NARA

Privacy Impact Assessment
for the

Enterprise Physical Access Control System

Points of Contact and Signatures

ISSO/IT Security POC	**PIA Author** (if different from POC)
Name: Office: Phone: Bldg./Room Number: Email:	Name: Deborah Anderson Office: B Phone: (301) 837-0972 Bldg./Room Number: A2/1201 Email: deborah.anderson@nara.gov
Chief Information Officer Name: Swarnali Haldar Office: I Phone: (301) 837-1583 Bldg./Room Number: A2/4500 Email: swarnali.haldar@nara.gov Signature and date signed: SWARNALI HALDAR Digitally signed by SWARNALI HALDAR Date: 2022.04.11 12:18:56 -04'00'	**System Owner** Name: Dave Adams Office: BX Phone: (301) 837-1720 Bldg./Room Number: A1/B7 Email: dave.adams@nara.gov Signature and date signed: DAVID ADAMS Digitally signed by DAVID ADAMS Date: 2022.04.08 15:38:33 -04'00'

Senior Agency Official for Privacy
Gary M. Stern
General Counsel
(301) 837-3026

Garym.Stern@nara.gov

Signature and date signed: GARY STERN Digitally signed by GARY STERN Date: 2022.04.08 09:00:14 -04'00'

[This PIA should be completed in accordance with the NARA 1609. The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: This section is an overview; the questions below elicit more detail.)

The EPACS (Enterprise Physical Access Control System) is a COTS (Commercial-off-the-shelf) product known as Lenel OnGuard (Cloud Edition). EPACS manages access to Archives I and Lyndon B. Johnson Library (LBJ), through the administration and monitoring of badge and door access information. Four additional sites (Ellenwood, Morrow, Carter Library and Washington National Records Center (WRNC)) are planned for implementation in Fiscal Year 2022 and additional sites are projected out for each fiscal year until all NARA owned locations are implemented. EPACS is accessed and deployed from the cloud via Amazon Web Services (AWS).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

EPACS manages access to Archives I and LBJ through the administration and monitoring of badge and door access information. EPACS contains the following information concerning NARA employees and contractors: legal name; date of birth; height; weight; hair color; eye color and assigned card number. EPACS provides auditing tools to create, maintain and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Each data element is necessary to positively identify the individual and to provide a badge giving the individual access to the building. Currently, audit logs are not checked to trace actions of users.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
☐	Statute	
☑	Executive Order	HSPD-12/FIPS 201
☐	Federal Regulation	
☐	Agreement, memorandum of understanding, or other documented arrangement	
☐	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "Other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
Example: Personal email address	✓	*B and C*	*Website will collect email addresses of individuals outside NARA*
Name	☑	A&B	First name, middle initial, last name
Date of birth or age	☑	A&B	Date of birth - Month/Day/Year
Place of birth	☐		
Gender	☐		
Race, ethnicity or citizenship	☐		
Religion	☐		
Social Security Number (full, last 4 digits or otherwise truncated)	☐		
Tax Identification Number (TIN)	☐		
Driver's license	☐		
Alien registration number	☐		
Passport number	☐		

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
Mother's maiden name	☐		
Vehicle identifiers	☐		
Personal mailing address	☐		
Personal email address	☐		
Personal phone number	☐		
Medical records number	☐		
Medical notes or other medical or health information	☐		
Financial account information	☐		
Applicant information	☐		
Education records	☐		
Military status or other information	☐		
Employment status, history, or similar information	☐		
Employment performance ratings or other performance information, e.g., performance improvement plan	☐		
Certificates	☐		
Legal documents	☐		
Device identifiers, e.g., mobile devices	☐		

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
Web uniform resource locator(s)	☐		
Foreign activities	☐		
Criminal records information, e.g., criminal history, arrests, criminal charges	☐		
Juvenile criminal records information	☐		
Whistleblower, e.g., tip, complaint or referral	☐		
Procurement/contracting records	☐		
Proprietary or business information	☐		
Location information, including continuous or intermittent location tracking capabilities	☑	A&B	Duty Station; Office #; intermittent location
Biometric data:			
- **Photographs or photographic identifiers**	☑	A&B	Photograph from badge
- **Video containing biometric data**	☐		
- **Fingerprints**	☐		
- **Palm prints**	☐		
- **Iris image**	☐		
- **Dental profile**	☐		
- **Voice recording/signatures**	☐		

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
- **Scars, marks, tattoos**	☐		
- **Vascular scan, e.g., palm or finger vein biometric data**	☐		
- **DNA profiles**	☐		
- **Other (specify)**	☐		
System admin/audit data:			
- **User ID**	☑	A&B	Collects UserID for EPACS privileged users
- **User passwords/codes**	☐		
- **IP address**	☑	A&B	Only available to a small subset of EPACS privileged users
- **Date/time of access**	☑	A&B	Collects date/time of physical access
- **Queries run**	☑	A&B	For investigations and troubleshooting purposes by EPACS privileged users only
- **Content of files accessed/reviewed**	☐		
- **Contents of files**	☐		
Other (please list the type of info and describe as completely as possible):	☑	A&B	Cardholder activity while in building
	☑	A&B	User activity while in EPACS system
	☐		
	☐		

3.2 Indicate below the source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	✓	Hard copy: mail/fax	☐	Online	☐
Phone	☐	Email	☐		
Other (specify):					

Other NARA records/sources (list systems):
Not applicable

Other government sources of information (list agency and source):
Not applicable

Non-government sources, check any that apply:					
Members of the public	☐	Public media, Internet	☐	Private sector	☐
Commercial data brokers	☐				
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the information will be shared and how that will occur, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer. (Check all that apply).

Recipient	How information will be shared			
	Individual users	Whole office/agency	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Within the office that collected the information	☐	☐	☑	For investigative purposes
With other offices within NARA	☑	☐	☐	For investigative purposes
With other agencies (list agencies):	☑	☐	☐	For investigative purposes
Public	☐	☐	☐	
Other (specify):	☐	☐	☐	

4.2 For non-archival information, if the information will be released to the public explain how the information will be de-identified, aggregated, or otherwise privacy protected. This question does not apply to archival information stored in a system that will undergo standard archival screening and processing in accordance with NARA 1601.

Not Applicable

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain why.

NARA 24 - Personnel Security Files

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Submission of the requested information is voluntary; however, refusal to provide such information will result in thd inability to obtain an access control card. Refusal to provide this information may also result in the inability to perform certain job related tasks because an individual will be unable to gain access to certain areas of the building where entry requires an access card. Without a Personal Identification Verification (PIV) card it may not be possible to log on to NARA computers or IT resources, impacting the ability to accomplish assigned tasks.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Users are not granted access to data within the system. Users can request changes as needed (i.e., name change, office location, etc.)

Section 6: Maintenance of Privacy and Security Controls

6.1 NARA uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

☑	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authority to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** 12/31/2021 **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding Plan Of Action And Milestones (POA&M) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POA&M documentation:**
☐	**This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:**
☐	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**
☑	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** System is monitored and maintained in accordance with all NARA and Federal policies/guidelines
☑	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by NARA policy**.
☑	**Indicate whether there is additional training specific to this system, and if so, please describe:** Yes, system training is provided as part of the contract

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The system resides on NARA's AWS environment and is monitored, patched and maintained in accordance with all NARA and Federal policies and guidelines.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by NARA.)

Records created and maintained in Enterprise PACS will primarily be covered by GENERAL RECORDS SCHEDULE 5.6: Security Records, Item 120, Personal identification credentials and cards. Temporary. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "Records" maintained in a "System Of Records," as defined in the Privacy Act of 1974, as amended).

☐ No. ☑ Yes.

7.2 Please cite and provide a link (if possible) to existing SORN(s) that cover the records, and/or explain if a new SORN is being published:

SORN NARA 24 - Personnel Security

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to NARA of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

Enterprise antivirus software and endpoint protection is deployed to EPACS components and monitored. Only authorized system administrators and application administrators will have authority to perform system monitoring. These individuals will have the appropriate clearances before monitoring authority is granted.

All users must login to EPACS with a unique user id and password and work processes of EPACS users can be monitored within the EPACS system. Users can only access those Agency records stored in EPACS according to the rights granted by their Administrators.

In addition, the Lenel OnGuard software being used to develop EPACS has extensive security controls built into the core functionality of the system. Furthermore, the EPACS SSP identifies the implementation of security controls appropriate for the Moderate baseline based on the NIST 800-53.

An initial EPACS security scan and assessment was conducted by NARA's independent assessors and the privacy related risks have been remediated. A Security Assessment Package is being prepared by the independent assessor that will include a Security Assessment Report (SAR), SSP, Risk Assessment Report (RAR), POA&M, and Certifier's recommendation. An ATO will be granted for the system by the appropriate authorizing officials in FY22. An annual assessment of select security and privacy controls is conducted by NARA's independent assessors. The SAR, RAR and POA&M are updated accordingly based on the results of the annual assessment. In addition to the annual assessment of security and privacy controls implemented on the system, the Cyber Security & Information Assurance Division (IS) and the Operations and Infrastructure Branch (IOO) have installed and monitors NARA's continuous monitoring tools deployed on the system. These tools are used to scan the system for vulnerabilities and configuration compliance and monitored for malicious activity.

Use this page for additional comments; specify which Section or page for which this is a continuation

Characters remaining: 5998