

Department of the Interior
Privacy Impact Assessment

July 15, 2013

Name of Project: Physical Access Control System (PACS)

Bureau: Interior Business Center (IBC)

Project's Unique ID: 010-00000704 00-00-01-05-02-00

A. CONTACT INFORMATION:

Who is the Bureau/Office Privacy Act Officer who reviewed this document?
(Name, organization, and contact information).

Teri Barnett
Departmental Privacy Officer
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street NW, Mail Stop 5547 MIB
Washington, DC 20240
202-208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, the system contains information needed to confirm the physical identity of individuals, including full name, date of birth, headshot photo, height and weight.

a. Is this information identifiable to the individual¹?

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Yes, full names, dates of birth and headshot photos are identifiable to an individual. Height and weight data individually or in combination may also be identifiable to an individual.

b. Is the information about individual members of the public?

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

No.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, the information pertains to Federal employees and contractors who require regular access to the Department of the Interior buildings located at 1849 C Street NW, Washington DC (known as the main interior building, or MIB), and 1951 Constitution Avenue NW, Washington DC (known as the South Interior Building, or SIB).

In addition to Department of the Interior employees and contractors who work at the MIB or SIB and require building access, the system will contain information about employees and contractors who work at the General Services Administration (GSA) building at 1800 F Street, Washington DC, and the Office of Personnel Management building at 1900 E Street, Washington, DC.

2) What is the purpose of the system/application?

The purpose of the system is to ensure the safety and security of the MIB and SIB by controlling physical access to both buildings. The system will permit entry to the MIB and SIB by authorized employees and contractors with appropriate identification.

The system will also permit GSA and OPM employees at nearby facilities to access the MIB and SIB as part of an “open campus” initiative designed to share building resources. Reciprocal rights will be granted to MIB and SIB personnel to access GSA and OPM buildings.

3) What legal authority authorizes the purchase or development of this system/application?

5 USC 301; Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995; HSPD-12 OMB M-10-06, Policy for a Common Identification Standard for Federal Employees and Contractors August 27, 2004.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Individuals who require regular, ongoing access to the MIB or SIB, including Departmental employees, contractors, students, interns or volunteers. The system also facilitates building access by (1) individuals authorized to perform or use services provided in Departmental facilities (e.g., Credit Union, Fitness Center, etc.) who have appropriate Federal identification credentials, and (2) employees and contractors who work at nearby GSA and OPM buildings who will be granted access to the MIB and SIB under an “open campus” initiative.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information is from obtained from individuals applying for an ID badge who will be stationed at the MIB or SIB.

Information is also obtained from GSA and OPM as a part of an “open campus” initiative; information provided by GSA and OPM will have been collected from GSA and OPM personnel for ID credentialing purposes.

b. What Federal agencies are providing data for use in the system?

As described above, both GSA and OPM will provide some of the data contained in the system.

c. What Tribal, State and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

Information is collected from individuals applying for an ID badge who will be stationed at the MIB or SIB.

Information is also obtained from GSA and OPM as a part of an “open campus” initiative; information provided by GSA and OPM will have been collected from GSA and OPM personnel for ID credentialing purposes.

3) Accuracy, Timeliness, and Reliability

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

With the exception of information provided by OPM and GSA, all data will be obtained from DOI sources, including DOI employees and contractors. OPM and GSA are responsible for the accuracy of the data they provide; OPM and GSA information will not be independently verified by DOI.

b. How will data be checked for completeness?

Data will be verified by comparing the information held in DOI’s Active Directory system, which provides an updated listing of active DOI employees.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Data will be verified by comparing the information held in DOI’s Active Directory system, which provides an updated listing of active DOI employees. Data is updated when employment status, marital status, bureau assignments, etc, change. Agency and Departmental clearance forms will trigger the necessary changes, along with changes identified in the Active Directory system.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, Privacy Act Notice HSPD-12: Physical Security Files — interior, DOI-46.

D. ATTRIBUTES OF THE DATA:

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

Yes, the use of the data is relevant and necessary to physically identify individuals for building access purposes. 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.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No, the system will not derive or create previously unavailable data through aggregation from the information collected.

3) Will the new data be placed in the individual's record?

Not applicable - the system will not derive or create previously unavailable data through aggregation from the information collected.

4) Can the system make determinations about employees/public that would not be possible without the new data?

Not applicable - the system will not derive or create previously unavailable data through aggregation from the information collected.

5) How will the new data be verified for relevance and accuracy?

Not applicable - the system will not derive or create previously unavailable data through aggregation from the information collected.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The data is not being consolidated.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Processes are not being consolidated.

- 8) How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Records are retrievable by name, organization/office of assignment, agency point of contact, company name, date of entry, time of entry, location of entry, ID security card issue date, ID security card expiration date, and ID security card serial number.

- 9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The system has limited reporting capabilities, and only the System Manager and System Administrators have the ability to generate reports. Reports produced on individuals will include name and time and location of access. Reports are only run upon request by appropriate DOI officials in response to investigations pertaining to security breaches. Reports are not run to verify employee time and attendance.

- 10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

Individuals are required to provide the information in order to obtain identification credentials; employment with the Department is voluntary.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The system will be operated from a single server located in the MIB security office.

- 2) What are the retention periods of data in this system?**

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item No. 17. Unless retained for specific, ongoing security investigations:

(1) Records relating to individuals other than employees are destroyed two years after ID security card expiration date.

- (2) Records relating to date and time of entry and exit of employees are destroyed two years after date of entry and exit.
- (3) All other records relating to employees are destroyed two years after ID security card expiration date.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Computer records of individuals will be deleted from the system in accordance with the records retention period listed above. Printed records will be handled according to the Department of the Interior General Records Schedule 18, dated June 1988 under the section of Security and Protective Services Records.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

The major technology being employed is the use of smart cards, which DOI has previously employed for employee access purposes.

5) How does the use of this technology affect public/employee privacy?

The use of this system will have a minimal affect on the privacy of individuals. There will be a minimal amount of data collected and maintained in the system. All data will be used strictly for the purpose of securing the MIB and SIB and controlling access by individuals. In addition, individuals are fully aware of the system and its usage by virtue of the credentialing process and the routine card swipes required to access the MIB and SIB.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes, the system has a very limited ability to identify, locate and monitor individuals by logging the entry of individuals to the MIB and SIB.

7) What kinds of information are collected as a function of the monitoring of individuals?

The location and time of entry to the MIB and SIB will be recorded.

8) What controls will be used to prevent unauthorized monitoring?

Only the System Manager and System Administrators will have access to the data in the system, and 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..

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Interior Department — Privacy Act Notice, HSPD-12: Physical Security Files — interior, DOI-46.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The system is not being modified, and the Privacy Act system of records notice will not require amendment or revision.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

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

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access granted to security personnel only as necessary to perform job duties. User access is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Each user will have access limitations. Security staff will be able to add/delete records, search the data base for particular items, print reports, and grant/deny access to specific entrance/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 wish to enter the MIB or SIB.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Access granted to individuals 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.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Contractors are not being used for the design and development of the system.

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

As described above, data is shared between DOI, OPM and GSA. However, DOI, GSA and OPM systems do not directly share data; data is shared by the systems through occasional data transfers using encrypted USB drive devices.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The System Administrator and System Manager will have responsibility for ensuring privacy protections.

- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

Yes, as described above, GSA and OPM will engage in limited data sharing with DOI to facilitate an “open campus” between the three agencies.

- 9) How will the data be used by the other agency?**

As described above, GSA and OPM will engage in limited data sharing with DOI to facilitate an “open campus” between the three agencies.

- 10) Who is responsible for assuring proper use of the data?**

The System Manager is ultimately responsible for maintaining the system, including providing oversight for the system and ensuring proper use.