US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/06/2025

OPDIV:

NIH

Name:

Secure Physical Access Control and Environmental Systems (SPACES)

PIA Unique Identifier:

P-9913522-772476

The subject of this PIA is which of the following?

Minor Application (child)

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.

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

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

The Secure Physical Access Control & Environmental System (SPACES) is an on-premises, enterprise physical access control system that integrates and manages physical access devices, authorization services, video surveillance, and emergency communication for the National Cancer Institute (NCI) facilities. SPACES validates NIH-issued personal identity verification (PIV) cards to control access to the facility when the clearance of the PIV card matches the clearance of authorized for the given facility.

The system also records video in NCI buildings and provides on-site officers with a unified interface for monitoring video events in real time. In addition, SPACES manages emergency communication devices located throughout the facility’s parking garage.

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

NCI's Physical Access Control (PACS) is interconnected with the NIH Physical Access Control System-Interconnected system (PACSIS), which maintains its own Privacy Impact Assessment (PIA), including all legal authorities documented.
When an individual, e.g. employee or contractor, is issued a PIV card, PACSIS pushes their PIV card records to SPACES and they are able to swipe their PIV card to access NCI buildings.
The PIV card photo will be used in conjunction with video surveillance to verify the individuals identity. The video images are stored on disks and can be reviewed when a security violation occurs.
In addition, SPACES accesses the following information when authenticating the individuals PIV card:
Name
HHS ID to uniquely identify each individual.
NIH site location e.g., State, City.
Standard Administrative Code (SAC)
Agency e.g. NIH
Sex
Clearance
Personnel type e.g. Employee, contractor
Expiration date
HHS Operating divisions (OPDIV)
Date/Time of badge issuance
Card Authentication Key (CAK) and PIV digital certificates
Federal Agency Smart Credential Number (FASC-N)
Credential Serial #- issued to a card during badge issuance.
Card Status (credential/employment status) e.g., Active, disabled temporary, Lost or stolen

These same information is collected from other government agency when importing card record into SPACES.

In addition, SPACES queries certificate authority revocation lists via the Internet using the Online Certificate Status Protocol (OCSP) or the Server-based Certificate Validation Protocol (SCVP).

Users log in to SPACES using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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.

The Secure Physical Access Control & Environmental System (SPACES) is an on-premises, enterprise physical access control system that integrates and manages physical access devices, authorization services, video surveillance, and emergency communication for the National Cancer Institute (NCI) facilities. SPACES validates NIH-issued personal identity verification (PIV) cards to control access to the facility when the clearance of the PIV card matches the clearance of authorized for the given facility.

The system also records video in NCI buildings and provides on-site officers with a unified interface for monitoring video events in real time. In addition, SPACES manages emergency communication devices located throughout the facility’s parking garage.

NCI's Physical Access Control (PACS) is interconnected with the NIH Physical Access Control System-Interconnected system (PACSIS), which maintains its own Privacy Impact Assessment (PIA), including all legal authorities documented.
When an individual, e.g. employee or contractor, is issued a PIV card, PACSIS pushes their PIV card records to SPACES and they are able to swipe their PIV card to access NCI buildings.
The PIV card photo will be used in conjunction with video surveillance to verify the individuals identity. The video images are stored on disks and can be reviewed when a security violation occurs.
In addition, SPACES accesses the following information when authenticating the individuals PIV card:
Name
HHS ID to uniquely identify each individual.
NIH site location e.g., State, City.
Standard Administrative Code (SAC)
Agency e.g. NIH
Gender
Clearance
Personnel type e.g. Employee, contractor
Expiration date
HHS Operating divisions (OPDIV)
Date/Time of badge issuance
Card Authentication Key (CAK) and PIV digital certificates
Federal Agency Smart Credential Number (FASC-N)
Credential Serial #- issued to a card during badge issuance.
Card Status (credential/employment status) e.g., Active, disabled temporary, Lost or stolen

These same information is collected from other government agency when importing card record into SPACES.

In addition, SPACES queries certificate authority revocation lists via the Internet using the Online Certificate Status Protocol (OCSP) or the Server-based Certificate Validation Protocol (SCVP).

Users log in to SPACES using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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
Employment Status
Sex
Personnel Type, NIH Site Location (City/State), HHS OPDIV, HHS ID, Clearance
Badge Expiration date, Date/Time of badge issuance
FASC-N, SAC Codes, Digital Certificate, Credential Serial Number, Card Status

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose of PII is validation/authentication of PIV cards and credential information for physical access to federal facilities. The photo will be used in conjunction with video surveillance for identification purposes.

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

A development environment is used to mimic the production system for testing, troubleshooting and upgrading systems purposes.

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

5 U.S.C. 301 and 302; 5 U.S.C. 5901; 5 U.S.C. 7903; 40 U.S.C. 318a; 42 U.S.C. 241, 44 U.S.C. 3101 and 3102, and Executive Order 9397.

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)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Government Sources
Within the OpDiv
Other HHS OpDiv
Non-Governmental Sources
Public
Private Sector
Other

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

No

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

SPACES does not directly collect information from individuals through the use of their PIV card. PIV card records are shared from the source system PACSIS. PACSIS combines the data from the NIH Enterprise Directory (NED) and the HHS Smart Card Management System (SCMS),NED and SCMS

maintain their own Privacy Impact Assessments (PIA), including all legal authorities documented. Upstream sources providing data to the SPACES hold responsibility for establishing informed consent, acknowledging safe and responsible usage and sharing of collected data, and notifying the individuals that their personal information is collected.

Although not required, NCI may post signs that inform individuals of surveillance activities, but in some cases, an individual may not have seen or had an opportunity to view posted signage before being observed or recorded on video. For use of video recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy.

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.

PIV card records are not collected by SPACES; therefore, 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. . Individuals may take action to prevent the new or continued collection or use of video surveillance by removing themselves from the area under surveillance. Offering individuals the opportunity to provide affirmative consent to the collection or use of PII is not feasible for the specified use of the system.

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

PIV card records are not collected by SPACES; therefore, there is no process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system. 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. . Individuals may take action to prevent the new or continued collection or use of video surveillance by removing themselves from the area under surveillance. Offering individuals the opportunity to provide affirmative consent to the collection or use of PII is not feasible for the specified use of the system.

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.

PIV card records are not collected by SPACES; therefore, there is no opportunity to resolve individuals' concerns. However, systems providing data to SPACES are responsible for resolving concerns when individuals believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate."

Although not required, NCI may post signs that inform individuals of surveillance activities, but in some cases, an individual may not have seen or had an opportunity to view posted signage before being observed or recorded on video. For use of video recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy.

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

The NIH IT Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use manage or operate NIH applications or systems must attend complete security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management, and Emergency Preparedness). 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).

n/a

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 following NIH Records Retention Schedules:

Item 07-105, Information Technology Operations and Maintenance records
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.
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: 07-209: PKI administrative records.
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.
(N1-GRS-07-3, item 13a1).

Item: 07-211: Public Key Infrastructure (PKI) transaction-specific records.
Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of

operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period. (N1-GRS-07-3, item 13b)

Item : 09-412 Operations and Facilities Management: Facility security management operations records.
Destroy when 30 days old, but longer retention is authorized if required for business use. (DAA-GRS-2021-0001-0003)

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

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.

Technical Controls:
Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls:
Server rooms, LAN closets and NCI Command Center are protected by key lock and Badge/PIV combinations. Visitors enter the facility after signing in and going through the screening process by NCI security personnel located at the front and back entrances. Visitors are escorted by authorized personnel to SPACES controlled area. Visitors are required to fill out the visitor sign-in sheet before accessing SPACES server rooms. The Command Center security personnel verify valid ID and check if the forms are filled out correctly. Visitors are accompanied by NCI technical staff and their activities are monitored until they leave the facility. Security personnel monitor all security cameras, building entrance and exit access point.