US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/17/2025

OPDIV:

NIH

Name:

Physical Access Control System-Continuum Interconnectivity System (PACSIS)

PIA Unique Identifier:

P-5682828-754512

The subject of this PIA is which of the following?

Electronic Information Collection

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

There is no change to this system. This validation is intended to refresh content and update the status of Physical Access Control System-Continuum Interconnectivity System (PACSIS).

Describe the purpose of the system.

The NIH Physical Access Control System Interconnectivity (IS) middleware (PACSIS) is used to collect and send all NIH badge requests at the Bethesda location to NIH Physical Access Control System-Continuum (PACS-C), which is responsible for granting physical access to NIH facilities.

Describe the type of information the system will collect, maintain (store), or share.

PACSIS collects, maintains, and shares the following personally identifiable information (PII): Full name, work address, email, phone number, badge photo, biometric (fingerprint), Department of Health and Human Services (HHS) Personal Identity Verification (PIV) card number, Operating Division (OPDIV), employment status, and Federal Agency Smart Credential Number (FASC-N), including card expiration date, username, and personal identification number (PIN). Data is

collected for all NIH employees (federal and contractors). The PACSIS system combines the data from NIH Enterprise Directory (NED) and HHS Smart Card Management System (SCMS) before sending the data to PACS-C system. NED and PACS-C maintain their own Privacy Impact Assessments (PIAs), including all legal authorities documented. The PACSIS system component does store the data and after transformation shares it with PACS-C (current) system and PACS-AE (new) system.

NIH employees log into the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

PACSIS is used to collect and send all NIH badge requests at the Bethesda location to PACS-C, which is responsible for granting physical access to NIH facilities.

The PACSIS collects, maintains, and shares the following PII: Full name, work address, email, phone number, badge photo, biometric (fingerprint), HHS PIV card number, OPDIV, employment status, and FASC-N, including card expiration date, username, and PIN. Data is collected for all NIH employees (federal and contractors). The PACSIS system combines the data from NED and HHS SCMS before sending the data to PACS-C system. NED and PACS-C maintain their own Privacy Impact Assessments (PIAs), including all legal authorities documented.

NIH employees log into the system using the IAM Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
Photographic Identifiers
Biometric Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
HHS PIV Card number
OPDIV
FASC-N (including card expiration date, username, and PIN)

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Volunteers, retirees, extended visitors, special government employees (NIH board members), service providers, and Tenants.

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The primary purpose of the PII is for electronic information collection and data transformation of the NED and SCMS data required by the PACS-C for physical access to NIH facilities.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 301; 5 U.S.C. 5901; 5 U.S.C. 7903; 40 U.S.C. 318a; 42 U.S.C. 241

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0216, Administration: NIH Enterprise Directory

09-25-0054 Administration: Property Accounting (Card Key System) HHS/NIH/ORS

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

1615-0047, Employment Eligibility Verification: 05/31/2027

3206-0182, Declaration for Federal Employment: 08/31/2026

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Several Interconnection Security Agreement (ISA) exists with Center for Information Technology (CIT) for the secure connection to HHS systems. Another ISA exists between NED for the secure connection to support the Homeland Security Presidential Directive (HSPD-12) PIV Production.

PACS-C maintains ISA for PACSIS (Electronic Information Collection) with:
NIH Enterprise Directory System (NED)
HHS Smart Card Management System (SCMS)
National Institute of Environmental Health Sciences (NIEHS)
National Cancer Institute (NCI)

Describe the procedures for accounting for disclosures.

Written requests to the System Manager are reviewed to determine if a record exists. The requester must also verify his or her identity by providing either a notarization of the request or a written certification and understands that the knowing and willful request for acquisition of a record under false pretenses is a criminal offense. During the time of PII collection, the Division of Personnel Security (DPS) office notifies the individual any disclosures for PII use. PACSIS' audit logs are reviewed weekly by System Owner(s)/System Administrators.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals understand they are required to provide their information as part of the onboarding process. Opportunities to further understand the use of their PII occur during the completion of the Electronic Application (eAPP) Questionnaire for Investigations Processing profile, including the provision of background information. eAPP is a web-based automated system used in collecting information from individuals for employment background investigation.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

PII is derived from NED. There is no opt-out option. The information collection is required as part of the hiring process. Individuals may decline to give the PII, but then they would not be able to work for NIH. NED maintains its own PIA, including all legal authorities.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

NED is the source system. Consent for major changes is handled by NED. NED maintains its own PIA, including all legal authorities.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals may contact the NIH Information Technology (IT) Service Desk and if necessary, a ticket is assigned to the PACSIS operations and support team for action. For information that downloads from NED, individuals may also contact the NED team directly at nedteam@mail.nih.gov. An email request is planned for use to obtain individual consent. As such the NIH global email system is in place and capable of reaching NIH PIV card holders.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

PACSIS undergoes regular and periodic reviews. The PII is downloaded from NED is reviewed when HHS PIV cards also known as badges are renewed. The timeline for badge renewal depends upon the type of badge and typically ranges from one (1) year to five (5) years. Alternatively, individuals have the option to conduct ad hoc reviews of their own PII through NIH NED Self Service.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Information system users are approved by PACS-C System Owner management for PACSIS access based on their technical/functional role in administering, developing, and supporting the daily job functions of PACSIS.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Annual review of system users' roles are done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions of PACSIS.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Users with additional roles for system administration, risk management, leadership, continuity of operations and safety receive additional training for ethics, equal opportunity and diversity, The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act), and use of strategic sourcing.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the NIH Records Retention schedule Records Schedule System .

Item 07-105, Information Technology Operations and Maintenance records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications.
Disposition: Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA-GRS-2013-0005-0004).

Item: 07-204: System access records. Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA-GRS-2013-0006-0004)

Item: 07-211: Public Key Infrastructure (PKI) transaction-specific records and Item: 07-209: PKI administrative records.
Records relate to transaction-specific records that are generated for each transaction using PKI digital signature technology (N1-GRS-07-3, item 13b), and records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process (N1-GRS-07-3, item 13a1).
Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the

maximum level of operation of the CA, or when no longer needed for business, whichever is later.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.