EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Enterprise Physical Access Control System (ePACS)	
Preparer: Jackie Brown, ISSO **James Cunningham, SO**	**Office: Office of Mission Support, Office of Administration**
Date: 7/15/2022	**Phone: 202-564-0313**
Reason for Submittal: New PIA____ Revised PIA_ ___ Annual Review_X___ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

Homeland Security Presidential Directive (HSPD) 12 was issued on August 12, 2004. HSPD-12 calls for a mandatory, Government-wide standard for the issuance of secure and reliable forms of identification to executive branch employees and employees of Federal contractors for access to Federally controlled facilities and networks.

The National Institute for Standards and Technology (NIST) further defined the standards through the issuance of Federal Information Processing Standards (FIPS) Publication 201 including a description of the minimum requirements for a Federal Personal Identification Verification (PIV) system. The PIV card is designed to link a person's identity to an ID credential, which gives a person the ability to physically access federally controlled buildings and logical access to information systems.

In 2005, EPA began issuing PIV credentials to its personnel through the EPA Personnel Access and Security System (EPASS) program. The EPA transitioned the internal EPASS badge program to USAccess, GSA's managed service for the issuance and lifecycle support of HSPD-12 compliant badges.

The transition promotes EPA's strategic goals, which includes the modernization of business practices and leveraging of cost-effective, federally managed services supporting the merging of redundant functions across agencies. The primary benefit is to support secure and efficient issuance and maintenance of Personal Identity Verification (PIV) Credentials to EPA employees and contractors.

The GSA HSPD-12 Managed Service Office (MSO) established the USAccess program as an efficient way for Federal agencies to issue common HSPD-12 approved credentials to their employees and contractors.

A Human Resource Representative, Contracting Officer's Representative (COR), a Grant Officer, or a Project Officer initiates a request for an USAccess badge. This request is submitted to a USAccess Sponsor. It is the USAccess Sponsor that creates your record in USAccess and submits a request to begin the process of obtaining a badge. Once sponsored, Applicants are scheduled to complete the enrollment process which initiates the identify verification and background processes. For more information on the 9-step process to obtain a PIV credential, please visit How to Obtain a Credential.

In 2008, EPA began upgrading its facility PACS to be compatible with the PIV cards and now in the process of consolidating systems into once centralized Enterprise Physical Access Control System (ePACS). Enterprise PACS is comprised of non-traditional IT hardware such as Personal Identify Verification (PIV) card readers, control panels, closed circuit video cameras, building intrusion detection sensors, alarm keypads, emergency door buttons, etc. that are tightly integrated into one PACS system that is centrally managed in a virtual server environment.

The ePACS will use the EPASS smartcard to link the credential to a person's ability to access federally controlled buildings, by using attributes such as the Card Authentication Key Certificate (CAK), Card Holder Unique Identifier (CHUID) and PIV certificates. The ePACS software is a Commercial Off-The-Shelf (COTS) application, name C-Cure 9000 from vendor, Software House. This software configures a device to an event, e.g., an alarm sounds when a door is forced open, a CCV begins recording when motion is detected, building doors automatically lock predicated on a specific door schedule, and a doorbell rings when a visitor presses a button on an intercom pad (with a video camera), and a door unlocks when the EPASS badge is touched to the door card reader. Each building can be custom configured locally (based upon its unique events as described) using the C-Cure 9000 COTS software that is installed centrally and hosted at the National Computer Center (NCC).

Enterprise PACS currently operates in EPA's Regions 3, 4, 6, 7, 8, 9 and 10 locations. For accurate identification and communication purposes, going forward, ePACS name will transition to Enterprise Physical Access Control System (ePACS).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

- **Homeland Security Presidential Directive (HSPD-12)** is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. It requires the development and implementation of a government-wide standard for secure and reliable forms of identification for Federal employees and contractors.

- **OMB 11-11**- Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors.

- **Executive Order 12977.** Established the ISC to develop standards, policies, and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, non-military federal facilities in the United States.

- **Executive Order 13467.** Established to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Federal Government employment, contractor employee fitness, and eligibility for access to classified.

- **OMB Circular A-130,** which references NIST SP 800-116 to ensure continued deployment and use of the identity credentials accessing Federal facilities OMB M-11-11.

- **OMB Memorandum 05-24,** ***Implementation of Homeland Security Presidential (HSPD) 12*** *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 2005. This memorandum provides implementing instructions for HSPD-12 and the Standard (NIST FIPS 201).

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

The System Security Plan (SSP) for the ePACS is current with an ATO expiration date of 12/16/2022.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Data is not stored nor maintained in the cloud

Section 2.0 Characterization of the Information

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

A subset of data, as indicated below, is transferred from the USAccess badge (chip) into ePACS upon enrollment of employees into ePACS for physical access:

Table 1: PIV Card Object

Field Name	Definition
First Name	Personnel's first name
Surname	Personnel's last name
Middle Initial	Personnel's middle initial
Full name	Personnel's first name, last name, and middle initial
Group Name	Region name
Group ID	Region ID number
Logon Name	Employee ID number
SN3	FASCN
Enabled Until	Card Expiration
XdPIV2	GUID
CertSerialNo	Certificate Serial Number
PKCS7	Certificate for PIV or Card Auth
Revocation Date	Date the certificate was revoked
Certpolicy	PIV Auth or Card Auth

2.2 What are the sources of the information and how is the information collected for the system?

The source of the information is collected via the chip on the USAccess badge. The chip includes data from the USAccess credential (Table 1, Section 2.1). Once a user is issued a PIV card (USAccess badge), the PIV card is enrolled into ePACS. The enrolment process occurs when the employee visits a badge office to pick up the PIV card.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, the system does not use information from commercial sources.

2.4 Discuss how accuracy of the data is ensured.

Data is obtained from the USAccess PIV card, and accuracy of the information is dependent upon the PIV Card Objects (as specified in Table 1, Section 2.1). Information obtained from users are adjudicated before a PIV card is issued. Thus, the accuracy is dependent on information provided by the user and the adjudication process.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

If ePACS operators' access and use PII data in an unauthorized manner.

Mitigation:

Only employees with proper credentials are granted access to ePACS (Authentication) as Operators. Operators are further limited to their regions Roles based access is used to restrict operators to the security domain for which they have responsibility. In addition, audit log are generated for each atomic action and are monitored by ePACS system administrators... In addition, role based access security is used for File, Application and Database server authorization after successful authentication.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Only authorized users of ePACS will have system end user access. Operator based user role-based permissions, restrict the information that may be viewed or modified, with data segmented for their specific location. This segmentation by location restrict views to data being used by another location with a physical access control system. System end users are assigned permission that commensurate with their physical security responsibilities. Privileges granted for that purpose must comply with the principles of least privilege, which requires that each user be granted the most restrictive set of privileges needed for the specific task.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

ePACS follow access control procedues documented in CIO 2150-P-01.2.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, there are no other system end user components with assigned roles and responsibilities within the system.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

ePACS is for official business only, and not available to the public or external parties. Only authorized EPA employees who perform a physical security role and requires system end user access will be provisioned an account to ePACS. EPA Interim Policy Notice 17-01 Security clauses are added to ePACS contracts for information technology support services, for contractor personnel supporting EPA badge offices, and for security guards.

Review EPA Interim Policy Notice and ensure clauses are in the ePACS contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

NARA regulations require that electronic records be retrievable and usable for as long as needed to conduct Agency business and meet NARA approved disposition. ePACS is covered by Schedule 1012, item c. Records are retained and disposed of in accordance with EPA's records schedule 1008 item A. Records are kept until anemployee or contractor no long need access to EPA buildings and facilities andin accordance with NARA record schedules.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Records are retained for as long as the employee is employed at EPA, or physical access is revoked. Records kept indefinitely can be altered

Mitigation:

Only IT System Administrators and ePACS Operators, system end users have access to records. ePACS retains an audit trail of all changes to an employee record.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

ePACS is for official business only. ePACS does not support external sharing.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

ePACS is for official business only. ePACS does not support external sharing.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

There is no information sharing within any other Agency or organization as it pertains to physical access.

4.4 Does the agreement place limitations on re-dissemination?

ePACS is for official business only. ePACS does not support external sharing.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:
None. ePACS is for official business only. ePACS does not support external sharing.

Mitigation:
None. ePACS is for official business only. ePACS does not support external sharing.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

In accordance with OMB M-11-11, physical access to controlled EPA spaces must accept and electronically verify PIV credentials. To be issued a PIV card, the employee must proceed through a personnel enrollment process that consists of data elements necessary to verify the identity of the individual, including a background investigation and collection of PII.

ePACS consumes data collected by EPA secuirty Management Division, Personnel Secuirty System version 2.Once in ePACS, only authorized personnel have access based on assigned roles. Audit monitoring is in place to ensure data isused as intended.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The EPA’s Information Security Program provides annual security and privacy awareness training to all employees (Information Security and Privacy Awareness Training). Only authorized EPACS Operator (system end users) have access to the system. All system end users must adhere to federal and Agency directives related to privacy policies and procedures.

5.3 <u>Privacy Impact Analysis</u>: Related to Auditing and Accountability

<u>Privacy Risk</u>:

Low risk of improper audit.

<u>Mitigation</u>:

HSPD-12 instructs agencies to follow NIST FIPS 201 guidance for PIV Card issuance. NIST FIPS 201 specifies the minimum, physical access record, data elements to establish a physical access record. The system contains PII. Each ePACS physical access record retains an audit trail for accountability.

Section 6.0 Uses of the Information

The following questions require a clear description of the system’s use of information.

6.1 Describe how and why the system uses the information.

How: A subset of the information (as described in Table 1, Section 2.1) is loaded from the chip on the PIV card when enrolled for physical access. Once loaded, then physical access to specific building entrances/exits is assigned. Why: HSPD-12 explicitly requires the use of PIV credentials “in gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems.”

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes X No. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Information can be retrieved by card holder’s first and last name, and other personal identifiers. Information retrieved using personal identifiers include name, card ID number, Employee ID, FASC-N, card expiration, GUID, certificate serial number, certificate for PIV or Card Authentication, certificate revoke date and door access schedule.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

GSA/GOVT-7, HSPD-12 USAccess. ePACS operates under SORN EPA-62R EPASS.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Unauthorized use of information by none authorized personnel. Insider threat.

Mitigation:

Only authorize users who have been duly adjudicated are allowed access to EPACS as regional or global operators. Actions performed by users and Operators of EPACS are audited. In addition, Splunk is used to monitor system activities including successful/unsuccessful login attempts. Audit log reports are customizable and are run on a regular basis.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Information is added to ePACS via the PIV card as outlined in the overview. A person must fulfil all requirements, including consent to uses of information, before a credential is issued, i.e. PIV card. For more information on the 9-step process to obtain a PIV credential, please visit How to Obtain a Credential. Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

When a user registers for a PIV card and is issued a PIV card (USAccess badge), the employee is provided instructions that information will be collected and how to obtain a record of the information. If an employee does not want their information collected in ePACS(for the sole purposes of physical security), a Common Access Card (CAC) can be provided, or a “paper” badge (for those locations without ability to provide a CAC). A CAC looks just like a PIV card, but without the data as provided in Table 1, Section 2.1 on chip, nor does it include any personal identifiers on the outside of the CAC. However, all permanent EPA employees are required to obtain an PIV card. Employees with CAC will be required to go through XRAY at secure entrances and will not have be able to login into their EPA issued laptops (called LACS). Need to verify if the CAC card reference is correct.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Low risk of inadequate notice

Mitigation:

The notice of Information collected is sent prior to issuing a PIV card.

Section 8.0 Redress

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. EPA's Privacy Act regulation, 40 CFR Part 16, Section 16.3, sets forth the procedure that individuals must follow to access, correct or amend personal records. (See http://www.epa.gov/fedrgstr/EPAGENERAL/2006/January/Day-04/g45.htm.)

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Individuals not having the ability to access and/or modify their own ePACS records directly.

Mitigation:

Should the EPA employee or contractor wish to make corrections to their own ePACS record, they are to contact the National Privacy Program office to remedy their complaint and seek resolution or contact their local Security Office. Redress is accomplished by corrections to the PIV card, which is then used to update an employee ePACS record.