. Purpose of the PSR is to evaluate compliance with the minimum physical security standards identified in this chapter, to identify conditions in DLA Disposition Services field activity operations potentially subject to criminal exploitation, and to observe existing crime prevention practices utilized by the DLA Disposition Services field activity staff. DES Battle Creek Public Safety Branch personnel will conduct PSRs once every 3 years. When funding, scheduling, or other operational problems preclude accomplishment of the mandatory 3-year visits, DES Battle Creek Public Safety Branch 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, DES Battle Creek Public Safety Branch personnel will provide reviewing officials with checklists identifying the minimum physical security requirements of this chapter. DES Battle Creek Public Safety Branch personnel will perform antiterrorism vulnerability assessments (VAs) of the DLA Disposition Services field activity in conjunction with the PSR.~~

#### C4.6.7. Classified Materials.

C4.6.7.1. **DLA Disposition Services** 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 **DLA Disposition Services** 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.

C4.6.7.2. For detailed procedures to be followed when classified or possible classified material is identified or discovered within the disposal system are found see Section 2, Chapter 1 – Logistics (C1.4.3.).

#### C4.6.8. ADP (Information Technology) Security.

C4.6.8.1. **DLA Disposition Services** 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.

C4.6.9. Security of Hazardous Material / Hazardous Waste.

C4.6.9.1. **DLA Disposition Services Field Activities** storing hazardous waste and / or hazardous materials will comply with as a minimum the following Security directives:

C4.6.9.1.1. DOT Security Regulation (HM-232).

C4.6.9.1.2. 67 FR 6963.

C4.6.9.1.3. 40 CFR Parts 262/264/265.

C4.6.9.1.4. 49 CFR Par 172.

C4.6.9.2. **DLA Disposition Services Field Activities** storing hazardous waste and /or hazardous materials must have a DOT Security Plan as required by **DLA Disposition Services** policy.

C4.6.9.3. **DLA Disposition Services Field Activities** with a conforming storage facility (Part B permit) must submit to the host security agency for "Controlled Area" designation. Should the host decline to make such designation, retain such declination in writing. Comply with host directives and instructions on "controlled area" management.

C4.7. **Force Protection.**

C4.7.1. Scope.

C4.7.1.1. Department of Defense (DoD) 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 do not always target critical military or government assets to achieve their goals. DLA and **DLA Disposition Services** field activity employees and assets are not immune from terrorist activity, either domestic or foreign.

C4.7.1.2. **DLA Disposition Services** 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. **DLA Disposition Services** field activities that are tenants must meet the requirements outlined in this instruction to the maximum extent possible and activity leader 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 DES Battle Creek Public Safety Branch. All disputes with the host must be promptly elevated up the chain of command for resolution.

C4.7.2. DLA Disposition Services Area Manager/Field Activity Leader Responsibilities.

C4.7.2.1. In order to carry out these responsibilities, **Area Managers/field** activity leaders will as a minimum, accomplish the following:

C4.7.2.1.1. Ensure employees are informed of current threats. Maintain most current **host** threat statement/**threat assessment** ~~and any appropriate threat statements provided by the host.~~ A briefing by host investigative or force protection personnel may satisfy this requirement.

C4.7.2.1.2. Establish and maintain a close liaison with host officials to ensure timely receipt of intelligence information as it applies to the protection of the **DLA Disposition Services** field activity. When information is received, take appropriate measures in coordination with host force protection officials and the **DLA Installation Support at Battle Creek, Security and Emergency Services Branch.**

**NOTE:** Normally, only unclassified intelligence information may be provided to the activity. Refer providers of classified intelligence information to the **DLA Installation Support at Battle Creek, Security and Emergency Services** Branch. Ensure that the **DLA Disposition Services field activity** is incorporated in the installation FPCON notification

matrix and that **DLA Disposition Services field activity** employees are aware of actions mandated by host installation FPCON protocols. Should the host wish to provide classified intelligence information to the **DLA Disposition Services field activity**, contact the **DLA Installation Support at Battle Creek, Security and Emergency Services** Branch for assistance and guidance.

C4.7.2.1.3. 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.

C4.7.2.1.4. Ensure that AT/FP needs and requirements are addressed in the activity budget.

C4.7.2.1.5. Maintain necessary physical protective measures for activity infrastructure and facilities.

C4.7.2.1.6. Ensure appropriate emergency reaction plans are in place. These normally are host installation plans; however, they may be supplemented as necessary by the activity.

C4.7.2.1.7. Train activity employees on responsibilities during emergencies. Exercise emergency plans ~~regularly~~ **annually or as dictated by host emergency plans and procedures and/or the Learning Management System (LMS).**

C4.7.2.1.8. Ensure the **DLA Disposition Services** field activity is integrated in host antiterrorism plans. Train employees on activity and owner/user responsibilities as outlined in the plan.

C4.7.2.1.9. 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.

C4.7.2.1.10. Ensure that formal agreements are in effect with the host for all required AT/FP support. Notify the **DLA Installation Support at Battle Creek, Security and Emergency Services** Branch promptly of shortfalls or disputes with host over requirements or activity needs.

C4.7.2.1.11. Submit DRMS Form 2030 (DRMO Security Project Management) for funding in support of identified antiterrorism / physical security needs at the DLA Disposition Services field activity site.

#### C4.7.3. Emergency Plans and Exercises.

C4.7.3.1. Each **DLA Disposition Services** field activity must possess current working plans (usually host plans) that address at a minimum, the following scenarios:

C4.7.3.1.1. Fire.

C4.7.3.1.2. Armed Assault (robbery, workplace violence, etc.).

C4.7.3.1.3. Bomb Threats.

C4.7.3.1.4. Bomb Detonation.

C4.7.3.1.5. Hostage Situations.

C4.7.3.1.6. Chemical/Biological agent dispersal.

C4.7.3.1.7. Mass Casualty.

C4.7.3.1.8. Natural Disasters (common to the locality).

C4.7.3.1.9. Country Noncombatant Evacuations (OCONUS Only).

C4.7.3.2. Plans should provide for:

C4.7.3.2.1. Notification of emergency response personnel.

C4.7.3.2.2. Notification of activity employees and visitors.

C4.7.3.2.3. Evacuation procedures. Gathering/Rally Points.

C4.7.3.2.4. Response to incident by security and emergency personnel.

C4.7.3.2.5. Employee roles and responsibilities.

C4.7.3.2.6. Isolation of incident.

C4.7.3.2.7. Reporting requirements.

C4.7.3.3. 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 recommended. 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.

C4.7.3.4. 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.

C4.7.3.5. Actual (real-world) activation of any emergency plan requires SITREP initiation as soon as time allows. If computer information systems are affected, telephonic or facsimile reporting is mandated.

#### C4.7.4. Antiterrorism Prescriptive Standards.

C4.7.4.1. In addition to security standards as listed previously in this chapter and in DLA Physical Security **Manual Guide**, the following prescriptive standards are established to specifically address the threat of terrorism at DLA and **DLA Disposition Services** activities.

C4.7.4.2. Maintain positive access control measures to prevent intrusion by unauthorized personnel.

C4.7.4.3. Compliance with Unified Facilities Criteria (UFC 4-010-01), DoD Minimum Antiterrorism Standards for Buildings. This document applies to inhabited buildings. Inhabited buildings are officially defined as buildings routinely occupied by 11 or more personnel, and with a population density of more than one person per 430 gross square feet. Most **DLA Disposition Services** field activity buildings do not meet this threshold. However, field activities should

comply with this document to the maximum extent possible, and apply compensatory measures when compliance is not practical or cost-effective. For buildings that meet or exceed the “inhabited building” definition, compliance is mandatory. Requests for waivers to antiterrorism standards for buildings are to be submitted in accordance with instructions in Section 1, Chapter 1.

Waivers, Exceptions and Deviations. The more common standards within the UFC that apply to most **DLA Disposition Services** field activities are:

C4.7.4.3.1. Standard 1 – Minimum Standoff Distances.

C4.7.4.3.1.1. Restrict parking within ~~33~~ **12** feet of inhabited buildings **for a very low level of protection. Standoff distances will be met based on the conventional construction standoff distance (Table B-2-UFC 4-010-01) based on the specific construction of the walls and whether they are load bearing or not of the facility.** ~~DRMS Form 2031, No Parking Signs are available to assist activities in restricting parking.~~

C4.7.4.3.1.2. Keep all unsearched vehicles at a minimum distance as prescribed by the design-based threat.

**NOTE:** This will normally be determined during the vulnerability assessment performed at the **DLA Disposition Services field** activity. If this distance is not possible due to a wide variety of factors, apply appropriate and reasonable compensatory measures.

C4.7.4.3.1.3. 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:

C4.7.4.3.1.3.1. Conduct random searches of vehicles entering the area or conduct searches in accordance with AT/FP guidelines on the installation.

C4.7.4.3.1.3.2. Monitoring of the standoff zone via CCTV.

C4.7.4.3.1.4. Negotiate with host officials to achieve the appropriate standoff zone around **DLA Disposition Services** buildings/areas. Unresolved disputes will be elevated to HQ DLA Public Safety Office through command channels.

C4.7.4.3.1.5. Restrict the placement of trash containers (which may be used to conceal an explosive device) within ~~33~~ **12** feet of inhabited buildings.

C4.7.4.3.2. Standard 2 – Unobstructed Space.

C4.7.4.3.2.1. Maintain an “unobstructed space” free of obstructions ~~within 33-~~ **feet** of inhabited buildings **based on specific construction of the walls and whether they are load bearing or not of the facility.** There should be nothing in this space that would allow the concealment of an object or device of 150mm (6 inches) greater in height.

C4.7.4.3.2.2. Ensure that gutters, windowsills, doorways, sewer grates, etc. are considered and modified to prevent concealment of a device.

C4.7.4.3.2.3. Train employees to be alert for suspicious items, conditions, persons, vehicles, and what to do if they encounter something.

C4.7.4.3.3. Standard 3 – Drive-Up/Drop-Off Areas.

C4.7.4.3.3.1. Limit parking at areas designed to drop off or pickup property.

C4.7.4.3.3.2. Do not allow unattended vehicles in or near receiving areas.

C4.7.4.3.4. Standard 8 - Building Overhangs.

C4.7.4.3.4.1. Avoid building overhangs with inhabited spaces above them where people could gain access under the overhang.

C4.7.4.3.5. Standard 10 – Windows, Skylights and Glazed Doors.

C4.7.4.3.5.1. Install a minimum of 6-mm (1/4 inch) nominal laminated glass for all exterior windows, skylights and glazed doors, or a suitable substitute such as 6-mm fragmentation film (See US Army Corps of Engineers United Facilities Guide Specification 08850) <<https://www.drms.dla.mil/drms/intranet/suppservices/fragfilmspecs.pdf>>.

C4.7.4.3.5.2. Ensure frames are of sufficient strength and construction to support ultimate yield stresses consistent with the glazing material.

C4.7.4.3.5.3. Ensure that newly installed windows and glazed doors meet the prescribed standard in the UFC.

C4.7.4.3.6. Standard 12 – Exterior Doors.

C4.7.4.3.6.1. Ensure that all exterior doors into inhabited areas open outwards.

C4.7.4.3.7. Standard 14 – Roof Access.

C4.7.4.3.7.1. Eliminate external access where possible or secure internal ladders or stairways with locked cages or similar mechanisms.

C4.7.4.3.8. Standard 18 - Emergency Air Distribution Shutoff.

C4.7.4.3.8.1. Provide an emergency shutoff in the HVAC control system that can immediately shut down air distribution throughout the building. Locate the switches for easy access to building occupants.

C4.7.4.3.9. Standard 22 – Mass Notification.

C4.7.4.3.9.1. All inhabited buildings must have a timely means to notify occupants of threats and instruct them what to do in response to those threats.

C4.7.4.4. 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. Posting of FBI, ATF or host placards / guides is encouraged. Video training materials are available from the [DLA Installation Support at Battle Creek, Security and Emergency Services](#) Branch.

C4.7.4.5. Develop procedures covering the visual inspections of mail and package. Discourage or prohibit the receipt of personal mail.

C4.7.4.6. 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.

#### C4.7.5. New Construction/Renovations/Relocation.

C4.7.5.1. 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 [DLA Installation Support at Battle Creek, Security and Emergency Services](#) Branch will review such plans by ~~preparing a threat assessment~~ in accordance with the Army TM 5-853 Volumes 1 and 2 and Unified Facilities Criteria (UFC) 4-010-01 and 4-010-02 (FOUO); determining appropriate construction standards to deter and prevent damage from a terrorist attack. Recommendations will be made in writing. [DLA Installation Support at Battle Creek, Engineering and Environmental Services](#) Branch ~~will secure~~ and [DLA Installation Support at Battle Creek, Security and Emergency Services](#) Branch will coordinate on all construction projects.

C4.7.5.2. The [DLA Installation Support at Battle Creek, Security and Emergency Services](#) AT/FP Officer will develop a prioritized list of AT/FP criteria to be considered by site-selection teams prior to the relocation of any [DLA Disposition Services](#) activity. [A baseline assessment in coordination with the U.S. Army Corps of Engineers will be conducted prior to any relocation of a DLA Disposition Services site to ensure that prescriptive protection measures are met.](#) The site-selection team will use the criteria to determine if the proposed facility provides adequate protection against terrorist attacks.

#### C4.7.6. Training.

C4.7.6.1. Employees must be trained on a regular basis concerning self-protective measures against terrorists.

C4.7.6.2. 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 Combatant Command (COCOM) commander Web-based

training at <https://atlevel1.dtic.mil/at/> meets this requirement. Contact the **DLA Installation Support at Battle Creek, Security and Emergency Services Branch** /~~Force Protection Team~~ for additional information and assistance.

C4.7.6.3. 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.

C4.7.6.4. Employees must also be trained on local antiterrorism and emergency policies and procedures.

C4.7.6.5. Provisions for the above training must be included within the ISA or MOU/MOAs with host installations.

#### C4.7.7. Force Protection Conditions (FPCONS).

C4.7.7.1. The DoD Force Protection Condition (FPCON) System 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 **DLA Disposition Services** field activity will comply with all tasked host installation FPCON measures, when responding to threats against installation facilities, assets and personnel. Notify **DLA Disposition Services** HQ via SITREP of FPCON elevation. When FPCON is reduced by order of installation commander or other authority, make a follow- up SITREP.

C4.7.7.2. 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.

C4.7.7.3. 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.

C4.7.7.4. 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.

C4.7.7.5. 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.

C4.7.7.6. 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.

C4.7.8. Vulnerability Assessment Protocols. Security Program Review (SPR)/Vulnerability Assessments

~~C4.7.8.1. Each DLA Disposition Services field activity will receive an antiterrorism-vulnerability assessment (VA) at least once every three years. Representatives from the DLA or DES Battle Creek Public Safety Branch will conduct the VA. Normally, the DES DLA Public Safety Office will conduct assessments for all OCONUS sites, and DES Battle Creek Public Safety Branch will assess CONUS sites. The DES Battle Creek Public Safety Branch will conduct a compliance-oriented security review in conjunction with the VA. Public Safety personnel performing assessments will use as a minimum, this instruction, the DLA Physical Security Guidebook, Unified Facilities Criteria (UFC 4-010-01), and appropriate Joint Service Integrated Vulnerability Assessment (JSIVA) benchmarks in conducting the assessment.~~

C4.7.8.1. The purpose of the SPR is to evaluate compliance with the minimum physical security standards identified in this chapter, to identify conditions in DLA Disposition Services field activity operations potentially subject to criminal exploitation, and to observe existing crime prevention practices utilized by the DLA Disposition Services field activity staff. DLA Installation Support at Battle Creek, Security and Emergency Services personnel will conduct SPRs once every three years. When funding, scheduling, or other operational problems preclude accomplishment of the mandatory three year visits, DLA Installation Support at Battle Creek, Security and Emergency Services personnel will request the assistance of host asset officials in conducting physical security reviews of the affected facilities. To ensure uniformity in the reviews, DLA Installation Support at Battle Creek, Security and Emergency Services personnel will provide reviewing officials with checklists identifying the minimum physical security requirements of this chapter.

C4.7.9. Security Program Reviews/Vulnerability Assessment Protocols

C4.7.9.1. Each DLA Disposition Services field activity will receive a SPR/VA at least once every three years. Representatives from the DLA Installation Support at Battle Creek, Security and Emergency Services Branch will conduct the SPR/VA. Normally, the DLA HQ Installation Support Office will conduct assessments for all OCONUS sites, and DLA Installation Support at Battle Creek, Security and Emergency Services Branch will assess CONUS sites. The DLA Installation Support at Battle Creek, Security and Emergency Services Branch will conduct a compliance-oriented security review. Security and Emergency Services personnel performing assessments will use as a minimum, this instruction, the DLA Physical Security Manual, UFC 4-010-01, DOD Minimum Antiterrorism Standards for Buildings, and appropriate Joint Service Integrated Vulnerability Assessment (JSIVA) benchmarks in conducting the assessment.

C4.7.9.2. The SPR/VAs will review the following areas:

- C4.7.9.2.1. Physical Security.
- C4.7.9.2.2. Electronic Security Systems, as applicable.
- C4.7.9.2.3. Law Enforcement Liaison and Intelligence Support.
- C4.7.9.2.4. Disaster Preparedness and Vulnerability to a Threat.
- C4.7.9.2.5. Force Protection Plans and Programs.
- C4.7.9.2.6. Plans and Support.
- C4.7.9.2.7. Resources.
- C4.7.9.2.8. Training.
- C4.7.9.2.9. Site-Specific Issues and Concerns.

C4.7.9.3. The DLA Disposition Services Area Manager/field activity leader will be required to assemble pertinent documents and/or obtain information necessary to conduct the SPR/VA. The following tasks should be completed prior to the arrival of the SPR/VA Team.

C4.7.9.4. 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.

C4.7.9.4.1. Assemble or create the following documents:

- C4.7.9.4.1.1. Activity budget.
- C4.7.9.4.1.2. Mail and Package screening procedures.
- C4.7.9.4.1.3. Current installation threat statement(s) (unclassified).
- C4.7.9.4.1.4. Procedures for vehicle and pedestrian access control procedures for gaining access to the DLA Disposition Services field activity and installation.
- C4.7.9.4.1.5. Host procedures for Intelligence information dissemination to the activity.
- C4.7.9.4.1.6. Procedures for activity and/or host response to emergencies.
- C4.7.9.4.1.7. As applicable, listing of internal guard posts and security patrols for each shift. (Activity internal only).
- C4.7.9.4.1.8. Host AT/FP Plan, as supplemented.

C4.7.9.4.1.9. Host Security Plan, as supplemented.

C4.7.9.4.1.10. Host Emergency/Disaster Preparedness Plan, as supplemented.

C4.7.9.4.1.11. Copies of **all ISAs, MOAs and/or MOUs with the host.** ~~agreements for police services, force protection, fire protection, emergency services, and civil engineering/public works.~~

C4.7.9.4.1.12. Records of exercises of emergency procedures for the past three years.

C4.7.9.4.1.13. Records of funding levels and requests for funding for the past two years.

C4.7.9.4.1.14. Records of staffing levels and requests for additional staffing for the past two years.

C4.7.9.4.1.15. Current activity COOP, as prescribed by **DLA Disposition Services Operations (DLA Disposition Services-O)** (CONUS sites only).

C4.7.9.4.1.16. Three copies of the following engineer documents:  
(Available through public works/civil engineering):

C4.7.9.4.1.16.1. Vicinity map showing the location of the activity with respect to the surrounding area.

C4.7.9.4.1.16.2. Scalable site plan of the installation or activity buildings, roads, parking, entrances, etc.

C4.7.9.4.1.16.3. Aerial photos (if available).

C4.7.9.4.1.16.4. Architectural floor plans showing space utilization, elevations, and sections of buildings housing assets.

C4.7.9.4.1.16.5. Structural floor plans, elevations, and sections of buildings housing assets showing typical construction.

C4.7.9.4.1.16.6. Drawings showing any electronic security systems (IDS, CCTV, access control, duress alarms, monitoring stations, etc.) related to the identified assets.

C4.7.9.4.1.16.7. Drawings showing any alternate power sources for security related equipment (UPS).

C4.7.9.4.1.17. Names/phone numbers of key individuals:

C4.7.9.4.1.17.1. Installation AT/FP Officer.

C4.7.9.4.1.17.2. Installation Law Enforcement Officer.

C4.7.9.4.1.17.3. Installation Officer responsible for providing intelligence information concerning terrorist threats.

C4.7.9.4.1.17.4. Installation Disaster Preparedness/Emergency Services Officer.

C4.7.9.4.1.17.5. Installation Physical Security/Resource Protection Program Manager.

C4.7.9.4.1.17.6. Installation Information Security Program Manager (person responsible for the protection of classified information).

C4.7.9.5. Identify points of contact in the responsible civil engineering or public works organization that can provide additional engineering information.

C4.7.9.6. Make all appropriate courtesy notifications to host and tenant agencies, (Installation Commander, AFOSI, USACIDC, NCIS, Security Forces/Security Police/Military Police, etc.).

C4.7.9.7. Arrange for any necessary camera, vehicle or security passes for each VA team member.

#### C4.7.10. Assessment Report Processing.

C4.7.10.1. The respective force protection officer will provide the activity leader with a written and oral out brief at the conclusion of the assessment.

C4.7.10.2. Upon finalization of the report, it will be transmitted electronically in a secure means (PKI) to **DLA Disposition Services Operations**, with a **45 30**-day suspense. Findings concerning **DLA Disposition Services MEO, RGO, Centralized Demilitarization Divisions Centers** or **Controlled Property Branches Centers** will be provided to the appropriate HQ **DLA Disposition Services** staff office. Reports on **DLA Disposition Services** overseas activities will be provided in hardcopy.

C4.7.10.3. ~~Activity chiefs will completely justify any non-acceptance of an assessment recommendation, with the understanding that the DLA Disposition Services Commander will decide whether or not the risk of non-acceptance will be taken.~~ **Activity leaders will respond to each finding using the DRMS Form 2029, December 2008, DRMS Vulnerability Assessment Report Worksheet, through their respective DLA Disposition Services Staff office, completely justifying a non-acceptance of an assessment recommendation within 90 days of receipt of the final report, with the understanding that the DLA Disposition Services Director will decide whether or not the risk of a non-acceptance will be taken.**

**C4.7.10.3.1. Directions for completing the DRMS Form 2029 are included in the report Appendix D.**

C4.7.10.4. For findings that require funding to correct or mitigate, the Area Manager/field activity leader must prepare and submit DRMS Form 2030, DRMO Security Project Management to the Security and Emergency Services at Battle Creek, Force Protection with all supporting cost estimates from the host installation.

C.4.7.10.4.1. The Area Manager/field activity leader should query the Host Installation as to the possibility of the Host funding some or all of the assessment recommendations.

C4.7.10.5. At sites where a contractor is present, any findings resulting from the SPR/VA or corrective action required by the contractor will be forwarded to the contractor through the COTR. The SPR/VA will be coordinated with the contractor management through the COR.