NIH POLICY MANUAL

1415 KEY, LOCK AND CARDKEY SERVICES
Issuing Office: ORS/DPS/CPB 496-9818
Release Date: 11/1/99

---

1. **Explanation of Material Transmitted:** This chapter establishes policy and describes the system for acquiring keys, locks, and the on-campus electronic access cardkeys.

2. **Material Superseded:** NIH Manual Chapter 1415 in its entirety.

3. **Filing Instructions:**

   Remove: NIH Manual Chapter 1415 dated 2/1/90

   Insert: NIH Manual Chapter 1415 dated 11/1/99

4. **Distribution:** NIH Manual Mailing Keys F-401 and F-402

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Manual System, contact the Office of Management Assessment, OA, on 496-2832.
- Online information, go to the NIH Home Page and enter this URL: **http://www3.od.nih.gov/oma/manualchapters**

KEY, LOCK AND CARDKEY SERVICES

Table of Contents

KEY, LOCK AND CARDKEY SERVICES

A. PURPOSE: This chapter establishes policy and defines procedures for (1) requesting and reassigning keys (door keys, desk keys, file cabinet keys, etc.); (2) changing locks and cylinders; (3) changing safe combinations; (4) requesting electronic access control cardkeys (on campus only); (5) locking sensitive areas; and (6) securing equipment.

B. BACKGROUND: Federal regulations note that the National Institutes of Health (NIH) is officially open to the public during normal working and visiting hours and for approved public events; it is closed at all other times. Hence, the locking of NIH facilities during non-duty hours is in keeping with these regulations.

Major buildings on the NIH enclave are secured by an electronically controlled door lock/building access system. The entrance doors to all other buildings on the enclave as well as corridor room doors are controlled by a mechanical key/lock system. Both systems are administered by the Division of Public Safety (DPS), Office of Research Services (ORS).

C. REFERENCES:

1. 45 Code of Federal Regulations, Part 3.41

2. NIH Manual 1130, Delegation of Authority, General Administration No. 8

3. NIH Manual 1381, Physical Security

4. NIH Manual 2300-940, Clearance of Personnel for Separation or Transfer

D. RESPONSIBILITIES:

1. The Director, NIH has delegated authority for the protection of NIH facilities and grounds to the
   Associate Director for Research Services (ADRS), ORS.
   This authority has been redelegated to the Director, DPS. Policies for the key, lock and security services program are established by the DPS with the approval of the ADRS.

2. The Locksmith Section, Crime Prevention Branch (CPB), DPS, is responsible for the management and operation of the established key and lock services program.

3. The Security Section, CPB, DPS, is responsible for the management of the electronic access control system, i.e., the issuance of cardkeys, programming of access levels, etc.

4. The Automated Systems Unit, Division of Engineering Services is responsible for the maintenance and repair of the electronic access control system.

5. The IC Administrative Officers, their support staff, and/or delegated program area staff are responsible for requesting and/or approving locksmith services through the Service and Supply Fund Activities System (SSFAS), a subsystem of the NIH Administrative Database System (ADB). In addition, they are responsible for the control and return of keys and the reporting of lost or stolen keys.

6. IC Cardkey Coordinators are responsible for approval/disapproval of Form NIH 2450, Request for
Cardkey and Record of Registration, the control and return of cardkeys, and the reporting of lost/stolen
cardkeys.

7. The IC Executive Officer is responsible for IC compliance with this policy.

8. NIH employees are responsible for complying with the policies stated in this chapter and for the safekeeping of all NIH issued keys, combinations, and access control system cards.

E. DEFINITIONS:

1. Employee - For the purpose of this chapter, any person employed by the Government or an NIH contractor who regularly reports for duty on the NIH enclave or at any of the NIH rental building.

2. IC Cardkey Coordinator - Authorizing/approving official responsible for the proper completion of the needed request forms for the issuance of the electronic access control cardkeys. (Normally the IC Administrative Officer.)

3. Administrative Database (ADB) System - The automated system administered and managed by the Center for Information Technology. It combines administrative and

financial data to support the NIH intramural program, including the purchase, receipt and payment of goods and services; the management and tracking of property inventories; as well as management of service and supply fund activities.

F. **POLICY:** It is the policy of NIH that buildings and rooms will be closed and locked except when open for business or other purposes. The Privacy Act of 1974 requires agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Privacy Act records. Normally such security is provided by locked cabinets or rooms.

1. Room Keys

The approved locking mechanisms at the NIH are key and cylinder locks and/or electronic access control system locks. All types of locking devices other than the standard mechanical keys/locks require the specific approval of the Director, DPS, in writing, prior to placing an order.

Employees will be issued one key for each room requested. One replacement of a lost key is allowed per employee. If a key is lost, the cylinder may need to be changed and new keys issued. The decision to rekey will be determined by the CPB upon evaluation of the circumstances surrounding the loss. Master keys and/or grand master keys will be issued only to police and fire officials. Any exception must be approved in writing by the Director, DPS.

Keys may be reassigned or transferred through the ADB by the IC Administrative Officer or their support staff when the employee to whom the key was originally issued no longer has need for the key.

KEYS WILL NOT BE ISSUED TO PARTICIPANTS IN THE STUDENT TEMPORARY EMPLOYMENT PROGRAM OR TO SUMMER APPOINTMENTS. Exceptions to this policy require the approval of the Director, DPS.

2. Cardkeys

KEY, LOCK AND CARDKEY SERVICES

All new electronic access control system installations require the approval of the Director, DPS. Upon approval, the proper failure mode will also be approved, i.e., fail safe or fail secure. The fail safe mode automatically unlocks doors in the event of an electrical power loss or the loss of communications with the access control system computer. The fail secure mode automatically locks doors in the event of an electrical power loss. This mode is used in the most critical areas and must be approved in writing by the Director, DPS.

An electronic access control cardkey will be issued to each employee who needs recurring access to a building during security hours (normally 6 p.m. to 6 a.m. Monday through Friday and/or anytime on weekends and holidays) or to interior facilities secured by the on-campus electronic access control system. Cardkey Coordinators should ensure cards are requested for all employees who need them in order to preclude the NIH emergency dispatchers having to admit employees during security hours.

Each cardkey is issued individually and is not transferable. A cardkey issued to an employee who has transferred or separated, or who no longer has a need for it, must be returned to the CPB, Building 31, Room B3B16, for reissuance.

A lost or stolen cardkey must be reported immediately by the cardholder so that it can be voided to prevent unauthorized use. During normal working hours, Monday through Friday, 7:30 a.m. to 5 p.m., call the CPB at 496-9818. During non-working hours or at all times when the theft or loss occurs at NIH, contact the DPS Emergency Communications Center at 496-5685. In addition, the cardholder should notify their IC Cardkey Coordinator so that a replacement card can be issued.

G. PROCEDURES

1. Keys or locks for rooms, desks or file cabinets

To request locksmith services, i.e., door key issuance; door cylinder change; door key reassignment, return, or loss; desk/file cabinet key issuance; or emergency key/lock services, a request must be entered into the SSFAS, ADB by an individual identified in the ADB through assignment of a user ID and approved by an authorized ADB Node

KEY, LOCK AND CARDKEY SERVICES

Approving Official. The complete user's guide for making locksmith service requests is available on-line at www-isb.cit.nih.gov/dbaslock.htm.
It is the responsibility of the ADB Node Approving Officials or the individuals to whom keys are assigned to pick up the keys from the Locksmith Section when notified through the ADB system that they are ready. Keys must be picked up within 30 days or they will be destroyed or returned to stock for subsequent reissuance.

Employees must sign and forward to the Locksmith Section, Building 31, Room B4BS04, Form NIH 452-1, Record of Receipt for Keys, for all keys issued. This form accompanies each key.

For emergencies involving key or lock failures, e.g., broken locks, keys, door knobs, etc., during normal working hours, Monday through Friday, 7:30 a.m. to 5 p.m., call the Locksmith Section, 496-3507. For emergencies during non-working hours or for lockouts occurring at anytime, i.e., staff locked out of their workplace, call the DPS Emergency Communications Center at 496-5685. The dispatcher(s) will take the necessary steps to ensure that the door lock or key problem is resolved.

2. Electronic Access Control Cardkeys

To request a new cardkey or replacement of a broken or lost cardkey, the employee should:

a. Contact the IC Cardkey Coordinator who will submit a completed Form NIH 2450, Request for Cardkey and Record of Registration, to the CPB, Building 31, Room B3B16. The IC Cardkey Coordinators can be determined by contacting the appropriate IC Administrative Officer.

b. Cardkeys will be delivered to the Cardkey Coordinators when ready.

c. Upon receipt of the cardkey, the employee (authorized cardholder) must sign Form NIH 452-4, Record of Receipt for Cardkey, and send it to the CPB, Building 31, Room B3B16.

3. Clearance Procedures

KEY, LOCK AND CARDKEY SERVICES

It is the responsibility of the IC Administrative Officer to ensure the return of door keys that are no longer needed. Keys should be returned to the Locksmith Section, CPB, DPS in Building 31, Room B4BS04.

The IC Cardkey Coordinator is responsible for returning cardkeys that are no longer needed. They should be returned to the CPB, DPS in Building 31, Room B3B16.

4. Reporting Non-working Cardkeys and/or Readers

For emergencies involving individual cardkeys during normal working hours, Monday through Friday, 7:30 a.m. to 5 p.m., call the CPB, 496-9818. During non-working hours, call the DPS Emergency Communications Center at 496-5685. The dispatcher(s) will take steps necessary to solve immediate problems and are authorized to call appropriate personnel should a need exist.

For emergencies involving reader or system failures at anytime, call the Automated Systems Unit, Division of Engineering Services at 496-2105.

5. Safe Lock Servicing and Combination Changes

The IC Administrative Officer should contact the Locksmith Section on 496-3507 immediately upon receipt of a safe, or whenever an employee with knowledge of a safe's combination leaves an organization.

6. Special Locking Requirements or Devices (including Cypher Locks or Electronic Access Control Readers)

An area's sensitivity depends on the type, value and vulnerability of the property to be protected or controlled. When a high degree of protection is justified by security needs, security of the area will be accomplished with the installation of a high security mechanical or electronic lock.

Requests for high security locks, along with justification for special security requirements for high risk/sensitive areas, should be submitted by memorandum to the Director, DPS, Building 31, Room B3B12. The Security Section, CPB will perform an

evaluation of the area, after which an approval/disapproval memorandum will be sent to the requester.

7. Securing Equipment

Theft deterrent devices are available for securing office and laboratory equipment. These devices are available on NIH-wide Blanket Purchase Agreements (BPAs). The CPB will provide consultation service to assist in selecting and ordering anchoring devices to secure office or laboratory equipment.

Keys to specially-installed security equipment such as cables, chains, anchor pads and other security devices may be retained by the IC Administrative Officer so that equipment can be repaired/serviced or moved from location to location as necessary. In such cases, the ICs are responsible for resecuring the equipment. If keys are not available, the security equipment provider must be contacted to unlock the anchoring devices. In emergencies, the Locksmith Section may be contacted and a request entered into the ADB system.

H. RECORDS RETENTION AND DISPOSAL: All records (**e-mail** and non-e-mail) pertaining to this chapter must be retained and disposed of under the authority of NIH Manual 1743, "Keeping and Destroying Records," Appendix 1, "NIH Records Control Schedule," Item 1300-C-9.

NIH e-mail messages. NIH e-mail messages (messages, including attachments, that are created on NIH computer systems or transmitted over NIH networks) that are evidence of the activities of the agency or have informational value are considered Federal records. These records must be maintained in accordance with current NIH Records Management guidelines. Contact your IC Records Officer for additional information.

All e-mail messages are considered Government property, and, if requested for a legitimate Government purpose, must be provided to the requester. Employees' supervisors, NIH staff conducting official reviews or investigations, and the Office of the Inspector General may request access to or copies of the e-mail messages.

E-mail messages must also be provided to Congressional committees if requested and are subject to Freedom of Information Act requests. Since most e-mail systems have

back-up files that are retained for significant periods of time, e-mail messages and attachments are likely to be retrievable from a back-up file after they have been deleted from an individual's computer. The back-up files are subject to the same requests as the original messages.

I. MANAGEMENT CONTROLS: The purpose of this manual issuance is to establish the NIH policy and describe the system for acquiring keys, locks and electronic access cards.

1. Office Responsible for Reviewing Management Controls Relative to this Chapter (Issuing Office): Through this manual issuance, the Division of Public Safety (DPS), Office of Research Services (ORS) is responsible for the method used to ensure that management controls are implemented and working.

2. Frequency of Review: Ongoing review that includes review of periodic reports to determine if changes are required.

3. Method of Review: The DPS will maintain oversight and ensure effective implementation and compliance with this policy through review of a myriad of resources, e.g., complaints received from NIH employees and Administrative Officers, police reports, property lost reports, and various system-generated reports.

4. Review reports are sent to: Director, DPS, Associate Director for Research Services, Deputy Director for Management, NIH. Issues of special concern will be brought immediately to the attention of the Associate Director for Research Services.