Privacy Impact Assessment
Enterprise Physical Access Control

- Version: 1.7
- Date: June 4, 2020

Prepared for: Departmental Administration-Office of Safety, Security, and Protection, Facility Protection Division

United States Department of Agriculture

Privacy Impact Assessment for the Enterprise Physical Access Control (ePACS)

Contact Point
Joe Reale
DA-OSSP-FPD
System Owner
United States Department of Agriculture
202-720-0824

Reviewing Official
Lisa McFerson
DA ITO ISSPM
United States Department of Agriculture
202-720-8599

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

Enterprise Physical Access Control System (ePACS) supports the United States Department of Agriculture (USDA) physical access compliance efforts of the USDA Homeland Security Presidential Directive 12 (HSPD-12). Following the completion of the PTA it was determined that the system contain PII and requires a PIA review.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

ePACS is operated by the ePACS Program Management Office (PMO) which is managed in the Office of Safety, Security, and Protection Facility Protection Division (FPD) and is hosted at USDA's Enterprise Data Center/Midrange System under an agreement to provide Platform as a Service (PaaS) capabilities.

This document is the Privacy Impact Assessment (PIA) for USDA's ePACS which incorporates compliance requirements from HSPD-12. HSPD-12 establishes a government-wide process to validate the identities of employees and contractors; establishes a baseline background investigation process for all government and contractor personnel; and institutes a government wide identification credential that is secure and reliable. ePACS deploys the HSPD-12 requirements for credentials and credential utilization, Federal Information Processing Standard 201-1 (FIPS 201-1), and the Office of Management and Budget (OMB) Memorandum M-11-11.

ePACS utilizes the Lenel OnGuard, commercial off the shelf software/client server application. ePACS provides the centralized infrastructure for utilization of the USDA standard identification card (LincPass) for physical access to federally controlled facilities. ePACS include the following functions:

(a) Issuance based on sound criteria for verifying an individual identity.
(b) Strong resistance to identity fraud, tampering, counterfeiting, and terrorist exploitation.
(c) Rapid electronic authentication.
(d) Issuance only by providers whose reliability has been established by an official accreditation process.

ePACS operate under the following SORN: USDA/OCIO-2: System name: eAuthentication Services (March 7, 2017, 82 FR 8503) and GSA/GOVT-7: System name: Personal Identity Verification Identity (Oct 23, 2015, 80 FR 64416).

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

ePACS generally handles Security Management Information including:

- Physical access card status
- Physical access card category
- Physical access card expiration date
- Physical access card holder emergency response responsibilities

ePACS also stores Personal Identity and Logistics information including:

- First Name
- Last Name
- Middle Name
- Date of Birth
- Photograph
- Federal Employee Agency
- Federal Employee Department
- Federal Employee Office Address
- Federal Employee Office Telephone Number
- Federal Employee Agency Smart Credential Number (FASCN)

In addition to the data provided by the ICAM identity management system, the ePACS may capture and store the following, height, hair color, eye color, signature image, biometric fingerprint biometric hand geometry and biometric iris.

1.2 What are the sources of the information in the system?

USDA's ICAM Shared Services identity management system (EEMS/EIMS) provides the

authoritative data elements to the ePACS information system. ICAM Shared Services identity management system information is provided via an encrypted 128-bit connection to a staging table within ePACS. The staging table then disseminates the current identity data to the information systems as applicable. Also, Non-Authoritative data is manually collected at the time of card issuance and stored into ePACS.

1.3 Why is the information being collected, used, disseminated, or maintained?

ePACS is focused on supporting the USDA efforts to comply with all policies and guidance relevant to HSPD-12 which protects USDA facilities. The information is collected in the application is disseminated through a predetermined reporting structure. The information is secured and maintained within a master database and two regional databases.

1.4 How is the information collected?

The authoritative data elements provided to the ePACS are provided by USDA's ICAM Shared Services identity management system. This identity data is provided from a series of USDA Human Resources databases which are consolidated into ICAM Shared services. The non-authoritative data is manually collected at the time of card issuance.

1.5 How will the information be checked for accuracy?

Automated integrity checks and business rules are performed on the data before it is disseminated from authoritative source systems to the ICAM Shared Services and then to ePACS. Within ePACS, a staging table is used to conduct a comparison of new data elements and current data elements to conduct consistency checks and update the ePACS Master Security Database (MSD).

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Formal Interconnection Security Agreements (ISA) have been established between the OCIO and OSSP regarding the interface between ICAM Share Services identity management system and ePACS.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

ePACS has minimal privacy risks associated with the collection and sharing of data. The primary data elements identified as Personally Identifiable Information (PII) within ePACS are first and last name, photographs, fingerprints, and date of birth. This information is stored in in an encrypted binary format stored on an encrypted SAN, which is monitored 24x7 by USDA's Enterprise Data Center. ePACS monitors and audits on a daily, monthly, and quarterly schedule.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The PII information is used to create or validate an ID Credential for the use of physical access to USDA facilities.

2.2 What types of tools are used to analyze data and what type of data may be produced?

ePACS only correlates limited information related to cardholders and is stored within an encrypted SQL database. Products of this data include site badge credentials and database archival reports.

2.3 If the system uses commercial or publicly available data, please explain why and how it is used.

ePACS does not use any commercial or publicly available data.

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

ePACS follows all required security controls deemed applicable by NIST-800-53 Rev. 4.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Information within the ePACS will be retained for 3 calendar years.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

ePACS archival data is rarely requested by authorized employees at USDA agencies. The risk in disseminating this information is minimized by requirements mandating that all SAN access is limited to a restricted pool of users with PIV cards (LincPass). ePACS uses encrypted SAN nodes hosted at Enterprise Data Center. Enterprise Data Center's VM server environment and SAN is monitored 24X7 under gold level support.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information may be shared with senior leadership across USDA through a series of Tableau dashboards and reports for the purpose of promoting data-driven decisions. The information shared will span data from different various administrative domains including IT, Finance, HR, Property, Operations, Homeland Security, and Property & Fleet. USAccess Shared Services Program, General Services Administration (GSA) provides ICAM Shared Services identity management system authoritative data. USDA's Human Resources systems (EmpowHR, Personnel Payroll, and Person Model), which provides regular data transfers to ICAM Shared Services identity management system and then ICAM sends data to ePACS. This information is classified as Security Management and Personal Identity and Logistics Information.

4.2 How is the information transmitted or disclosed?

ePACS securely transmits data. The disclosure of information is prohibited based on the "Need-to-Know" principle as those with authorized interest will have been granted access. To collect data from the USDA authorized information systems please note the following procedures are implemented: information provided through the ICAM Share Services interface is processed through a Staging Database table and the Master Security Database (MSD), which prepares it for placement in the Master PACS Database (MPD) and final distribution to secure agency access control segments within three PACS Regional Databases (PRD). Also, the information will be transmitted to the USDA Data Lake via secure file transfer methods such as SFTP, API, and Web Service. Once in the USDA Data Lake, data will be shared via a series of Tableau dashboards

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Risk when sharing within USDA is considered low-moderate. When data sharing within the network, encryption protocols ensure PII is not inadvertently shared in an unencrypted format. Data is encrypted in motion and at rest. In addition, access to data is limited to only those persons with a need-to-know using internal, granular governance process. Dissemination of information is governed by internal policy. Internal information sharing is limited to the VM

server boundaries within the information systems. The data is encrypted into unique data strings to further mitigate any risks to PII.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information within ePACS is not shared with external organizations; under current support agreements audits of the data for consistency may be conducted on occasions where corrective action may require access to the data. The support personnel will be required to have the appropriate Background Investigation (BI) and credentials prior to any audit activities.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or is the system allowed to share the personally identifiable information outside of USDA.

PII is not permitted to be shared outside of the USDA. Technical support contracts may require database components be corrected at the direction of USDA OSSP ePACS PMO personnel.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is not permitted to be shared outside the USDA OSSP.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information is not permitted to be shared outside the Department. Each user is required to agree to the Rules of Behavior which deny the sharing of information. However, if external access is required and approved, users would have to comply with the USDA Two Factor Authentication. This includes having applicable eAuthentication Service Credentials, PIV card (LincPass) and access to the VPN.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

ePACS operate under the following SORNs:

USDA/OCIO-2: System name: eAuthentication Services (March 7, 2017, 82 FR 8503). https://www.federalregister.gov/documents/2017/01/26/2017-01767/privacy-act-of-1974-revised-system-of-records#page-8504 and

GSA/GOVT-7: System name: Personal Identity Verification Identity (Oct 23, 2015, 80 FR 64416). https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacy-act-of-1974-notice-of-an-updated-system-of-records

6.2 Was notice provided to the individual prior to collection of information?

No. All PII information is collected by USDA Human Resources Department at time of initial employment with the USDA.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

No.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. PII information is collected as a basis for employment with the USDA.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals are notified about the processing of their information during the registration process for federal employment or acceptance as a federal contractor. Prior to access being granted to ePACS, system users will be required to acknowledge and agree to the Rules of Behavior of each application within the system. These measures have been implemented to prevent individuals from being unaware of the collection and processing of information. Failure to agree to these measures will explicitly deny the individual access to USDA facilities and its information systems. Credential holders are made aware of the use of their PII prior

to being sponsored for credentials that are acceptable for use in ePACS.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

There is no mechanism within ePACS for individuals to access PII information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

ICAM Shared Services provides the authoritative data elements to ePACS. Information errors that are not generated by malfunctioning software or hardware must be addressed with USDA HR representing the individual filing the complaint.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are not notified of the procedures for correcting information as there is no mechanism within the ePACS. Information errors that are not generated by malfunctioning software or hardware must be addressed with USDA HR representing the individual filing the complaint.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The individual has the ability to contact USDA HR to address any data correction issues.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There is no privacy risk associated with the redress described in sections 7.3 and 7.4.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Each application within ePACS is role based and privileges are based on the "Need-to-Know" principle. Registration and Approval of access to applications within ePACS are documented in the ePACS.

ePACS has three tiers of access that must be satisfied in order to receive access to the system. The first tier is meeting the two factor authentication guidelines of USDA. This includes a background investigation being processed to receive a credential and having received system access from the OCIO. The second tier is submitting a request for access and having a designated authority sponsor the individual. The final tier is being approved by the Change Control Board (CCB) and being authorized by the Chief, OSSP-FPD.

8.2 Will Department contractors have access to the system?

Yes. Access to the ePACS will be granted for both USDA employees and select non-employees with appropriate background checks and security clearances in place.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Prior to be granted access to the ePACS all individuals must acknowledge and agree to the terms of a Rules of Behavior document. Following this acknowledgement and based on the system access granted, training will be provided on the application of the tools, as well as the protection of the information. In addition, all individuals supporting the mission of USDA with access to its computing systems must annually complete the Information Security refresher provided by the OCIO.

8.4 Has Assessment and Authorization been completed for the system or systems supporting the program?

Yes. ePACS is currently in operation and maintains an Authority to Operate (ATO) which expired in June 2021. The system is currently in continuous monitoring.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

ePACS has been categorized as a moderate system per FIPS 199 Security Categorization. To protect the data within the ePACS, the Recommended Security Controls for Federal Information Systems and Organizations developed by NIST will be applied. These controls are defined in the Special Publication 800- 53 Revision 4. Within NIST SP 800-53 Rev. 4 are 18 families of controls that include, but are not limited to, Access, Auditing, Identification, Authentication and Media Protection. Compliance with these controls is maintained as Hybrid effort supported by ePACS PMO managed by OSSP and the host site, USDA's Enterprise Data Center PaaS environment. ePACS PMO will be responsible for ensuring compliance from the application and database perspective, while the Enterprise Data Center, as the host PaaS, will provide oversight of the Operating System, Hardware, Network and Physical Access to the Enterprise Data Center where the ePACS virtual environment is located. Additional details regarding the compliance with the controls designed to protect data within the ePACS is documented in the System Security Plan (SSP).

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the

information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

There are minimal security risks associated with the collection and sharing of information within ePACS. ICAM Shared Services data is transferred via encrypted 128 bit data VPN connection in binary format. This mitigates the capture and reconstitution of any PII in the system.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The ePACS is a Major Application operating under a Moderate security categorization per FIPS 199.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

No, ePACS does employ technology which may raise privacy concerns. All privacy concerns are mitigated by three factors, which are all required by USDA guidelines per NIST Recommendations. The first factor is that individuals must meet the requirements of the USDA two factor authentication process. This includes having a LincPass. Secondly, all individuals who access ePACS data must request access via a USDA Designated Authority. Access is granted following approval by the CCB or directly by the Chief, OSSP-FPD. Thirdly, following the approval of credentials, all individuals who obtain access to ePACS must acknowledge and agree to the terms of the Rules of Behavior.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes, however no third-party websites or applications are utilized.

10.2 What is the specific purpose of the agency's use of 3rd party websites

and/or applications?

No third-party websites or applications are utilized by the system.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

No third-party websites or applications are utilized by the system.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

No third-party websites or applications are utilized by the system.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

No third-party websites or applications are utilized by the system.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

No third-party websites or applications are utilized by the system.

If so, is it done automatically?

If so, is it done on a recurring basis?

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

No third-party websites or applications are utilized by the system.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

No third-party websites or applications are utilized by the system.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No third-party websites or applications are utilized by the system.

10.10 Does the system use web measurement and customization technology?

The system does not use any web measurement or customization technology.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

The system does not use any web measurement or customization technology.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

No third-party websites or applications are utilized by the system

Responsible Officials

JOSEPH REALE Digitally signed by JOSEPH REALE
Date: 2020.06.08 09:16:36 -04'00'

Joe Reale
DA OSSP, System Owner
United States Department of Agriculture

Date

Approval Signature

LISA MCFERSON Digitally signed by LISA MCFERSON
Date: 2020.06.09 11:42:52 -04'00'

Lisa McFerson
DA ITO, ISSPM
United States Department of Agriculture

Date