

DLIS-RW

November 27, 2001

KEY AND LOCK CONTROL

A. REFERENCES

1. DLAI 5710.1, Physical Security Program.
2. DoDD 5200.8, Security Of DoD Installations And Resources.
3. ***DLIS Instruction 5200.1, Key And Lock Control, March 2, 1998, (hereby superseded).***

B. PURPOSE. This instruction prescribes procedures and assigns responsibilities for all keys and locks in the possession of the Defense Logistics Information Service (DLIS); Defense Reutilization and Marketing Service (HQ DRMS); and Defense Logistics Agency Systems ***Integration Office (DSIO)***.

C. APPLICABILITY AND SCOPE. This procedure applies to all organizational elements of DLIS, HQ DRMS, ***DSIO***, and other DLIS supported activities.

D. DEFINITIONS

1. Conventional Combination Locks. This type of lock utilizes numbers, or other reference points, in order to align the lock's tumblers so that the locking device can move to an unlocked position. As with key operated locks, conventional combination locks are susceptible to manipulation and compromise.
2. Duplicate Keys. Store duplicate operating keys for emergency use (e.g., loss of a key or absence of the holder of the operating key). Store duplicate keys in a key repository separate from operating keys.
3. Interchangeable Cores. The interchangeable core system utilizes a type of lock with a removable core, replaceable by another core using a different key. Its main features are as follows:
  - a. Quickly replaceable cores.
  - b. Keying all locks into an overall master-keyed local system.
  - c. It is economical due to reduction in maintenance costs and new lock expense.
  - d. The system is flexible to the installation's needs.
  - e. It simplifies record keeping.
  - f. Secure the control key.
4. Key Operated Locks. This type of lock includes pin-tumbler, wafer, warded, and disc-tumbler locks.
5. KCO. Key Control Officer.
6. KLCC. Key and Lock Control Custodian.
7. Manipulation-Resistant Combination Locks. A manipulation-resistant lock designed so that the opening lever does not come in contact with the tumblers until setting of the combination. Such a lock furnishes a high degree of protection for sensitive material.

8. Master Keys. A single key that opens a series or system of locks. Discourage the use of master keys; however, if master keys are required, limit their use to the lowest organizational level possible.

9. Operating Keys. The key routinely used to activate the locking mechanism. Each key will operate only the individual lock or locks designed for that key.

10. Other Combination Locks. Combination locks with four or more tumblers may be desirable for containers or structures of highly critical items if these locks contain manipulation resistant features.

11. Relocking Devices. A relocking device on a safe or vault door furnishes an added degree of security against forcible entry. A relocking device increases the difficulty of opening a combination lock container by means of punching or drilling the lock or its parts. Use relocking devices for heavy-duty safes and vaults.

12. Reserve Locks With keys. Those locks and keys used to rotate other locks or to provide for new requirements. Secure these in the same manner as duplicate keys.

#### E. PROCEDURES

##### 1. Security And Control Procedures/Measures

a. Document overall accountability for locks and keys in the system as follows:

(1) Total number of locks being used by type (key or combination).

(2) Identification number (code/serial number or other) for each lock and key (permanently on key).

(3) Location of each lock.

(4) Number of keys to each lock.

(5) Record of personnel in possession of keys on a permanent basis to include key identification.

(6) Date when combination was changed on combination locks.

(7) List of personnel having knowledge of combination.

b. Control keys utilized for daily check out as follows:

(1) KCO or KLCC will ensure logging in and out of all keys issued from the key repository on appropriate DLA forms, i.e., DLA Form 1610, 1610a, 1610b, 1610c.

(2) Each person will retain all keys issued in their possession at all times. Do not leave keys in locks, in the vicinity of locks, nor transfer without keys being turned in and reissued.

(3) Retain keys not issued in the security key repository.

(4) Inventory and account for all keys in the key repository at the end of the business day.

(5) Secure the key repository when keys are not being issued or turned in. KCO/KLCC will attend during the issue and receipt of keys.

c. Keep the number of individuals authorized to draw/retain keys to the absolute minimum commensurate with security and operational requirements. Flexitime will not be the sole justification for key issuance.

d. Do not issue master keys or operating keys to security areas for personal retention or removal from the activity. This restriction also applies to keys that unlock repositories that contain keys to security areas.

e. Secure keys in containers of at least 20-gauge steel or material of equivalent strength when not in use. Attach key repositories to the structure to prevent easy removal and located in buildings or rooms with structural features that forestall illegal entry. Locate key repositories so that they are under the surveillance of operating personnel during duty hours. Keep repositories locked except to issue or return keys or to conduct inventories. Maintain separate key repositories for operating and duplicate keys.



f. Control operating and duplicate keys which control access to repositories containing keys to security areas (less utility areas) from and, when not in use, stored in central key repositories under 24-hours control of the activity security force. Facility Engineer controls keys to utility areas.

g. Maintain DLA Form 1610, Key Repository Index, for each repository within the key and lock system. Keep the DLA Form 1610 inside the repository to which it pertains and use it as the basis for inventories of keys controlled from the repository.

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

(1) Use DLA Form 1610a, Key Repository Accountability Record, to maintain accountability of the keys in each repository.

(a) Conduct two inventories each duty day for repositories that are not in use during nonduty hours. The individual who signs out the repository key at the beginning of the day will inventory the keys contained therein using DLA Form 1610. This individual will then complete the DLA Form 1610a, leaving the block entitled "SIGNATURE OF INDIVIDUAL RELIEVED OF RESPONSIBILITY" blank. Annotate the "REMARKS" block "Opening Inventory". Reverse the procedure at the end of the day. Leave the block entitled "PRINTED NAME AND SIGNATURE OF INDIVIDUAL ASSUMING RESPONSIBILITY" blank. Annotate the "REMARKS" block "Closing Inventory".

(b) For the central key repositories and all other repositories under 24-hour control, transfer accountability at the beginning of each shift. The individuals assuming and relinquishing responsibility will inventory the keys contained therein using the DLA Form 1610. They will then complete the DLA Form 1610a for that repository.

(c) Annotate discrepancies detected during repository inventories in the "REMARKS" block of the DLA Form 1610a. Report discrepancies immediately to both the Command Security Officer (CSO) and the activity KCO.

(2) Repository Custodians will use DLA Form 1610c, Key Control Register, to record the issue and turn-in of keys. Maintain a separate DLA Form 1610c for each repository. Lock DLA Form 1610c inside the repository to which it pertains when not in use. Record all keys removed from the repository on the DLA Form 1610c.

i. Authorized personnel will use DLA Form 1610b, Delegation of Authority-Key Control, to sign for keys. Heads of offices/directorates will designate individuals authorized to sign for repository keys and other keys. List all individuals authorized to sign for all keys listed on the same form.

j. Affix keys normally issued and used as a group as a set on rings of at least # 12 gauge wire, welded or brazed together, or its equivalent. Each ring will include a metal or plastic tag stamped or imprinted with a ring identification code. However, do not sign key rings out by their identification code. List each key on the ring by its serial number on the DLA Form 1610c. Stamp all duplicate keys with an "S" after the serial number.

k. All keys and padlocks within the key control system, to include keys issued for personal retention, will be physically inventoried by serial number at least once every 6 months. The KCO will maintain a record of the inventory until completion of the next scheduled inventory.

l. Rotate padlocks in use within the key and lock control system at least once every 12 months. Whenever possible, the rotation should be between different directorates or offices rather than within the same directorate of office. Secure padlocks not in use, along with the corresponding keys, in a locked metal container that meets the requirements of a key repository. Control access to the container in the same manner as for key repositories.

m. Do not, under any circumstances, leave locks hanging open on a hasp, staple, hook, or other device. In all cases, relock locks to the staple immediately after opening and remove the key.

n. Change all combinations to safes or vaults designed for classified storage and/or storage of unclassified Government property at least once every 12 months, or upon the reassignment or departure of an individual with knowledge of the combination or compromise, whichever occurs first. Maintain a record of each combination change for at least 30 days after the next change.

o. Optional Form 62, Safe or Cabinet Security Record, and Optional Form 63, Security Container Information, will be used in conjunction with each combination lock used to secure unclassified Government property.

p. DLAR 5200.12, paragraph 5-104, provides guidance concerning recording of safe or vault combinations by the activity control office. These provisions also apply to safes or vaults that store unclassified Government property.

q. Reset built-in combination locks to the standard combination 50-25-50 when safe or vaults when not in service. Reset combination padlocks to the standard combination 10-20-30.

2. Key Control Record. KLCCs will maintain key control records. Key control records will include the following information:

- a. Total number of keys and locks in the system, including lock cores, if any.
- b. Number of keys issued for personal retention and the names of persons issued the keys.
- c. Number of keys on hand.
- d. Number of locks in use.
- e. Number of reserve locks/keys.

#### F. RESPONSIBILITIES

1. Commander, DLIS-D, will appoint a Key Control Officer (KCO).

2. Key Control Officer (KCO), **Facilities and Supply Division, Directorate of Planning and Resource Management (DLIS-RW)** will:

a. Be responsible for a comprehensive system to account for all keys and locking devices used in or assigned to HQ DRMS, DLIS, **DSIO** and other DLIS supported activities.

b. Control the daily use of keys retained and used by HQ DRMS, DLIS, **DSIO** and other DLIS supported activities.

**c. Maintain this instruction in a current status and review it biennially.**

3. Heads of Offices/Directorates will appoint a Key and Lock Control Custodian (KLCC). Forward a copy of this appointment to the Command Security office (CSO) and the KCO.

4. Key and Lock Control Custodians (KLCCs) are responsible for all keys and locks issued to that directorate/office.

G. EFFECTIVE DATE AND IMPLEMENTATION. This instruction is effective and implemented upon **signature by the DLIS Deputy**.

H. INFORMATION REQUIREMENTS. (Reserved for future use.)

BY ORDER OF THE COMMANDER

/s/  
RICHARD B. MAISON  
Deputy