GSA Enterprise Physical Access Control System (E-PACS)

Privacy Impact Assessment

07/12/2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Table of contents

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about Enterprise Physical Access Control System (E-PACS). GSA's Office of Mission Assurance collects personally identifiable information ("PII") in order to operate and maintain E-PACS. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

System, Application or Project

GSA Enterprise Physical Access Control System (E-PACS)

System, application or project includes information about

Authorized federal employees or federal contractors, building occupants, interns, and volunteers who are seeking physical access to secured GSA-controlled facilities.

System, application or project includes

- Full Name
- Work Email Address
- Work Phone Number
- Organizational Affiliation
- Facial Photograph
- Badge Expiration Date
- Card State (status)

- User Principal Name (UPN)
- Federal Agency Smart Card Number (FASC-N)
- Cardholder Unique Identifier (CHUID)
- Public Key Infrastructure (PKI) Certificate - X509
- Card Authentication Key (CAK)
- Globally Unique Identifier (GUID)
- Access Authorizations specifying the facilities and area that cardholder are permitted to enter

Overview

The GSA Office of Mission Assurance Physical Security Division owns and manages the E-PACS. The application accepts, stores, and updates cardholder and FIPS-201 credential data from GSA and external sources. It stores cardholder identification data such as names, organizational affiliations and photographs; data extracted from the FIPS-201 credentials that are issued to the cardholders; and access authorizations specifying the facilities and areas that cardholders are permitted to enter, as well as the time periods during which such entry is authorized. Cardholder present their FIPS-201credentials (PIV cards) to GSA E-PACS-managed card readers and, based on the data extracted from these credentials and the associated access authorizations, the GSA E-PACS grants or denies access using electronic locking hardware and access control devices mounted at entry points. All access decisions and transactions are recorded and stored in the application.

During the cardholder registration process, a GSA building manager or contracted support staff enrolled the PIV-Credential holder. Upon enrollment, an individual will unlock his or her PIV Credential by inputting his or her truncated PIN. From there, the registration requires a full name, email address, and contact phone number in addition to the public X.509 certificates and the embedded JPEG image of the cardholder, which is stored in the E-PACS database. Only public elements from the PIV Credential are stored in the application.

The enrollment into the E-PACS utilizes external key-pads so the GSA employee or contractor registering the individual cannot see the PIN when entered to unlock the PIV Credential. As the PIN is entered, the application truncates the entry so it's not visible to the registrar. The information is stored and maintained by GSA and is not shared externally. Five (5) GSA security personnel administer the GSA E-PACS on a continual basis to manage/monitor real-time security events at facility entrances and/or GSA security operations control centers.

The E-PACS system owner determines what access can be granted to data/information provided by the E-PACS system through information sharing. Currently there are 3 systems where data is shared. The E-PACS system sends the user FASC-N and timestamp to the GSA BookIt Hoteling Solution in some locations via a one-way transmission of historic badge swipe information for turnstile entrance readers. The E-PACS system sends alarm information to the GSA Building Automation Systems (BAS) servers where applicable via a one-way connection via https. The E-PACS system sends alarm data to the TechOps hosted PSIM server via a one-way connection over https. The E-PACS system owner determines what access can be granted to data/information provided by the E-PACS system through information sharing. No additional guidance is provided in making these determinations.

Potential privacy risks include the inadvertent or unauthorized access to or disclosure of government employee or contractor data. To reduce risks, E-PACS collects and maintains the minimum amount of personal information that is necessary to verify and grant physical access to GSA-controlled facilities. In addition, once an individual is no longer employed with an agency, then the card is disabled through the agency's human resources system, the card will be deactivated and not permit access to GSA-controlled facilities. Access rights are continually updated when employees no longer require elevated access to particular facilities. Access to the PACS database is also limited to authorized system administrators with the level of access limited to the minimum amount necessary to perform that user's job responsibilities.

There is also a risk associated with the accuracy of data included in the PACS. Although most PII is provided directly by the individuals themselves, it is possible that data could be inaccurately entered or mistakenly associated with the wrong individual. To reduce the risk of data being inaccurately entered or incorrectly associated, electronic data collection tools are used to the greatest extent possible and authorized GSA Property Management team members are trained to enroll and gather the appropriate information, and are reminded of the importance of collecting accurate information.

The E-PACS utilizes a registration engine, access control systems, and intrusion detection systems. The HID pivCLASS registration engine enrolls the individuals into

the E-PACS, which requires the individual's full name, email address, and contact phone number. Additionally, it imports the X.509 certificates and JPEG image from the PIV Credential. Once the information is imported into the E-PACS, the information is stored in the GSA E-PACS and is not shared externally. When the users gain access to a GSA-controlled facility with their PIV Credentials, the readers are used to verify the data from the PIV cards, ensuring the credential is valid by verifying the Card Authentication Key (CAK) each time the credential is used. If a credential is valid, the user is granted access to the facility, and if it is found to have a revoked certificate, the user's card is suspended in the E-PACS and the user is denied access into the GSA-controlled facilities.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

E-PACS collects the information required for and related to physical access to GSA-managed facilities and restricted areas within facilities in all regions across the United States.

1.2 What legal authority and/or agreements allow GSA to collect the information?

- 5 U.S.C. Section 301 "Government Organization and Employees: Departmental Regulations"
- 40 U.S.C. Section 582 "Management of buildings by Administrator of General Services"
- 40 U.S.C. Section 585 "Lease Agreements"
- 40 U.S.C. Section 3101 "Public buildings under control of Administrator of General Services"
- 40 U.S.C. Section 11315 "Agency Chief Information Officer"
- 5 U.S.C. Section 552a(b) Privacy Act of 1974, "Government Organization and Employees: Records maintained on individuals."
- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors."
- Federal Information Processing Standard 201-2 (FIPS 201-2): Personal Identity Verification (PIV) of Federal Employees and Contractors

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

The information is searchable in the E-PACS database by name, phone number, email address, or Federal Agency Smart Card Number (FASC-N). The following SORN applies: GSA-OMA-1 E-PACS SORN (79 FR 75810, January 20, 2015)

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

This system is not an information collection request and therefore not covered by the Paperwork Reduction Act (PRA).

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

GSA retains records of PII collected in accordance with General Records Schedule (GRS) 5.6 and 4.2 as approved by the National Archives and Records Administration (NARA) for Security Records. Specific details are provided below:

GRS 05.6/020
(DAA-GRS-2017-0006-0002)

Record Title:
Key and Card Access Accountability Records - Areas Requiring Highest Level Security Awareness

Description:
"Records accounting for keys and electronic access cards. Areas requiring highest level security awareness. Includes areas designated by the Interagency Security Committee as Facility Security Level V."

Retention:
Temporary. Destroy 3 years after return of key, but longer retention is authorized if required for business use.

GRS 05.6/130
(DAA-GRS-2017-0006-0018)

Record Title:
Local Facility Identification and Card Access Records

Description:
"Temporary employee, contractor, and occasional visitor facility and network identification access card and identity management system records. Identification verification credentials issued by facility or building managers to provide local verification credentials and cards issued by facility or building managers to provide local identification and access. Includes:

• temporary identification cards issued to temporary employees, contractors, and occasional visitors who do not meet the FIPS 201 Standard requirements for PIV issuance

• supplemental cards issued to access elevators

• personnel identification records stored in an identity management system for temporary card issuance

• parking permits"

Retention:
Temporary. Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

GRS 04.2/140
(DAA-GRS-2013-0007-0013)

Record Title:
Personally identifiable information extract logs

Description:
"Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date."

Retention:

Temporary. Destroy when business use ceases.

GRS 04.2/130
(DAA-GRS-2013-0007-0012)

Record Title:
Personally identifiable information extracts.

Description
System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information.

Legal citation: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify.""

Retention:
Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

Privacy Risk: There is a risk associated with the accuracy of data included in the E-PACS. Although most of the PII data is generated by the individual, it is possible that data associated with individuals with the same name or similar names could be inaccurately entered.

There is also a privacy risk associated with the handling of PII that occur when data is extracted from the system and the individual using the data improperly distributes or stores the data. Additionally, there is a risk if an authorized individual misuses the system or conducts unauthorized activities.

Mitigation: To address potential occurrences of data being inaccurately entered, information is reviewed by the E-PACS administrators when an Elevated Access Request form is received. Information entered is compared to the information on the form. Additionally, in regards to handling of PII, access to information is granted on a "need-to-know" basis, access to the E-PACS requires a GSA domain account and a network connection. E-PACS user accounts are individually approved by the owner(s) of the system. All administrators and enrollers receive IT Security Awareness Training and have been vetted with a background investigation that allows network access. Access to the E-PACS is also role-based and all activities are logged.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Individuals are notified through the posted Privacy Act Notice at the bottom of the Access Request Form when they submit the form to the facility/building management team for access to federally-controlled space. It's also available in the GSA-OMA-1 EPACS SORN (79 FR 75810).

In compliance with the Privacy Act of 1974, 5 U.S.C. § 552a et. Seq., the following information is provided: Solicitation of the information is authorized by the Federal Property and Administrative Services Act of 1949, 40 U.S.C. § 47 et. Seq., as amended, and 5 U.S.C. § 2101a et. seq.; E.O. 9397 (1943). Disclosure of information is voluntary. This form will be used as a means to prepare and issue a credential or pass. Information will be transferred to appropriate Federal, State, local or foreign agencies when relevant to civil, criminal, or regulatory investigations or prosecutions; or pursuant to a request by GSA or any other agency in connection with hiring or retention of an employee, the issuance of a security clearance, the investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit. If some or any part of the requested information is not provided by the individual, the effect will be that the employee will not be issued a credential and will not be allowed to enter a GSA-controlled building after normal working hours or when the building is under security.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

E-PACS does not foresee any privacy risks pertaining to openness and transparency due to the notice provided on the Access Request form.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

Authorized federal employees or federal contractors, building occupants, interns, and volunteers who are seeking physical access to secured GSA-controlled facilities.

3.2 What PII will the system, application or project include?

Currently the system collects a full name, email and a contact phone number in addition to the public x509 certificates and the JPEG from the PIV is stored in the system. Only public elements from the PIV are stored in the system. The information is collected from GSA employees, Contractors, tenants, interns, and anyone with a HSPD-12 PIV compliant card meeting the requirements of FIPS-201 that require regular access to GSA facilities. The information is stored and maintained by GSA and is not shared externally.

When an individual enrolls, the PACS Service software extracts the data from the PIV Credential, it checks the certificate path and the revocation status. It adds the cardholder and credential information to the E-PACS. The PACS Service checks stored X.509 certificate status via the Federal Bridge. It then updates the E-PACS with new records from GSA Authoritative sources and status updates from the Federal Bridge or GSA sources. The E-PACS is the central data repository for cardholders, credential, and access privilege records. The revocation status that is received is used to determine the validity of the user and suspend the credential if necessary.

E-PACS utilizes the "least privilege" method, limiting administrative access and further limiting access to only the data needed for a person to perform his or her job within the system.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

The E-PACS uses PII (x509 certificates) in order to authenticate the identity of federal employees, contractors, or individuals who require or attempt electronic access into a GSA-controlled facility. When the user gains access to a GSA-controlled facility with a PIV Credential, the readers are used to verify the data from the PIV Credential by ensuring the credential is valid by verifying the Card Authentication Key (CAK) each time the credential is scanned for access. E-PACS collects and stores the "Revoked Certificate List," which is used to verify that an individual PIV is valid.

The PII (Name, work email and work phone) is also used by the system administrators to verify the identity of an individual when assigning physical access and in the event of an access related error or issue, to contact the individual. The JPEG image may be used to

identify a user as well as serve as a verification tool for guards to ensure the user gaining access is the true cardholder. The information is also used to validate the users' credentials and verify the revocation status. A collection of non-PII will not suffice as there is a need to uniquely identify each individual who has physical access to federally-controlled space.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

The application produces reports that document what activity took place, when, where, and by whom. The reports are created based on parameters that the system administrators enter. Aside from date and time-stamped user activity, the system can generate reports of access groups and members, which is gathered from the existing database of users and access rights.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

A limited number of administrators have access to the information. Limited administrators have the permissions to generate the reports. Reports are only generated and provided under the following approved reasons.

- Legal proceedings, where pertinent, to which GSA is a party before a court or administrative body.
- To a Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or carrying out a statue, rule, regulation, or order when GSA becomes aware of a violation or potential violation of civil or criminal law or regulation.
- To duly authorized officials engaged in investigating or settling a grievance, complaint, or appeal filed by an individual who is the subject of the record.
- To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), the Government Accountability Office (GAO), or other Federal agency when the information is required for program evaluation purposes.
- To another Federal agency in connection with the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation; clarifying a job; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision.

- To a Member of Congress or his or her staff on behalf of and at the request of the individual who is the subject of the record.
- To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant.
- To the National Archives and Records Administration (NARA) for records management purposes.
- To appropriate agencies, entities, and persons when (1) The Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.
- To the workspace and room scheduling system. When an individual swipes their card the FASC-N information is transmitted to automatically check them into previously reserved workspace. This is done as a convenience so the individual won't lose a seat assignment or conference room.

Measures are made to ensure administrative user accounts are disabled as soon as the user no longer requires the access. Information requests are verified and Legal Counsel is involved for questionable requests.

3.6 Will the system monitor the public, GSA employees or contractors?

The EPACS may be used to identify the last known devices used by an authorized individual who is enrolled in the system for physical access; however, access logs are not actively monitored. They are only created upon an approved request or in the assistance effort to troubleshoot access issues into a facility. As most facilities are not controlled with a read-in/read-out function, tracking an individual in real time is not possible.

3.7 What kinds of report(s) can be produced on individuals?

The E-PACS has the capability of producing transactional reports documenting activities on the E-PACS. (date/time-stamped reports with reader usage by individuals; audit

reports of whom has access to particular groups). Those reports are only accessible by few administrators and are only disseminated if authorized.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

For data collection reports, reports are de-identified by removing the names associated with the date/time-stamped entries. Recipients of the reports only see the device and date/time-stamp of the transaction type. The Office of Administrative Services typically requests this type of report.

Reports containing date/time-stamped user activity are only created for approved investigation-type requests. These reports are provided directly to the investigative authority performing the approved investigation.

Access group reports provide a list of users who have access to a particular restricted elevated access group. These reports are sent to the group's "owner," or office's program manager. The purpose of this audit report is to ensure only specific users have the appropriate access to particular space.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

All data collected is pertinent to ensure appropriate access is added to the proper individuals. The information is used to verify the identity of an individual and in the event of an access related error or issue, to contact the individual. A collection of non-PII will not suffice as there is a need to uniquely identify each individual who has physical access to federally-controlled space. If a person refuses to provide the requested information, it could delay the user gaining physical access to a controlled-facility.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

All information collected for the E-PACS is limited to necessary information to operate E-PACS. All data collected is pertinent to ensure appropriate access is added to the proper individuals. The information is used to verify the identity of an individual and in the event of an access related error or issue, to contact the individual. A collection of non-PII will not suffice as there is a need to uniquely identify each individual who has physical access to federally-controlled space. If a person refuses to provide the requested information, it could delay the user gaining physical access to a controlled-facility.

The information collected is only accessible to a limited number of authorized system administrators with the level of access limited to the minimum amount necessary to perform that user's job responsibilities.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

The information collected at the time of enrollment is not shared externally with the exception of investigative purposes with law enforcement agencies. It is not shared for time or record-keeping for managerial purposes. Information may also be shared for auditing purposes, which may include providing an agency with an access list of who has access to a particular access group. The application produces reports that document what activity took place, when, where, and by whom. The reports are created based on parameters that the system administrators enter. Aside from date and time-stamped user activity, the system can generate reports of access groups and members, which is gathered from the existing database of users and access rights.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

The system collects a full name, the public x509 certificates, and the JPEG directly from the PIV Credential upon enrollment into the system. Only public elements from the PIV are stored in the system. The additional information collected from the individual upon enrollment includes the middle name, if not directly imported from the credential, an email address, and a phone number. This information is necessary in order to provide the individuals with the appropriate electronic physical access to a facility.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

The E-PACS system owner determines what access can be granted to data/information provided by the E-PACS system through information sharing. Currently there are 3 systems where data is shared. The E-PACS system sends the user FASC-N and timestamp to the GSA BookIt Hoteling Solution in some locations via a one-way transmission of historic badge swipe information for turnstile entrance readers. The E-PACS system sends alarm information to the GSA Building Automation Systems (BAS) servers where applicable via a one-way connection via https. The E-PACS system sends alarm data to the TechOps hosted PSIM server via a one-way connection over https. The E-PACS system owner determines what access can be granted to data/information provided by the E-PACS system through information sharing. No additional guidance is provided in making these determinations.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Potential privacy risks include the inadvertent or unauthorized access to or disclosure of government employee or contractor data. To reduce risks, E-PACS collects and maintains the minimum amount of personal information that is necessary to verify and grant physical access to GSA-controlled facilities. In addition, once an individual is no longer employed with an agency, then the card is disabled through the agency's human resources system, the card will be deactivated and not permit access to GSA-controlled facilities. Access rights are continually updated when employees no longer require elevated access to particular facilities. Access to the PACS database is also limited to authorized system administrators with the level of access limited to the minimum amount necessary to perform that user's job responsibilities.

There is also a risk associated with the accuracy of data included in the PACS. Although most PII is provided directly by the individuals themselves, it is possible that data could be inaccurately entered or mistakenly associated with the wrong individual. To reduce the risk of data being inaccurately entered or incorrectly associated, electronic data collection tools are used to the greatest extent possible and authorized GSA Property Management team members are trained to enroll and gather the appropriate information, and are reminded of the importance of collecting accurate information.

The E-PACS utilizes a registration engine, access control systems, and intrusion detection systems. The HID pivCLASS registration engine enrolls the individuals into the E-PACS, which requires the individual's full name, email address, and contact phone number. Additionally, it imports the X.509 certificates and JPEG image from the PIV

Credential. Once the information is imported into the E-PACS, the information is stored in the GSA E-PACS and is not shared externally. When the users gain access to a GSA-controlled facility with their PIV Credentials, the readers are used to verify the data from the PIV cards, ensuring the credential is valid by verifying the Card Authentication Key (CAK) each time the credential is used. If a credential is valid, the user is granted access to the facility, and if it found to have a revoked certificate, the user's card is suspended in the E-PACS and the user is denied access into the GSA-controlled facilities.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

The information imported directly from the PIV Credential reflects the issuing agency's record of information and should be accurate. If errors are found, the user must report it to the issuing authority within his or her agency to correct it.

The information provided upon enrollment is verified by the E-PACS administrator and compared to the elevated access form submitted by the facility's building manager or approving official. To address potential occurrences of data being inaccurately entered, information is reviewed by the E-PACS administrators when an Elevated Access Request form is received. Information entered is compared to the information on the form. If information is missing or is inaccurate, the E-PACS administrator may correct it when adding the elevated access based on the enrollment form.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

The E-PACS utilizes a registration engine, access control systems, and intrusion detection systems. The HID pivCLASS registration engine enrolls the individuals into the E-PACS, which requires the individual's full name, email address, and contact phone number. Additionally, it imports the X.509 certificates and JPEG image from the PIV Credential. Once the information is imported into the E-PACS, the information is stored in the GSA E-PACS and is not shared externally. When the users gain access to a GSA-controlled facility with their PIV Credentials, the readers are used to verify the data from the PIV cards, ensuring the credential is valid by verifying the Card Authentication Key (CAK) each time the credential is used. If a credential is valid, the user is granted access

to the facility, and if it found to have a revoked certificate, the user's card is suspended in the E-PACS and the user is denied access into the GSA-controlled facilities.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

Access to the PACS database is limited to authorized system administrators with the level of access limited to the minimum amount necessary to perform that user's job responsibilities. System administrators are federal employees who must have a minimum of a Tier 2 background investigation. Upon approval by the system owner, user-specific administration levels are provided based on administrator's need. Administrators are provided a unique username and may only access the system while on the GSA network.

Upon termination of employment or a change of assignment, administrative rights are removed or modified according to the situation.

6.2 Has GSA completed a system security plan for the information system(s) or application?

An SSP was previously completed 12/10/17. ATO was granted on 5/31/18.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

Security protocols are leveraging the TechOps GSS physical security settings for the off-site data center. E-PACS utilizes the GSA IT protocols for accessing the servers, using multi-factor authentication. Administrators utilize SSO and Short Name Accounts (SNAs).

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

EPACS leverages the GSA IT Incident Response Plan structure. An email alert is also sent to the EPACS team in the event of a failed login attempt.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

There is a privacy risk associated with handling of PII that occurs when data is extracted from the system and the individual using the data improperly distributes or stores the data. Additionally, there is a risk if an authorized individual misuses the system or conducts unauthorized activities. Additionally, in regards to the handling of PII, access to information is granted on a "need-to-know" basis, access to the E-PACS requires a GSA domain account and a network connection. E-PACS user accounts are individually approved by the owner(s) of the system. All administrators and enrollers receive IT Security Awareness Training and have been vetted with a background investigation that allows network access. Access to the E-PACS is also role-based and all activities are logged.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

Federal employees and contractors who routinely access GSA-controlled facilities via the electronic access are legally required to have and use a PIV-Credential to gain such access, and may also be required to use PIV Credentials on card readers to access certain internal locations. If an individual refuses to provide the appropriate information for the E-PACS, then they may be refused electronic access to the GSA-controlled facility. All information provided to or collected by E-PACS may be used for security and law enforcement purposes.

7.2 What procedures allow individuals to access their information?

GSA provides individuals with the ability to have access to their personally identifiable information (PII) maintained in its system of records. Individuals may request their records by contacting the E-PACS Program Manager. Additionally, individuals may submit a Freedom of Information Act (FOIA) request for access to their PII for information about any PII about them that is maintained in the E-PACS. Requests may be submitted to EPACS@gsa.gov.

7.3 Can individuals amend information about themselves? If so, how?

Individuals may correct inaccurate or erroneous information or update it by contacting their local property managers who may submit an additional Elevated Access Request form with the updates or corrected information, or by reaching out to the E-PACS team at EPACS@gsa.gov.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Individual participation may be enabled at the enrollment level if a property manager allows the individual to enter his or her own middle name, email address, and phone number. It is possible that data could be inaccurately entered or mistakenly associated with the wrong individual after entered. To reduce the risk of data being inaccurately entered or incorrectly associated, electronic data collection tools are used to the greatest extent possible and authorized GSA Property Management team members are trained to enroll and gather the appropriate information, and are reminded of the importance of collecting accurate information.

The same risk is present even without individual participation because if the user does not enter the information, the property management team would still have to manually input information to complete an enrollment into E-PACS. If errors are caught during the enrollment, the building management team notifies the E-PACS team for correction.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

All GSA employees and assigned contractor staff receive the Privacy Act and IT Security Awareness training, and have undergone necessary suitability investigations and receive security clearances for access to classified national security information and facilities.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

E-PACS administrator accounts are individually approved by the E-PACS system owner, and authorized by the Director of Physical Security. All administrators must have received the mandatory GSA IT Security Awareness Training and Privacy Act training. All administrators have been vetted for access to GSA Information Systems or for access to security information. Access to E-PACS is role-based and users of the system have access to a limited subset of data based on the concept of least privilege/limited access.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

The only individuals with access to the E-PACS are the E-PACS Administrators. All administrators' user access is based on pre-defined system owner and management authorized job roles and official duties. E-PACS administrators may only input, update, and delete records or fields to which they are authorized to have access and a need-to-know. Additionally, access control software on E-PACS prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Risks are minimal because the system currently collects a full name, email and a contact phone number in addition to the public x509 certificates and the JPEG from the PIV is stored in the system. These elements are only public elements from the PIV.

Erroneous data deletion is a possible risk; however only a limited number of administrators have that capability.

---

[1] OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.