NIH Policy Manual

1405 - NIH Physical Access Control

Issuing Office: OD/OM/ORS/SER/DPSAC **Phone:** (301) 451-4766

Release Date: 9/24/2015 ?

Transmittal Notice

1. **Explanation of Material Transmitted:** National Institutes of Health (NIH) campuses and facilities have implemented increased security measures mandated by Homeland Security Presidential Directive (HSPD)-12. This chapter establishes policy and describes procedures for gaining physical access to NIH owned or leased facilities. This chapter covers the issuance of identification (ID) badges and the authorization of physical access to NIH locations.
2. **Filing Instructions:**
   Insert: NIH Manual 1405 dated 9/24/2015.

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Manual System, contact the Division of Management Support, OMA on 301-496-2832, or enter this URL: http://oma.od.nih.gov/public/MS/manualchapters/Pages/default.aspx

A. Purpose

The purpose of this chapter is to establish policy for the issuance of identification (ID) badges and the authorization of physical access to NIH locations.

B. Background

The NIH faces a significant challenge in maintaining security and providing physical access for geographically dispersed campuses which have a unique combination of sensitive facilities, hospitals and research that are utilized by tens of thousands of employees, contractors, affiliates and visitors each day. The NIH utilizes Physical Access Control Systems (PACS) to facilitate timely access to NIH facilities while meeting regulatory security requirements. These systems allow for automated entry based on access rights which are granted on an individual basis.

The Office of Research Services (ORS), Office of Security and Emergency Response (SER), Division of Personnel Security and Access Control (DPSAC) maintains overall responsibility for managing physical access to NIH facilities. The execution of this responsibility is

conducted by the local/satellite security offices at NIH installations. The security offices at each NIH facility manage both the PACS and individual access requests.

Access permissions are provided in conjunction with the issuance of an ID badge. NIH issues several different types of ID badges. The type of ID badge issued to an individual is dependent on various factors as outlined in Manual Chapter 1443: Homeland Security Presidential Directive (HSPD)-12 Implementation Policy. For details on current types of ID badges, please visithttp://www.ors.od.nih.gov/ser/dpsac/badge/Pages/NIH-Badging-Authority-by-Classification-Table.aspx. The operations of issuing ID badges are largely governed by HSPD-12 which mandates the establishment of a government-wide standard for secure and reliable forms of identification. HSPD-12 was created to eliminate wide variations in the quality and security of forms of identification used to gain access to federal facilities and systems. To satisfy the requirements of HSPD-12, the National Institute of Standards and Technology (NIST), developed the Federal Information Processing Standard (FIPS) 201-2, "Personal Identity Verification of Federal Employees and Contractors." FIPS 201-2 specifies a standard to be implemented for issuing ID badges.

C. Policy

Managing access control supports the biomedical research goal of NIH by contributing to a safe work environment through issuing authorized ID badges. It is the policy of the NIH that ID badges will only be issued after successfully completing the security requirements as outlined in Manual Chapter 1443: HSPD-12 Implementation Policy. Individuals are then authorized physical access to NIH locations based on their specific job duties.

The local/satellite NIH security offices operate as the badging authority responsible for issuing ID badges to individuals who require physical access to NIH facilities. NIH facilities with ID badge issuance services and the requisite security office are outlined in the table below.

Table 1 NIH Security Badging Offices

NIH Facility / Location	Security Office / Contract Office
NIH Campus / Bethesda, MD	ORS Division of Personnel Security & Access Control (DPSAC) / (301) 451-4766
Bayview Research Center / Baltimore, MD	ORS Division of Personnel Security & Access Control (DPSAC) / (301) 451-4766
Rocky Mountain Laboratories, NIAID / Hamilton, MT	Access Control Office / (406) 363-9356
NIEHS Campus / Research Triangle Park, NC	Operations & Security Branch / (919) 541-5116
NCI-Frederick Campus / Ft. Detrick, MD	Security Office / (301) 846-1901

NCI-Shady Grove Campus / Rockville, MD	ORS Division of Personnel Security & Access Control (DPSAC) / (301) 451-4766
NIAID 5601 Fishers Lane / Rockville, MD	ORS Division of Personnel Security & Access Control (DPSAC) / (240) 669-5509

To facilitate timely access to buildings and offices, the NIH utilizes various PACS to manage physical access to the NIH campus and its buildings. NIH has the capability to use the various PACS to increase, decrease, restrict, or terminate an individual's access to NIH locations. This PACS is in compliance with NIH Manual Chapter 2808: NIH Enterprise Architecture Policy.

D. References

1. Federal Information Processing Standard (FIPS) 201-2, "Personal Identity Verification of Federal Employees and Contractors" http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
2. NIH Manual Chapter 1443, "HSPD-12 Implementation Policy"
3. NIH Manual Chapter 1743, "Keeping and Destroying Records"
4. NIH Manual Chapter 2808, "NIH Enterprise Architecture Policy"
5. HSPD-12-Homeland Security Presidential Directive http://www.dhs.gov/homeland-security-presidential-directive-12

E. Definitions

1. **Access control:** A process that grants, denies or restricts a person's entrance to a facility based on approved criteria.
2. **Affiliates:** Individuals requiring access to NIH and who are not employees or contractors (e.g., special volunteers, tenants, guest researchers, fellows, etc.)
3. **Badging Authority/Office:** The NIH office responsible for issuing ID badges.
4. **Federal Information Processing Standards (FIPS 201):** Federal Publication developed by the National Institutes of Standards and Technology (NIST) as ordered by HSPD-12 to establish standards for identity credentials.
5. **HSPD-12:** Homeland Security Presidential Directive-12 is a Presidential Directive that requires the definition of a set of common, acceptable and achievable standards for Personal Identity Verification (PIV) of Federal employees and contractors. It is designed to enhance security, increase Government efficiency, reduce identity fraud and protect personal privacy.
6. **DPSAC HSPD-12 Program:** The DPSAC HSPD-12 Program provides program management oversight for the HSPD-12 initiative at NIH. It is responsible for ensuring that program goals are achieved and timeframes for delivery are met while streamlining security processes for the NIH community. This office plans and helps implement the

NIH HSPD-12 initiative. It provides program management and training to assure compliance with the Directive.

7. **Physical Access Control System (PACS):** A security database that stores information on all issued ID badges. This system is utilized to grant specific access to NIH facilities based on an individual's job duties.

F. Responsibilities

1. General Responsibilities

    a. **The Associate Director for Security and Emergency Response (ADSER)**, through the local/satellite security offices, is responsible for granting access to NIH facilities.
    b. **Institutes and Centers (IC) Executive Officers (EO)** manage the facilitation of access control requests. Requests are typically submitted via email by an Administrative Officer to the requisite security office.
    c. **Administrative Officers (AO)** ensure access control requests are submitted in accordance to the policies and procedures set forth in this chapter. The servicing AO is authorized to submit access requests for individuals to DPSAC and has the primary responsibility for providing administrative support to the individual in a particular organization.
    d. **NIH employees, contractors, affiliates and any other individual who is issued an ID badge** are responsible for complying with the policies stated in this chapter and for the safekeeping of their ID badge.
    e. **Office of Research Services (ORS)** plans and directs service programs for public safety and security operations, scientific and regulatory support programs, and a wide variety of other programs and employee services at NIH.
    f. **Division of Personnel Security and Access Control (DPSAC)** maintains overall responsibility for managing physical access to NIH facilities. DPSAC is responsible for identity proofing, enrolling and issuing badges to all employees, contractors and affiliates

2. Local and/or Satellite Security Offices Responsibilities

    Note: DPSAC plays an oversight role over the local and/or satellite Security Offices to ensure compliance with this policy.

    a. Manage access control operations. Ensure all processes and procedures are functioning effectively. Provide timely customer service support, generate system reports, respond to information technology (IT) requirements and manages quality control.
    b. Input, operate, and maintain PACS to control access to their NIH facilities. Grant access based on an individual's affiliation with the NIH and their job duties.
    c. Validate the identity of individuals in the PACS and verify that the appropriate access is authorized. Print, distribute, and input badge identification number into the PACS to activate the badge.

G. Procedures

1. Badge Issuance: Upon completion of the security requirements as outlined in Manual Chapter 1443, HSPD-12, individuals will be directed to their local/satellite badge issuance office. The badge issuance office will then verify both the identity of the person and their authorization before issuing the ID badge.
2. Lost, Stolen and Broken ID badges:

    a. Anyone with a badge issued by NIH must report lost/stolen ID Badges to the local/satellite security/badge issuance office and the individual's AO.
    b. Broken badges should be brought to the local/satellite security/badge issuance office for a replacement. If a broken badge has not expired, the individual will be issued a new badge. The expiration date on the new badge will be the same as the date on the broken badge.

3. Requesting Changes to Physical Access Privileges: Individuals receive only perimeter access when they initially receive their ID badge. An individual's AO may request additional access for the person by contacting their local/satellite security/badge issuance office. All requests must be in writing.
4. Departing NIH and Badge Collection: All individuals leaving NIH must contact their AO prior to their departure date. AOs must collect the individual's ID badge as part of the departure process. The ID badge must be returned to the local/satellite security/badge issuance office. Failure to surrender a badge will be reported to the Division of Police as possessing unauthorized property. When possible, withholding of payments may be authorized.
5. Help Desk and Help Requests:

    a. AOs should submit a request for change in physical access to the local/satellite security/badge issuance office. All requests must be in writing.
    b. Individuals having problems with the operation of their badge should contact their local/satellite security/badge issuance office.
    c. Planned power outages should be reported to the local/satellite security/badge issuance office as outages affect card readers and ability to lock down areas through the PACs system.

H. Records Retention and Disposal

All records 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 Schedules" (as amended). These records must be maintained in accordance with current NIH Records Management and Federal guidelines. Contact your IC Records Liaison or the NIH Records Officer for additional information.

I. Internal Controls

1. **Required Documentation:** The information mentioned in this policy is subject to the Privacy Act of 1974, as amended (5 U.S.C. Section 552a). Information stored within this record system must be maintained in accordance with the NIH Privacy Act Systems of Record Notices (SORNs) listed below. DPSAC is responsible for ensuring the confidentiality of all documents is maintained for the Physical Access Control Systems (PACS) as well as the proper release to authorized individuals, of information collected and used at NIH. The following SORNs are applicable for the record systems:

    a. 09-25-0054 - - Andover Continuum Access Control System, HHS/NIH/OD/ORS/DPSAC
    b. 09-25-0216 - NIH Electronic Directory, HHS/NIH
    c. 09-25-0220 - Johnson Controls Pegasys System, HHS/NIH/NIEHS/OM/OSB (pending release in 2015)

    In addition to the above published and pending SORNs, Privacy Impact Assessments (PIAs) for the PACs utilized at the NIH are also in place for the following IT systems:

    a. NIH OD ORS Andover Continuum Badging System
    b. NIH NIEHS Pegasys System

2. **Office Responsible for Reviewing Internal Controls Relative to this Chapter:** DPSAC is responsible for ensuring that internal controls are implemented and working properly. Internal controls include: Testing PACS systems upgrades prior to deployment; assuring access requests are submitted in writing; communicating PACS systems changes with the NIH community; and assuring compliance with FIPS-201-2.
3. **Frequency of Review:** DPSAC will maintain an ongoing review of procedures to determine if changes are necessary that will better serve the NIH community. At a minimum, this manual chapter will be reviewed on an annual basis.
4. **Method of Review:** DPSAC will ensure effective implementation and compliance with this policy by analyzing NIH community feedback, reviewing system-generated reports and communicating with internal resources.
5. **Type of Review:** Ongoing internal risk assessments.

    Review Reports are sent to: Associate Director for Security and Emergency Response (ADSER), Director, Office of Research Services (ORS), and the Director, Division of Personnel Security and Access Control (DPSAC).