U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Physical Access Control System (PACS)
Bureau/Office: Office of Law Enforcement and Security
Date: July 9, 2018
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Office of Law Enforcement and Security (OLES) Interior Complex Security Operations Office operates the Physical Access Control System (PACS) to support their mission to safeguard Department of the Interior (DOI) personnel, property, and information, and to prevent and deter individuals from reaching DOI personnel and controlled areas to which they could pose a security risk.

PACS is the physical security operations system that supports visitor management, physical access control, intrusion detection and video surveillance functions at the Main Interior Building (MIB), DOI's Headquarters facility in Washington, DC, to ensure the safety and security of individuals within the DOI MIB. PACS also stores employee and visitor personally identifiable information (PII) required for ongoing authorization and monitoring of physical access to the MIB, credit union, child day care, etc. Physical and network security access is based on sound criteria to verify an individual's identity that are strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation.

The PACS system contains information on individuals that require regular, ongoing access to the MIB, including DOI employees, contractors, students, interns or volunteers. The system will permit entry to the MIB by authorized employees and contractors as well as members of the public who enroll their children into the General Services Administration (GSA) Child Care Center located in the MIB, with appropriate identification. The system also facilitates building access by (1) individuals authorized to perform or use services provided in DOI facilities, such as the Credit Union or Fitness Center, who have appropriate Federal identification credentials, and (2) employees and contractors working at GSA and Office of Personnel Management (OPM) to access the MIB as part of an "open campus" initiative designed to share building resources. Reciprocal rights will be granted to the MIB personnel to access GSA and OPM buildings.

Visitor management functions consist of records of visitor identity verification, and entry and exit of visitors who require access to the MIB. Visitors are processed through the Visitors' Center and are issued a temporary badge to access the MIB.

Video surveillance consists of Closed Circuit Television (CCTV) operated 24 hours a day. Turnstiles are placed at entry points in the MIB that allow persons to pass through with government issued personal identity verification (PIV) cards.

C. What is the legal authority?

Departmental Regulations (5 U.S.C. 301); Federal Information Security Act (Pub. L. 104-106, section 5113); E-Government Act (Pub. L. 104-347, section 203); Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521); Government Paperwork Elimination Act (44 U.S.C. § 3504); Homeland Security Presidential Directive-12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, Section 3001 (50 U.S.C. 435b); Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons; Executive Order 12968, Access to Classified Information; Federal Property Regulations, July 2002; and Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000704 Physical Access Control System (PACS) System Security Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

DOI-46, HSPD-12: Physical Security Files, 72 FR 11043, March 12, 2007

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Birth Date
☒ Other: *Specify the PII collected.*

PACS collects, verifies, or maintains records on individuals requiring regular access to DOI-controlled facilities and information systems or individuals that are issued HSPD-12 compliant credentials. The PACS system contains the data fields above, as well as the following data fields: signature; hair color; eye color; height; weight; agency affiliation (e.g., employee, contractor, volunteer, etc.); PIV card issue and expiration date; personal identification number (PIN); PIV request form including citizenship and work permit number for foreign national contractors; PIV sponsor approval signature; PIV card serial number; copies of "I-9" documents (e.g., driver's license, passport, etc.); computer system user name; and user access and permission rights. The system contains images and videos collected from audio/visual recording devices such as surveillance cameras and CCTV located at the MIB and perimeter for security purposes, which may also contain vehicle identification, license plate, and state of issuance.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☐ Email
☒ Face-to-Face Contact
☐ Web site
☒ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*

PIV card data is obtained from USAccess during the employee onboarding process. The PACS system verifies employee identity by PIV card data through a card reader.

☒ Other: *Describe*

CCTV and surveillance cameras in the MIB and perimeter.

D. What is the intended use of the PII collected?

PII collected and maintained in PACS is used to ensure only authorized employees and contractors with proper identification are permitted entry into the MIB. PII is used to support visitor management, physical access control, intrusion detection and video surveillance functions at the MIB to ensure the safety and security of individuals. PACS collects, stores, verifies, or maintains PII for ongoing authorization and monitoring of physical access to DOI-controlled facilities and information systems. PII is used by OLES to permit entry to the MIB by authorized employees and contractors as well as members of the public who enroll their children into the GSA Child Care Center.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Security office personnel, system administrators, and security guard staff at the entrances to the MIB will have access to the data in the system for the purpose of verifying the identity of individuals who are authorized to enter the MIB but do not have their identification credentials with them.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Limited information may be shared with DOI bureaus and offices regarding their employees who require access to the MIB, including date and time of entry and exit and location, and video footage only after approval from the Assistant Director of Internal Security.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII is shared with the Federal Protective Service and other Federal agencies for investigation of emergency response situations or the violation, enforcement or implementation of a statute, rule, regulation or license. Information may also be shared with other Federal agencies to allow DOI employees access to that agency's facility or when DOI controls access to facilities occupied by that agency. This sharing of information is authorized and described in the routine uses published in the DOI-46, Physical Security Access Files system of records notice, which may be viewed at: https://www.doi.gov/privacy/sorn.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

PII is shared with state or local agencies for investigation of emergency response situations or the violation, enforcement or implementation of a statute, rule, regulation or license as authorized and described in the routine uses published in the DOI-46, Physical Security Access Files system of records notice, which may be viewed at: https://www.doi.gov/privacy/sorn.

☒ Contractor: *Describe the contractor and how the data will be used.*

PII is shared with DOI contract security guard staff who monitor the MIB entrances, and verify the identities of employees, visitors and any individuals who access the MIB.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals can decline to provide the identifying information required for registration in PACS or entry to the MIB; however, failure to do so can result in denial of entry to the MIB or limited or escorted access to the MIB.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is provided upon request that states the proper authorities for collecting information; the purpose of the information collection; how DOI will share information outside of the Department; and a disclosure statement explaining that visitors are not required to provide their PII, but that failure to do so may result in a denial of access to DOI controlled facilities.

☒ Privacy Notice: *Describe each applicable format.*

A privacy notice is posted on the security desks at the MIB entrances and on the PIV II Card Access Request Form. Notice is also provided through the publication of this privacy impact assessment and the DOI-46 Physical Security Files system of records notice, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records may be retrieved manually by identifiers such as; name, image; organization/office of assignment; date, time or location of entry or exit; ID security card number; or date.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

PACS has limited reporting capabilities. Reports may be generated by the System Manager and System Administrators upon request by DOI officials in response to security breach investigations. Reports produced on individuals will include name and time and location of access. PACS reports are not intended to be used to verify employee time and attendance; however, there may be cases where employee ingress or egress times are requested for administrative or investigative purposes. Video recordings of incidents may be produced for investigative purposes, and may be generated by authorized DOI Security staff for law enforcement entities such as, but not limited to, the U.S. Park Police, U.S. Secret Service, Department of Homeland Security Federal Protective Service, and Office of Inspector General.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

PIV card data is obtained from the USAccess system and it is the responsibility of the sponsoring agency to verify the accuracy of the information collected for USAccess during the onboarding process. Visitor identity is verified by government issued identification, which is presumed to be accurate at the time presented by the individual requesting access to the MIB. Proprietary signature/encryption, along with visible timestamps are incorporated on video that is saved for accuracy.

B. How will data be checked for completeness?

PIV card data is obtained from the USAccess system and it is the responsibility of the sponsoring agency to verify the information is complete during the onboarding process. Visitor data is collected directly from visitors and is presumed to be complete at the time presented by the individual requesting access to the MIB. Captured video events include short clips before and after the incident occurs so that the specific incident is captured in its entirety.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

PIV card data is obtained from the USAccess system and it is the responsibility of the sponsoring agency to verify the information collected for USAccess is current during the onboarding process. PACS will authenticate users through the DOI domain. Timestamps are incorporated in videos and saved for accuracy.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Facilities security and protective service records in this system are retained in accordance with the DOI Department Records Schedule (DRS) 1 - Administrative bucket, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001). The disposition for these records is generally temporary. Records are cut off as instructed in the agency records manual, or at the end of the fiscal year in which the record is created, then destroyed 3 years after cut-off. Retention periods for security violation files relating to investigations referred to administrative or law enforcement organizations may vary depending on the subject matter, legal requirements and Departmental policy.

Some records may be maintained as Long-term Administration Records. The disposition for these records is temporary. Records are cut off as instructed in the agency records manual, or at end of fiscal year in which files are closed, then destroyed 7 years after cut-off.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Records of individuals will be deleted from the system and printed records will be handled in accordance with the records retention period listed above. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to the privacy of individuals due to the volume of sensitive PII contained in the system. There is a risk that individuals may gain unauthorized access to the information in PACS. System security controls are in place to prevent access by unauthorized individuals to sensitive information. PACS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. PACS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties. Access to information is role-based and is only granted on a need-to-know basis, and requires DOI credentials. The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training. All employees must agree to the DOI Rules of Behavior before being allowed to access the DOI network or any information systems. A general warning banner is displayed upon first logging into the DOI network that informs users that misuse of any system may subject employees to penalties.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored has intentionally been limited; only the minimal amount of data needed for identification purposes is maintained and used by the system. Records are maintained in accordance with the DRS that was approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

There is a risk that a prospective visitor's access may be denied based on the submission of inaccurate information. If a visitor is denied access based on submission of PII that pertains to someone else that has a criminal record, that information will have been supplied by the visitors themselves or by their sponsors. Visitors may contact the building security office to discuss the reasons for the denial or accuracy of their information.

There is a risk that individuals providing information do not have adequate notice that their PII will be collected or stored in PACS. This risk is mitigated by the publication of this PIA and the DOI-46 Physical Security Files system of records notice, and the privacy notice posted at the entrances to the MIB.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The use of the data is relevant and necessary to ensure the security of DOI personnel and facilities and physically identify individuals for building access purposes.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

The system does not derive or create previously unavailable data through aggregation from the information collected.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

Security office personnel, system administrators, and security guard staff at the entrances to the MIB will have access to the data in the system for the purpose of verifying the identity of individuals who are authorized to enter the MIB but do not have their identification credentials with them.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is granted to security personnel to perform job duties. User access is password-protected. Each person granted access to the system at guard stations are individually authorized to use the system. Each user will have access limitations. Security staff will be able to add or delete records, search the database for particular items, print reports, and grant or deny access to specific entrance and exit locations. Security guards will have limited access to data and will only be able to access information needed to verify the identity of individuals who enter the MIB.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act contract clauses are included in the contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

PACS is an identity management system and can identify individuals and monitor them entering and leaving the MIB for security purposes. PACS has the capability to monitor and audit users, including who accessed the system; time and date of access; and activities within the system. PACS also utilizes

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

PACS identifies individuals' identity through PIV card and other identification upon entry and exit of the MIB. PACS uses surveillance cameras and CCTV, which capture images and video of individuals entering and leaving the MIB and perimeter area for security purposes. PACS has the capability to audit users, including who accessed the system; time and date of access; and activities within the system.

M. What controls will be used to prevent unauthorized monitoring?

The System Manager and System Administrators will have access to the data in the system. System access is password-protected. Each person granted access to the system must be trained and individually authorized to use the system. All system users are required to follow established internal security protocols.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. Describe

Turnstiles are placed at entry points in the MIB to ensure only authorized individuals enter the MIB. The Visitor Processing Center (VPC) will help security personnel separate visitors from DOI employees and perform screenings in a secured and controlled area.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training

☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The PACS Information System Owner and Information System Security Officer will have the ultimate responsibility of implementing adequate controls and protecting the privacy rights of individuals affected by the use of the system and interface with other systems. The Information System Owner and the PACS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with the Privacy Act and other Federal laws and policies for the data managed and stored within the system, and for making decisions on Privacy Act requests for notification, access, amendments, and complaints in consultation with the DOI Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Assistant Director, Internal Security, Office of Law Enforcement and Security has responsibility for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The PACS Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the DOI Privacy Officer.