# NIH Policy Manual

## 1405 - NIH Physical Access Control

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

**Approving Official(s):** DDM

**Release Date:** 6/29/2023 ?

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 procedures for gaining 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. This chapter has been revised to adhere to the 5-year review requirement outlined in Manual Chapter 1710 – Publishing and Maintaining Policies in the NIH Policy Manual. The Scope of the policy was added, the Background was revised to reflect the applicable federal standards, the NIH Security Badging Offices table was removed from the Policy statement, the Responsibilities and Procedures sections were formatted, and a new definition was added. Please see Appendix 1 for additional details.
2. **Filing Instructions:**
   **Remove:** NIH Policy Manual, Chapter 1405, dated 9/15/2015
   **Insert:** NIH Policy Manual, Chapter 1405, dated 06/29/2023

**PLEASE NOTE:** For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Policy Manual, contact the Division of Compliance Management, OMA on 301-496-4606, or enter this URL: https://oma.od.nih.gov/DMS/Pages/Manual-Chapters.aspx.

### A. Purpose

The purpose of this chapter is to establish a policy for the issuance of identification (ID) badges and the authorization of physical access to NIH campuses, buildings, and specific locations within them

## B. Scope

This policy applies to the NIH Bethesda, Maryland, Rocky Mountain Laboratories, Hamilton, Montana, Research Triangle Park, North Carolina, National Cancer Institute, Frederick Maryland, the National Cancer Institute Shady Grove campuses, the Bayview Research Center, Baltimore Maryland, as well as NIH leased facilities.

## C. Background

The NIH faces a significant challenge in maintaining security and providing physical access to geographically dispersed campuses that 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 ORS, SER, Division of Physical Security Management (DPSM), approves the use and installation of electronic locking systems. 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 permission levels are provided in conjunction with the issuance of an ID badge. NIH issues several different types of ID badges dependent on various factors outlined in Manual Chapter 1443: Homeland Security Presidential Directive (HSPD)-12 Implementation Policy. For details on current types of ID badges, please visit the NIH Badging Table.

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) 201-3 "Personal Identity Verification of Federal Employees and Contractors." FIPS 201-3 specifies a standard to be implemented for issuing ID badges.

Controlling access to NIH facilities on an emergency and non-emergency basis is paramount to providing a safe working environment for research to be conducted in support of the NIH mission.

## D. Policy

The NIH's policy is to only issue ID badges to individuals after completing the security requirements outlined in Manual Chapter 1443: HSPD-12 Implementation Policy. Individuals are then authorized physical access to NIH locations based on the roles and responsibilities of their position description.

NIH utilize various PACS in compliance with NIH Manual Chapter 2808: NIH Enterprise Architecture Policy, OMB-M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management to manage, increase, decrease, restrict, or terminate access to NIH campuses, buildings, or specific locations within them.

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 identified in **Appendix 2**.

## E. Responsibilities

1. **The Associate Director for Security and Emergency Response (ADSER)**, **Office of Research Services (ORS)** is responsible for:

    a. Planning and directing service programs for public safety, security operations, scientific and regulatory programs, and a wide array of other service programs.
    b. Providing services dedicated to supporting NIH's biomedical research goals in a safe work environment for NIH employees, visitors, research, and facilities.
    c. Providing oversight of the access control program to ensure compliance with this policy.
    d. Managing physical access control to NIH facilities.
    e. Identifying conditions where limited access to space may be granted and emergency /non-emergency access will be maintained.
    f. Addressing when key overrides are permitted (i.e., generally limited to fire department access) as part of a card reader installation.
    g. Ensuring all processes and procedures are functioning effectively.
    h. Providing timely customer service support.
    i. Generating system reports.
    j. Responding to information technology (IT) requirements and managing quality control.
    k. Providing input on the operations PACS to control access to NIH facilities.
    l. Granting facility access based on an individual's affiliation with the NIH and organizational responsibilities.
    m. Validating and identifying individuals in the PACS and verifying that the appropriate access is authorized.
    n. Printing, distributing, and inputting badge identification numbers into the PACS to activate the badge.
    o. Issuing ID badges to employees, contractors, affiliates, and other individuals.

p. Determining the required security level and the device to install to mitigate the risk.

2. **The NIH Institutes, Centers, and Offices (ICOs)** are responsible for:

    a. Managing organizational access control requests consistent with Facility Access Control (FAC) guidelines.
    b. Providing administrative support for access control requirements.
    c. Submitting access control requests to the responsible security office.
    d. Notifying the Division of Physical Security Management (DPSM) at DPSM-ServiceRequest@mail.nih.gov to obtain approval and assistance before commencing any task related to the installation of a card reader not associated with a construction project. This includes unique circumstances such as card reader installation requests to doors that also have hard keys with lock cylinders, in which case DPSM will require justification and a key control plan for approval.
    e. Complying with Federal Protective Services (FPS) and Department of Homeland Security (DHS) Interagency Security Committee (ISC) Standards along with NIH requirements in leased facilities, when applicable.
    f. Ensuring access control requests comply with the terms and conditions stipulated in this policy.
    g. Identifying spaces that require restricted access and the controls in place to support emergency and non-emergency access.

3. **The NIH Office of Research Facilities (ORF),** is responsible for:

    a. Providing keys for access control systems when authorized.
    b. Reporting planned power outages to the local/satellite security badge issuance offices to minimize impacts to card readers and the ability to lock down areas through the PACS system.
    c. Managing the contract that includes the installation of, and repairs to, badge readers.

4. **NIH employees, contractors, affiliates, and any individual** issued an ID badge is responsible for complying with the policies stated herein and for the safe keeping of ID badges.

## F. Procedures

1. **NIH employees, contractors, affiliates, and any individual** in need of an ID Badge must provide two original documents consistent with the requirements of NIH Policy Manual 1443-Homeland Security Presidential Directive 12 (HSPD-12) Implementation Policy for background investigations and validation.

    a. Must report lost/stolen badges to the local/satellite security badge issuance office and the associated ICO the individual works for.

b. Broken badges should be brought to the local/satellite security/badge issuance office for a replacement.
c. 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.
d. Individuals departing NIH must contact their AO before their departure date.

2. **The NIH ICOs:**

a. **Administrative Officers** with the requisite security training must:

1. Sponsor individuals to obtain an HHS ID badge (PIV Card) in accordance with NIH Policy Manual 1443.
2. Request issuance of an ID badge to an individual.
3. Complete sponsorship actions for HHS ID Badges through the NIH Enterprise Directory (NED).
4. Identify the roles and responsibilities of applicants for issuance of the correct category of ID badge.
5. Remain aware of the individual's status and continuing need for holding an ID badge and updating NED accordingly.
6. Request written changes to physical access privileges to access restricted or other sensitive areas in NIH facilities. If you have any questions, please contact the Access Control office at facilityaccesscontrol@mail.nih.gov or (301) 451-4766.
7. Collect individual ID badges when they depart the NIH and return it to the local/satellite security badge issuance office within eighteen (18 hours) of termination.

    i. Failure to surrender a badge will be reported to the Division of Police as possessing unauthorized property.
    ii. When possible, withholding of payment may be authorized.

8. Contact ORS DPSM at DPSM-ServiceRequest@mail.nih.gov when planning the installation of a card reader to control access to a sensitive area.

3. **The ADSER, ORS:**

a. **Local and/or Satellite Security Offices, ORS**

1. Inputs, operates, and maintains PACS to control access to NIH facilities as shown in **Appendix 2**.
2. Validates the identity of individuals in the PACS and verifies the appropriate access is authorized by NIH Policy Manual 1443 for NIH-owned and leased facilities exclusive of those with direct leases through the General Services Administration (GSA).

3. Prints, distributes, and inputs badge identification number into the PACS row to activate a badge.
4. Grants access to NIH facilities based on the individuals position description.
5. Maintains a list of restricted access spaces to include individuals and organizations authorized access on an emergency and non-emergency basis.

b. **Division of Personnel Security & Access Control (DPSAC), ORS:**

1. Reviews operations of the Local and/or Satellite Security Offices to ensure compliance with this policy.
2. Ensures the effectiveness of the standard operating procedures for accessing restricted spaces on an emergency and non-emergency basis complies with the applicable Federal Protective Services (FPS), DHS Interagency Security Committee (ISC) Standards, and NIH requirements.
3. Utilizes **Appendix 2 – Access to Controlled/Restricted Space in NIH Facilities** to ensure access to controlled areas on an emergency and non-emergency basis.

c. **Division of Physical Security Management (DPSM), ORS**:

1. Ensures that physical and engineering security initiatives at all NIH-owned or leased facilities comply with federally mandated physical security requirements and approved security systems that mitigate current and emerging threats. This includes electronic access control security, Video Surveillance System (VSS), and electronic door locking systems.
2. Assesses facilities to determine the required security level and the appropriate devices to install to mitigate the risks to include card key readers.
3. Reviews and approves or denies requests for keys to access restricted areas controlled by a card reader system in owned facilities.
4. 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, the security of the area will be accomplished with the installation of a high security mechanical or electronic lock and card reader. Requests for electronic controlled locks and card reader access should be submitted to DPSM-ServiceRequest@mail.nih.gov. DPSM Security Specialist will evaluate the area for an approval decision.
5. Requests for high-security mechanical locks, along with justification for special security requirements for high-risk/sensitive areas, should be submitted to DPSAC and DPSM for evaluation and collaboration with ORF ASU Locksmith Section. Generally, these are not issued, and requests must be approved by the DPSM director.
6. For leased facilities with a direct lease through GSA, serves as the Facility Security Committee (FSC) Facilitator as a consultant for security-related

items, decision making, costs, and implementation.

4. **The Division of Facilities Operations and Maintenance (DFOM) Technical Support Team (TST)/Security/Locksmith, ORF:**

    a. Provides keys for access control systems when authorized.
    b. Utilizes **Appendix 3** to provide emergency and non-emergency access to designated areas.

5. **The NIH Clinical Center (CC):**

    a. Utilizes the following Clinical Center Administrative Policies to manage access to clinical spaces:

        1. CC Administrative Policy FP-004- Managing Access in the Clinical Center Complex, as part of the program to manage security risks, staff can request and be issued a key(s) and/or card key reader access to areas in the Clinical Center Complex (CCC) based on their duties and responsibilities.

            i. Oversight of the CCC program is within the office of the Chief Operating Officer.
            ii. Doors in patient care units and departments accessible by card key readers also have locksets to permit access in the event of a disruption or outage.
            iii. Where required by law, certain offices and laboratories are sensitive with restricted access controlled by the Division of Police.

    b. S-002 Security Risk Management in the Hospital

        1. Used to manage risks within the hospital by completing evaluations and implementing prudent control measures to reduce the risk of damage and harm to persons and property.
        2. Incorporates electronic, physical, and/or administrative controls.

## G. 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.201-3.pdf
2. Office of Management and Budget (OMB) Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential and Access Management
3. National Institutes of Standards and Technology (NIST) SP-800: Guidelines for the Use of PIV Credentials in Facility Access

4. DHS Homeland Security Presidential Directive: 12: Policy for Common Identification Standards for Federal Employees and Contractors
5. DHS Interagency Security Committee (I iT SC) Standards: The Risk Management Process for Federal Facilities
6. NIH Manual Chapter 1415 – Key and Lock Services
7. NIH Manual Chapter 1443, "HSPD-12 Implementation Policy"
8. NIH Policy Manual, Chapter 1743 *Keeping and Destroying Records*, available at: https://oma1.od.nih.gov/manualchapters/management/1743/
9. NIH Manual Chapter 2808, "NIH Enterprise Architecture Policy"
10. Clinical Center Administrative Policy FP-004-Managing Access in the Clinical Center Complex
11. Clinical Center Administrative Policy S-002 – Security Risk Management in the Hospital

## Appendix 1: Policy Updates

1. Added a section entitled: "Scope".
2. Background

    a. Revised reference to the applicable Federal Information Processing Standard.
    b. Provided a link to the NIH Badging Table.

3. Policy – removed Table 1 – NIH Security Badges Offices and included it as Appendix 2.
4. Reformatted the policy to reflect the current template.
5. Responsibilities – expanded discussion of the roles of each organization.
6. Procedures

    a. Expanded discussion of the procedures applicable to each organization.
    b. Added procedures for the Division of Physical Security Management, ORS, the NIH Clinical Center, and the Division of Facilities Operations and Maintenance, ORF.

7. Definitions – added Clinical Center Complex.
8. Added Appendix 3 – Access to Space in NIH Facilities.

## Appendix 2: NIH Security Badging Offices

| NIH Facility / Location | Security Office / Contract Office |
|---|---|
| NIH Campus / Bethesda, MD | ORS Division of Personnel Security/ (301)-402-9755 & Access Control (DPSAC) / (301) 451-4766 |
| Bayview Research Center / Baltimore, MD | ORS Division of Personnel Security/ (301)-402-9755 & Access Control (DPSAC) /(301) 451-4766 |
| Rocky Mountain Laboratories, NIAID / | Access Control Office / (406) 363-9356 |

| | |
|---|---|
| Hamilton, MT | |
| 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 / (301)-402-9755 & Access Control (DPSAC) / (301) 451-4766 |
| NIAID 5601 Fishers Lane / Rockville, MD | ORS Division of Personnel Security & Access Control (DPSAC) / (240) 669-5509 |

## Appendix 3: Access to Space in NIH Facilities

| **SCENARIOS** | **NORMAL BUSINESS HOURS (6:30 a.m. - 5:00 p.m. unless identified otherwise)** | | **OUTSIDE NORMAL BUSINESS HOURS** | |
|---|---|---|---|---|
| | **Primary Point of Contact for Access to Space** | **Secondary Point of Contact for Access to Space** | **Primary Point of Contact for Access to Space** | **Secondary Point of Contact for Access to Space** |
| **Emergency Events** | | | | |
| Flood due to utility system failure | NIH Maintenance Call Desk Dial: 301-435-8000 | ORF Locksmith Dial: 301-496-3508 | NIH Maintenance Call Desk Dial: 301-435-8000 | NIH Maintenance Call Desk Dial: 301-435-8000 |
| Medical Issue | Emergency Communication Center (Dial 911 from an NIH Phone or 301-496-9911 from a Cell Phone) | NIH Maintenance Call Desk Dial: 301-435-8000 | Emergency Communication Center (Dial 911 from an NIH Phone or 301-496-9911 from a Cell Phone) | NIH Maintenance Call Desk Dial: 301-435-8000 |
| Isolated power outage | NIH Maintenance Call Desk Dial: 301-435-8000 | ORF Locksmith Dial: 301-496-3508 | NIH Maintenance Call Desk Dial: 301-435-8000 | NIH Maintenance Call Desk Dial: 301-435-8000 |

| | | | | |
|---|---|---|---|---|
| Staff member locked out of office | NIH Maintenance Call Desk Dial: 301-435-8000 | ORF Locksmith Dial: 301-496-3508 | NIH Maintenance Call Desk Dial: 301-435-8000 | NIH Maintenance Call Desk Dial: 301-435-8000 |
| Staff member locked out of area with controlled access | ORS Division of Police (7:00 a.m. - 3:00 p.m.) | Dial: 301-496-5685 (7:00 a.m. - 3:00 p.m.) | NIH Maintenance Call Desk Dial: 301-435-8000 | NIH Maintenance Call Desk Dial: 301-435-8000 |
| **Non-Emergency Events** | | | | |
| Flood due to utility system failure | NIH Maintenance Call Desk Dial: 301-435-8000 | ORF Locksmith Dial: 301-496-3508 | NIH Maintenance Call Desk Dial: 301-435-8000 | NIH Maintenance Call Desk Dial: 301-435-8000 |
| Medical Issue | ORS Division of Police (7:00 a.m. - 3:00 p.m.) | Dial: 301-496-5685 (7:00 a.m. - 3:00 p.m.) | Emergency Communication Center (Dial 911 from an NIH Phone or 301-496-9911 from a Cell Phone) | NIH Maintenance Call Desk Dial: 301-435-8000 |
| Isolated power outage | NIH Maintenance Call Desk Dial: 301-435-8000 | ORF Locksmith Dial: 301-496-3508 | NIH Maintenance Call Desk Dial: 301-435-8000 | NIH Maintenance Call Desk Dial: 301-435-8000 |
| Staff member locked out of office | NIH Maintenance Call Desk Dial: 301-435-8000 | Dial: 301-496-5685 (7:00 a.m. - 3:00 p.m.) | NIH Maintenance Call Desk Dial: 301-435-8000 | ORF Locksmith Dial: 301-496-3508 |
| Staff member locked out of area with controlled access | ORS Division of Police (7:00 a.m. - 3:00 p.m.) | Dial: 301-496-5685 (7:00 a.m. - 3:00 p.m.) | Emergency Communication Center Dial: 301-496-5685 | Emergency Communication Center Dial: 301-496-5685 |

## Appendix 4: 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 federal government employees or contractors but who have an official business relationship with the NIH (e.g., special volunteers, tenants, guest researchers, fellows, etc.)
3. **Badging Authority/Office:** The NIH office responsible for issuing ID badges.
4. **Card Reader**: A device that reads the data contained in access cards and allows entry into secured areas.
5. **Clinical Center Complex**: The Building 10 Complex consists of the Mark O. Hatfield Clinical Research Center (CRC), the Warren Grant Magnuson Building, and the Ambulatory Care Research Facility (ACRF).
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. **DPSM-ServiceRequest@mail.nih.gov** – Dedicated email address for submission of physical security requests, questions, or other physical security-related communications, including installation, relocation, or decommissioning requests, to DPSM.
8. **Facility Security Committee (FSC)** - Facility tenant leadership group which convenes to address security issues at applicable facilities such as multi-tenant leased facilities by ISC Risk Management Process (RMP). The FSC is typically chaired by the tenant occupying the most space within said facility or their designee.
9. **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.
10. **Federal Protective Service (FPS)** - A federal law enforcement agency providing integrated security and law enforcement services to federally owned and leased buildings, facilities, properties, and/or any other federal assets.
11. **General Services Administration (GSA)** - Central management agency responsible for setting federal policy for federal procurement and real property management and information resources.
12. **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.
13. **Key:** metal keys that are used to open the door, not on card readers.
14. **Override Keys:** Metal keys that are used to open a door when the card read malfunctions or there is a loss of power.

15. **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.
16. **Security Sensitive Area:** A designated area or function with elevated security risks based on a hospital-wide assessment of property and occupants or regulatory mandates. Typically, security-sensitive areas meet one of the following criteria: vulnerable patients, monetary resources, medications, NIH-defined restricted areas for hazardous agents or high energy equipment, personally identifiable information, or critical operations such as the NIH Cashier's Office.