

# NIH Policy Manual

## 1443 - Homeland Security Presidential Directive 12 (HSPD-12) Implementation Policy

**Issuing Office:** OD/OM/ORS/SER/DPSAC **Phone:** [\(301\) 443-8717](tel:3014438717)

**Release Date:** 9/18/2015 ?

Transmittal Notice

1. **Explanation of Material Transmitted:** This manual chapter establishes the [Homeland Security Presidential Directive 12 \(HSPD-12\)](#) implementation policy for the National Institutes of Health (NIH).
2. **Filing Instructions:**

**Remove:** N/A.

**Insert:** Manual Issuance 1443, dated 09/18/2015.

**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: <https://oma.od.nih.gov/DMS/Pages/Manual-Chapters.aspx>.

### A. Purpose

The purpose of this document is to establish a comprehensive policy for the implementation of Homeland Security Presidential Directive 12 (HSPD-12) at NIH. This policy document aims to ensure that NIH complies with all applicable federal authorities, policies, and directives.

This policy establishes the requirements for obtaining an identification (ID) badge for all employees, contractors, and affiliates who require physical access to NIH facilities and access to NIH Information Technology (IT) networks and information.

### B. Background

The Homeland Security Presidential Directive 12 (HSPD-12) was issued August 27, 2004. The stated intent of this directive is as follows:

"There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these

variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification."

### C. Policy

All federal employees, contractors, and affiliates who require physical access to NIH facilities and logical access to NIH IT networks and information are required to obtain an ID badge. To obtain an ID badge, an individual's personal identity must be verified in accordance with HSPD-12 requirements and the appropriate background investigation must be completed and favorably adjudicated. Individuals may be issued an ID badge on an interim basis if they meet the requirements as outlined in this policy.

NIH will adhere to all requirements of HSPD-12 and its implementing instructions as prescribed in the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) FIPS 201 Standard for all persons who work at or for NIH.

NIH, in accordance with Department of Health and Human Services (HHS) policy, issues or accepts several types of ID badges for physical and network/system (logical) access:

**Figure 1 NIH Issues and Accepts Badge Types**

| <b>Badge Name</b>  | <b>System Access</b>                    |
|--|---|
| HHS ID Badge (Personal Identity Verification = PIV Card) | Both physical and network/system access |
| Restricted Local Access (RLA) Badge                      | Both physical and network/system access |
| Local-Based Physical Access (Legacy) Badge               | Physical access only                    |
| Alternate Logon Token (ALT)                              | Network/system access (logical) only    |

1. **HHS ID Badge (PIV Card):** In accordance with HSPD-12, the HHS ID Badge shall be the primary ID badge used to facilitate physical access to NIH facilities and enable strong authentication for access to NIH networks, information systems, and information. Use of the HHS ID Badge to authenticate users of NIH networks, applications, and physical access control systems provides a higher level of assurance than by user name and password.

- a. **Eligibility:** PIV-eligible staff includes most individuals who require physical access for more than six months. For a complete, list of eligible categories, please see appendix A. All PIV-eligible staff must be sponsored by an approved authority. At the NIH, Institute and Center (IC) Administrative Officers (AO),

who have undergone specific training, serve as authorized sponsors. All sponsorship actions for HHS ID Badges must be completed through the NIH Enterprise Directory (NED). A PIV Card will not be issued to a person if:

- i. The individual is known to be or reasonably suspected of being a terrorist;
- ii. The employer is unable to verify the individual's claimed identity;
- iii. There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;
- iv. There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;
- v. There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or
- vi. There is a reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

**b. Supplemental Credentialing Standards:** NIH has the flexibility to apply supplemental credentialing standards in addition to the six basic standards above. The supplemental standards are intended to ensure that the granting of a PIV Card to an individual does not create unacceptable risk, when the individual is not subject to an adjudication of suitability for employment in the competitive service under 5 CFR part 731, of qualification for employment in the excepted service under 5 CFR part 302 or under a similar authority, or of eligibility for access to classified information under E.O. 12968. These standards may be applied based on the risk associated with the position or work on the contract.

NIH may consider denying or revoking a PIV Card to an individual based on one of these supplemental credentialing standards. In the following standards, an "unacceptable risk" refers to an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects.

- i. There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV Card poses an unacceptable risk;
- ii. There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV Card poses an unacceptable risk;
- iii. There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a PIV Card poses an unacceptable risk;

- iv. There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV Card poses an unacceptable risk;
- v. There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV Card poses an unacceptable risk;
- vi. A statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV Card poses an unacceptable risk; or
- vii. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

c. **Issuance:** All staff eligible for an HHS ID Badge require, at a minimum, a National Agency Check with Written Inquiries (NACI) (or higher) federal background investigation. Issuance of an HHS ID Badge requires, at a minimum:

- i. The completion of a Federal Bureau of Investigation (FBI) fingerprint check, with favorable results. The cost of the FBI fingerprint check is borne by the NIH Institute or Center requesting the HHS ID Badge (PIV Card).
- ii. The initiation of a federal background investigation, the cost of which is also borne by the NIH Institute or Center requesting the investigation. Initiation is defined as:
  - The proper completion of the e-QIP electronic questionnaire and other required background investigation forms by the individual;
  - Review of the background investigation forms by the Division of Personnel Security and Access Control (DPSAC) for accuracy and completeness; and
  - Submission of the investigative request to the Office of Personnel Management (OPM).

Once these requirements are completed, the individual may be issued an HHS ID Badge (PIV Card).

Applicants with a completed NACI (or higher) identified as adjudicated and closed in the OPM's Central Verification System (CVS) need not be reinvestigated if they have not had a break in service exceeding 24 months. A fingerprint check is not required although collection of two fingerprints remains a requirement to support biometric matching on the HHS ID Badge (PIV Card).

Adjudication of background investigations for NIH PIV-issuance purposes shall be conducted in accordance with the requirements outlined in the

HHS Personnel Security & Suitability Policy and the HHS Personnel Security/Suitability Handbook.

Failure to comply with the background investigation process will result in the removal of physical and/or logical access and may result in administrative actions up to and including termination.

- d. **Badge Color Coding:** The HHS ID Badge shall be color coded, as indicated in the table below. The color coding shall be used as a background stripe behind the employee's name.

**Figure 2 HHS ID Badge Color Coding**

|                     |  |
|---------------------|--|
| <b>White Stripe</b> | NIH federal employees (Note: Common Access Cards issued to U.S. Public Health Service Commissioned Corps members also will have white stripe.)                   |
| <b>Green Stripe</b> | U.S.- National staff working under a contract with NIH or under an affiliate classification (i.e., Fellow, Special Volunteer, Guest Researcher, or Collaborator) |

- e. **Acceptance:** The HHS ID Badge (PIV Card) issued in accordance with all applicable HSPD-12 provisions and as such meets the reciprocity requirements and may be accepted by other HHS Operating Divisions (OpDivs), federal departments or agencies in accordance with their suitability/security policies.

**2. Restricted Local Access (RLA) Badges:**

- a. **Eligibility:** RLA Badges are issued to all NIH staff members who are foreign nationals (including lawful permanent residents), short-term staff (less than 6 months), and intermittent staff who require access to NIH system (logical access) and/or access to NIH facilities (physical access), but do not qualify for an HHS ID Badge (PIV Card). For a complete list of eligible categories, please see Appendix A. All RLA-eligible staff must be sponsored by an approved authority, i.e., an Institute or Center AO. At the NIH, Administrative Officers (AO), who have undergone specific training, serve as authorized Sponsors. All sponsorship actions for RLA Badges must be completed through the NIH Enterprise Directory (NED).
- b. **Issuance:** All staff eligible for an RLA Badge will require a favorable FBI fingerprint check for final issuance. Foreign nationals (including Lawful Permanent Residents) are also required to complete a National Agency Check (NAC) or other appropriate background investigation. Initial issuance of an RLA Badge to foreign nationals requires, at a minimum:
  - i. The completion of an FBI fingerprint check, with favorable results.

ii. Initiation or the successful completion of a NAC or other appropriate background investigation. This process includes but is not limited to the following actions:

- The proper completion of the security questionnaire via the electronic e-QIP questionnaire and other required background investigation forms;
- Review of required background investigation forms by DPSAC for accuracy and completeness; and
- Submission of the investigative request to the OPM.

c. **Badge Color Coding:** The RLA Badge shall be color coded, as indicated in the table below. The color coding shall be used as a background stripe behind the employee's name.

**Figure 3 RLA Badge Color Coding**

|                          |   |
|--------------------------|---|
| <b>Orange<br/>Stripe</b> | All foreign nationals (including Lawful Permanent Residents), short-term and intermittent staff |
|--------------------------|---|

d. **Acceptance:** Restricted Local Access (RLA) Badges are issued in accordance with NIH security policies with no reciprocity expressed or implied on the part of other HHS OpDivs or federal departments or agencies.

### 3. Local-Based Physical Access (Legacy) Badges:

- Eligibility:** Local-Based Physical Access (Legacy) Badges are issued to individuals that require unfettered physical access to NIH facilities, but are not eligible for an HHS ID Badge (PIV Card) or RLA Badge. For a complete list of eligible categories, please see Appendix A. All Legacy-eligible staff must be sponsored by an approved authority. At the NIH, Administrative Officers (AOs), who have undergone specific training, and other entities designated by the Office of Research Services (ORS) or the Office of Security and Emergency Response (SER) serve as authorized Sponsors.
- Issuance:** All staff eligible for a Legacy Badge will require a favorable FBI fingerprint check or, in certain circumstances, a name check for final issuance.
- Acceptance:** Legacy Badges are issued in accordance with NIH security policies with no reciprocity expressed or implied on the part of other HHS OpDivs or federal departments or agencies.

### 4. Alternate Logon Token (ALT) Card:

- Eligibility:** ALT Cards will be issued to NIH secondary account holders who already possess an active HHS ID Badge (PIV Card) or RLA Badge.

These ALT cards are issued to individuals who require access to NIH systems using logical attributes (e.g. administrator rights) that are different from those available on the individual's HHS ID Badge (PIV Card). An example would be an IT professional who would need to install software on a computer as the account administrator.

To prevent intentional or inadvertent unauthorized access to information or systems, NIH has established procedures, including separation of duties (as listed below in the ALT Role Descriptions), to assure that logical attributes are accurate.

Only staff from NIH owning the relevant logical systems can act as Sponsor and directory administrator for any ALT Card. ALT Cards will contain, at a minimum, authentication certificates for logical access to NIH networks.

## D. References

1. [Homeland Security Presidential Directive \(HSPD\) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004](#)
2. [OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive \(HSPD\) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," dated February 3, 2011](#)
3. [OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive \(HSPD\) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 5, 2005](#)
4. Memorandum from Deputy Secretary to HHS Staff and Operating Division Heads, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors," dated April 15, 2011
5. [Federal Information Processing Standards 201 Standard \(most current version is FIPS 201-2\), "Personal Identity Verification of Federal Employees and Contractors." August 2013](#)
6. [Federal CIO Council, "Personal Identity Verification Interoperability for Non-Federal Issuers," dated May 2009](#)
7. HHS/ASA/OSSI, ["HHS Personnel Security & Suitability Policy"](#) and ["Personnel Security/Suitability Handbook."](#)
8. [OPM Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," – dated July 31, 2008](#)
9. [Federal Identity, Credential and Access Management \(FICAM\) Roadmap and Implementation Guidance v2.0, dated December 2011](#)
10. [Office of Personnel Management \(OPM\) Federal Investigations Notice No. 06-04, "HSPD-12" – Advanced Fingerprint Results," dated June 8, 2006](#)
11. [National Institute of Standards and Technology \(NIST\) Special Publication 800-79-1 \(SP 800-79-1\), "Guidelines for the Accreditation of Personal Identity Verification Card Issuers," dated June 2008](#)

12. [NIH Manual Chapter 1743, "Keeping and Destroying Records"](#)

## E. Definitions

1. **Alternate Logon Token (ALT) Card** - Logical Access Card issued through the HSPD-12 Program that is not graphically personalized, that contains an embedded computer chip, and is used exclusively for logical access. Situations in which an ALT Card might be issued include where alternate logical attributes are needed (e.g., system administrator) and where temporary or backup logical access is required.
2. **Affiliates** - A range of individuals who are not federal government employees or contractors but who have an official business relationship with the NIH (e.g., Fellows, Guest Researchers, Special Volunteers, medical staff, student healthcare providers, visiting scientists, volunteers, etc.).
3. **Applicant** - An individual applying for an HHS ID Badge (PIV Card). The applicant may be a current or prospective federal hire, a federal employee, a contractor, or an affiliate
4. **Biometric (or biometric information)** - The stored, measurable, electronic information pertaining to physical characteristics or personal behavioral traits used to recognize the identity or verify the claimed identity of an applicant. Includes facial images, fingerprints, and iris scan samples. Facial images and fingerprint templates (sample data points of the fingerprint) are included as biometric information on the HHS ID Badge (PIV Card) and the RLA Badge.
5. **Card Management System** - The HHS system that supports the full lifecycle of the HSPD-12 Access Cards Management Program.
6. **Cardholder** - An individual possessing an ID badge.
7. **Common Access Card (CAC)** - A PIV Card issued by the Department of Defense (DoD), including to U.S. Public Health Service Commissioned Corps personnel.
8. **Contractor** - Any individual (industrial, commercial, or other entity) who has executed a contract with the NIH (or one of its components) or who is employed by a company that has executed a contract with the NIH (or one of its components) for the purpose of performing work for the agency.
9. **Employee** - Includes federal employees, as defined by 5 U.S.C. § 2105, who are employed by HHS and positions in the U.S. Public Health Service Commissioned Corps, as defined by 42 U.S.C. § 204.
10. **e-QIP** - Office of Personnel Management's (OPM) Electronic Questionnaires for Investigation Processing (e-QIP), which is the online system to gather information required to conduct background investigations for federal security, suitability, fitness and credentialing purposes.
11. **Facilities** - Includes all NIH-owned or -controlled property.
12. **Foreign Nationals** - An alien, i.e., any person not a citizen of the United States or born outside the jurisdiction of the United States; a citizen of a foreign country; not a naturalized U.S. citizen under U.S. law. This includes legal permanent residents, also known as permanent resident aliens (22 U.S.C. § 6023(8) and 8 U.S.C. § 1101(a)(3)).
13. **Information System (or Information Technology System)** - The discrete set of information resources organized for the collection, processing, maintenance, use,



- sharing, dissemination, or disposition of information, as defined by the Federal Information Security Management Act of 2002 [(44 U.S.C. § 3502(8)].
14. **Local Based Physical Access Badge** - ID badge that is graphically personalized for visual identification that does not contain an embedded computer chip, and is only used for physical access.
  15. **Minor** - Anyone below age 16 and not eligible for an ID Badge, e.g. Latchkey Children. An NIH employee, as a parent can self-sponsor his or her child for an Accompanied Child Visitor Pass (ACVP), a non-technology badge, at no additional cost.
  16. **National Agency Check (NAC)** - A personnel security investigation, including fingerprint check, involving searches of the OPM Security/Suitability Investigations Index (SII); Defense Clearance and Investigations Index (DCII); Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary.
  17. **National Agency Check with Inquiries (NACI)** - A personnel security investigation combining a NAC plus written inquiries to law enforcement agencies, former employers and supervisors, references, residential verifications, and schools covering the past five years. NACIs are valid indefinitely (i.e., have no expiration date), provided that the individual has not had a break in service of more than 24 months.
  18. **Operating Division (OpDiv)** - An organizational component of the HHS, which also includes the Office of the Secretary (OS).
  19. **Personal Identity Verification (PIV) Card** - Known as the HHS ID Badge, this badge is graphically personalized with the holder's photo, contains an embedded computer chip and meets the technical specifications of FIPS – 201 Standard.
  20. **PIV Card Issuance Facility (PCIF)** - A PCIF is a physical site or location including all equipment, staff, and documentation that is responsible for carrying out one or more of the following PIV functions: enrollment/identity proofing; card production; card activation/issuance; or maintenance.
  21. **PIV Card Issuer (PCI)** - An OpDiv-level program responsible for providing ID badges.
  22. **Renewal** - Issuance of a new ID badge to an individual who is in possession of an unexpired and undamaged badge at the time of the renewal request.
  23. **Restricted Local Access (RLA) Badge** - An ID badge that is graphically personalized (including picture) to establish the holder's identity, contains an embedded computer chip, and meets the majority of the technical specifications of FIPS-201 Standard. Issuance of the RLA Badge is generally limited to NIH staff that are foreign nationals, short-term or intermittent staff requiring physical and logical access.
  24. **The Senior Authorizing Official (SAO)** - OpDiv individual who is responsible for all PIV Card Issuance (PCI) operations. The SAO has budgetary control, provides oversight, develops policy, and has authority over all functions and services provided by the PCI.
  25. **Sponsor** - A person affiliated with NIH (usually a trained AO) who verifies and authorizes the applicant's need for an ID badge, and initiates the badge enrollment and issuance process.

## **F. Responsibilities**

### **1. HSPD-12 Program Manager**

The HSPD-12 Program Manager serves as the NIH Senior Authorizing Official (SAO) and PIV Card Issuing Manager (PCIM) and manages the day-to-day operations of all PIV Card Issuing Facilities (PCIF). The HSPD-12 Program Manager is a federal employee, within DPSAC/SER/ORS, responsible for the administration and implementation of the HSPD-12 program within and across the NIH.

- a. Implements all operating procedures, ensures that all processes adhere to the requirements of the FIPS-201 standard and ensures all ID badge services performed at NIH are carried out in a consistent and reliable manner in accordance with HHS and OPM policies.
- b. Appoints personnel to fulfill the roles and responsibilities defined in FIPS-201 and this policy.
- c. Operates as the Role Administrator to grant system privileges to role holders. The Role Administrator duties can be delegated by the PCIM however all who hold the position of Role Administrator cannot perform any other roles in the process. The Agency Role Administrator is the individual responsible for managing the agency's Sponsor, Adjudicator, Registrar, and Issuer/Activators. The Agency Role Administrator will verify that the appropriate separation of duty policies are followed and will verify that all the training certification requirements have been met. All Role Administrators must complete the web-based HSPD-12 Role Administrator training, be certified and designated by HHS, and be sponsored before beginning HSPD-12 responsibilities.
- d. Responsible for ensuring NIH compliance and organizing submission of required reports to the HHS SAO.

### **2. Administrative Officer (Sponsor)**

Administrative Officers (AOs) with the required special training will serve as Sponsors. The Sponsor substantiates the need for an ID badge to be issued to the individual. This act is called sponsorship. The Sponsor requests the issuance of an ID badge to the individual. The Sponsor shall remain aware of the individual's status and continuing need for holding an ID badge as well as provide any updates to their information or status in NED.

### **3. Enrollment Official**

The individual responsible for confirming sponsorship, ensuring completion of an FBI fingerprint check, background investigation at the NACI level or higher, enrollment, identity proofing, and collecting biographic information such as a facial image and fingerprints. Enrollment Officials initiate background investigations when an individual has none on record.

### **4. ID Badge Issuer**

Authorized personnel responsible for producing and activating an ID badge following the completion of all identity proofing, background investigations, and related

requirements.

## **5. ID Badge Applicant/Holder**

- a. Provides requested documentation for proof of identity in accordance with HSPD-12, FIPS-201, HHS, OPM and NIH policies and procedures. This may include disclosure of personal information to initiate a background investigation or FBI fingerprint check. Providing personal information is voluntary; however, if an individual chooses not to provide the required information, s/he will not meet the job requirements and will therefore not be considered further. If the individual is already employed by NIH, administrative actions may be taken.
- b. Allows NIH or its representatives to capture biometric data (minimally two fingerprints and digital facial image).
- c. Authorizes NIH to perform an appropriate background investigation based on personnel roles/categories and sensitivity of resources to be accessed in accordance with federal guidelines.
- d. Wears/displays/safeguards the ID badge as required by applicable security policies and use the credential provided to access NIH facilities and resources.
- e. Notifies AO or badge issuance location of a lost, stolen, or damaged credential within 24 hours of noting its disappearance.
- f. Surrenders credential upon termination, departure, or official request. Failure to surrender badge will be reported to the Division of Police as possessing unauthorized property. When possible, withholding of payments may be authorized.

## **6. HSPD-12 Senior Agency Official for Privacy (SAOP)**

- a. Responsible for issuing policy, guidelines, and providing oversight with respect to collection and handling of credentials and other personally identifiable information (PII) from individuals.
- b. Ensures the PCI is in compliance with all relevant directives of the privacy laws and policies including, but not limited to FIPS 201, the [E-Government Act of 2002 \[E-Gov\]](#), the [Privacy Act of 1974 \[PRIVACY\]](#), [OMB Memorandum M-03-22](#), and OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

## **G. Procedures**

### **1. Lost, Stolen, Damaged or Forgotten ID Badges**

Reissuance due to a lost, stolen, or damaged ID badge does not require the individual to repeat the entire identity proofing and registration procedure. Those who need immediate access to NIH logical resources may be allowed by the Center for Information Technology (CIT) to use their User ID (Name) and password for a temporary period of time (e.g., 24 hours).

HHS ID Badge (PIV Card) and RLA Badge holders must report a lost or stolen badge to their AO immediately to allow the badge to be revoked as well as request a replacement. The AO must report the badge as lost or stolen in NED. The individual will then be instructed to appear at an ID badge issuance station for reissuance and must bring a state or federal government issued picture ID.

Lost or stolen Legacy Badges should be reported to an ID badge issuance office immediately for revocation and reissuance.

Damaged (i.e., broken) ID badges should be brought to an NIH ID badge issuance office. The local badge issuance office will determine whether to replace or fix the ID badge.

HHS ID Badge (PIV Card) and RLA Badge holders who have forgotten their ID badge should refer to local IC policy for logical access.

It is expressly forbidden to exchange, borrow or loan any of these credentials to another person for any reason. Counterfeiting, altering, or misusing a federal identification credential is punishable under Section 499, Title 18 of the U.S. Code.

- 2. Assessments and Accreditations** The HHS HSPD-12 Program Office will initiate Assessments and Accreditations every three years, or upon any major changes concerning applicants or processes. [NIST Special Publication 800-79-1, Guidelines for the Accreditation of Personal Identity Verification Card Issuers](#), provides guidance on how federal agencies issue, and prepare to issue, PIV Cards that comply with FIPS-201. These guidelines describe a set of attributes that should be exhibited by a PCIF in order to be accredited. They will be used for assessing the reliability of HHS organizations providing its PIV services.

Note that use of SP 800-79-1 for accrediting the reliability of a PCI must be done in addition to accrediting the security of computer systems used by the PCI by using [SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems](#) and [SP 800-53, Recommended Security Controls for Federal Information Systems as guidance](#).

### 3. Identity Proofing

Applicants are required to provide two identity documents in their original form. NIH is required to verify these documents to reasonably validate the claimed identity during the ID badge enrollment and issuance process. Consistent with applicable law, at least one of the two required identity documents provided at enrollment, and the single identity document required at issuance, shall be an unexpired federal or state government issued picture identification (ID). The photo ID requirement cannot be waived, consistent with applicable statutory requirements.

## 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.

Unauthorized possession of an ID badge can be criminally prosecuted under 18 U.S.C. §§ 499 and 701, which prohibit photographing or otherwise reproducing or possessing HHS identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both.

NIH administrative staff are required to revoke ID badges for the departing staff member prior to or on the day of departure. NIH administrative staff, supervisors, project officers, or other responsible points of contact (refer to local IC policy) must retrieve any and all ID badges from departing staff and return them to their local badge issuance location. ALT Cards must be collected and returned to the IC ALT Card Coordinator.

## I. Internal Controls

- 1. Office Responsible for Reviewing Internal Controls Relative to this Chapter:** The NIH HSPD-12 Program, Division of Personnel Security and Access Control (DPSAC), Office of Security and Emergency Response (SER), Office of Research Services (ORS), is responsible for ensuring that internal controls are implemented and working properly to include identity proofing, enrollment, badge issuance and maintenance of physical access control systems. Internal controls include ongoing monitoring of business processes to issue ID badges and conducting self-assessments of each PCIF.
- 2. Frequency of Review:** The DPSAC HSPD-12 Program 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.
- 3. Method of Review:** The DPSAC HSPD-12 Program will ensure effective implementation and compliance with this policy by analyzing NIH community feedback, reviewing system-generated reports and communicating with internal resources for non-compliance of this policy.

**Type of Review:** On-going internal risk assessments.

- 4. Review Reports are sent to:** Associate Director for Security and Emergency Response (ADSER); Director, ORS; Director, Division of Personnel Security and Access Control (DPSAC).

## Appendix A: NIH Badging Table

This table outlines the types of ID badge and security check required for various categories of individuals at the NIH.

| Badging Authority Chart   |                      |  |                         |                    | Revised:<br>6/24/15 |               |
|---|----------------------|--|-------------------------|--------------------|---------------------|---------------|
| Badge Type  | Classification       | Description  | NED <sup>1</sup> Record | Badging Authority  | Check               | Badge Length  |
| HHS ID Badge (PIV Card) or RLA Badge - Long-Term, more than 6 Months <sup>2</sup> | NIH Employees (FTEs) | Includes an individuals who are Wage Grade, Wage Leader, Wage Supervisor, General Schedule, Senior Executive Service, Scientific and Professional, Senior Biomedical Research Service, Title 42, Title 38, Title 32, Senior Leaders, and PHS Commissioned Corps and Students (other than summer students). | Yes                     | DPSAC <sup>3</sup> | BI <sup>4</sup>     | Up to 5 years |
|   | Contractors          | Contract staff who are paid by their employers, not by the NIH for services rendered via a procurement vehicle that provides program support services. Includes: Construction Management Personnel, Clinical /   | Yes                     | DPSAC              | BI                  | Up to 5 years |

|  |                   |   |     |       |    |               |
|--|-------------------|---|-----|-------|----|---------------|
|  |                   | Research / Administrative staff positions, Cafeteria Workers, Housekeeping Staff, Parking Lot Attendants and Shuttle Bus Drivers.   |     |       |    |               |
|  | Fellows           | Individuals who are appointed as trainees and receive NIH stipends. Includes Visiting Fellows, Intramural Research Training Award (IRTA) Fellows, and Cancer Research Training Award (CRTA) Fellows.  | Yes | DPSAC | BI | Up to 5 years |
|  | Guest Researchers | Guest Researchers are scientists, engineers, and students who are permitted to engage in scientific studies and investigations using NIH facilities. Under this program, these individuals further their own research by using equipment and resources that are otherwise | Yes | DPSAC | BI | Up to 5 years |

|                                     |   |   |     |       |                  |               |
|-------------------------------------|---|---|-----|-------|------------------|---------------|
|                                     |   | unavailable to them. They provide no direct services to NIH. They may not have any patient contact.   |     |       |                  |               |
|                                     | Collaborators (Clinical and Non-Clinical) | A non-NIH employee or trainee, employed by or associated with an outside organization, who performs clinical and/or non-clinical research or rotations at/or for NIH, pursuant to an agreement. Includes individuals on a CRADA or any other type of agreement. | Yes | DPSAC | BI               | Up to 5 years |
|                                     | Special Volunteers                        | Special Volunteers are individuals who provide research services, direct patient care, clerical support, technical assistance, or any other necessary services to the NIH.  | Yes | DPSAC | BI               | Up to 5 years |
| Restricted Local Access (RLA) Badge | Any Short-Term Individuals                | Any classifications of individuals who meet the above descriptions for  | Yes | DPSAC | SAC <sup>6</sup> | 6 months      |



|   |  |  |        |                  |     |              |
|---|--|--|--------|------------------|-----|--------------|
|   |  | an HHS ID Badge (PIV Card), but will be at NIH for less than 6 months  |        |                  |     |              |
|   | Summer Students                            | Temporary, full and part-time NIH employees and FAES employees who are summer hires (at NIH during summer months only).  | Yes    | DPSAC            | SAC | 9/30 of CY   |
| Legacy Badge-Extended Visitors: Individuals who are not directly or indirectly paid by the NIH nor conduct research at the NIH. Sponsor must be a PIV-Approved AO | Tenants <sup>8</sup>                       | Non-NIH Employees who are connected to ORF and ORS in providing support services to the entire NIH. Includes, but not limited to: R&W staff, FAES, FNIH , NIH Credit Union staff, Children's Inn staff, and Child Care Center staff. | Yes/No | DP <sup>11</sup> | SAC | Up to 1 year |
|   | Volunteers (other than Special Volunteers) | A non-paid individual who provides a service to the NIH. Includes, but is not limited to: Red Cross, Sunday Supper Providers, Patient Ambassadors, Playroom Attendants, Family Friends, Language                                     | Yes    | DP               | SAC | Up to 1 year |

|  |                      |  |     |    |     |              |
|--|----------------------|--|-----|----|-----|--------------|
|  |                      | Interpreters, Patient Greeters, Social Worker Interns, and participants in an IC's volunteer internship program. These individuals may come at any time throughout the year. |     |    |     |              |
|  | Clinical Rotators    | A medical or dental student who participates in a 4 - 15 week clinically oriented elective rotation in one of the specialty fields and biomedical disciplines at the NIH.    | Yes | DP | SAC | 6 months     |
|  | Service Providers    | Individuals who have an employment relationship to provide services which support the NIH mission. (Examples: UPS, FedEx, vending machine or food suppliers, movers, etc.)   | No  | DP | SAC | Up to 1 year |
|  | Construction Workers | Individuals who support NIH construction efforts and are not employees of the NIH. This category may get a Visitor Badging   | No  | DP | SAC | Up to 1 year |

|                                   |  |   |                          |    |                    |               |
|-----------------------------------|--|---|--------------------------|----|--------------------|---------------|
|                                   |  | System (VBS) Badge issued by the Division of Police (DP).   |                          |    |                    |               |
|                                   | Alumni   | An individual who previously worked at the NIH and would like to continue research in an ad-hoc capacity.   | No                       | DP | SAC                | Up to 1 year  |
|                                   | Transportation Visitor <sup>12</sup>                                 | An individual who needs physical access to an NIH campus and/or transports an NIH employee to work or a child to an NIH day care facility (Taxi drivers go through CVIF and traditionally get no ID badge). | No                       | DP | SAC                | Up to 1 year  |
| Flash Pass (Non-technology badge) | Grounds Maintenance  | Individuals who provide landscaping, snow removal, and other services to the grounds.   | No                       | DP | SAC                | Up to 1 year  |
|                                   | NIH related Board Members/Special Government Employees <sup>13</sup> | Non-NIH staff who are Members of an NIH or IC Advisory Committee, Board or Council or Program Advisory Committee. Special Government Employees are  | No/Ye<br>s <sup>14</sup> | DP | NCIC <sup>15</sup> | Up to 3 years |

|  |                            |  |    |    |      |              |
|--|----------------------------|--|----|----|------|--------------|
|  |                            | also included in this category.  |    |    |      |              |
| Legacy Badge: No Full Background Check | Retirees                   | An individual who has retired from the NIH and would like to continue research and support for his/her IC in an ad-hoc capacity.   | No | DP | NCIC | Up to 1 year |
|  | Patient Guardian/Caregiver | A maximum of two (2) Patient Escorts/Visitors per patient.   | No | DP | NCIC | Up to 1 year |
|  | NIH Residents              | Non-NIH employees who reside on the NIH campus.  | No | DP | NCIC | Up to 1 year |
|  | Patients                   | Patients/Protocol Participants   | No | DP | NCIC | Up to 1 year |
|  | Blood & Platelet Donors    | Donors who visit the NIH with the purpose of donating blood or platelets to the Clinical Center.   | No | DP | NCIC | Up to 1 year |
|  | Medical Professionals      | Medical Practitioners are individuals working at other medical institutions who attend lectures, such as Grand Rounds, WALS, etc. This supports the NIH mission of education and sharing research in the medical | No | DP | NCIC | Up to 1 year |

---

|  |  |        |  |  |  |  |
|--|--|--------|--|--|--|--|
|  |  | field. |  |  |  |  |
|--|--|--------|--|--|--|--|

---

<sup>1</sup>NIH Enterprise Directory (NED)

<sup>2</sup>Foreign nationals (including Lawful Permanent Residents) will be issued an RLA Badge in lieu of an HHS ID Badge (PIV Card)

<sup>3</sup> Division of Personnel Security and Access Control (DPSAC)

<sup>4</sup> Background Investigation (BI)

<sup>5</sup> Cooperative Research and Development Agreement (CRADA)

<sup>6</sup> Special Agency Check = Fingerprints sent to Office of Personnel Management (OPM) for criminal history check

<sup>7</sup> Foundation for Advanced Education in the Sciences (FAES)

<sup>8</sup> Not all Tenants are entered into NED

<sup>9</sup> Recreation and Welfare (R&W)

<sup>10</sup> Foundation for the National Institutes of Health (FNIH)

<sup>11</sup> Division of Police (DP)

<sup>12</sup> The sponsoring Institute or Center (IC) must pay for the individual's FBI fingerprint check.

<sup>13</sup> May also include but are not limited to physicians that come to campus for the Director of the NIH Clinical Center or NIH Director and only get a one year badge upon completion of NCIC check.

<sup>14</sup> Special Government Employees (SGEs) are entered into NED, however Board Members are not entered into NED.

<sup>15</sup> National Crime Information Center (NCIC)