Privacy Impact Assessment (PIA)

Name of Project: Archives II Physical Access Control System

Project's Unique ID: AII PACS

Legal Authority(ies:	**44 U.S.C. 2104; HSPD-12; FIPS 201-2; ISC Standard: The Risk Management Process for Federal Facilities**

Purpose of this System/Application: The AII PACS technology supports access to NARA controlled facilities through the administration and monitoring of badge and building/door access and information. The NARA AII PACS is owned and operated by BX and supports efforts to achieve compliance with the Homeland Security Presidential Directive 12 (HSPD-12). The architecture consists of the Physical Access Control System (PACS) Server-Client architecture which operates a Commercial Off-the-Shelf (COTS) product - Lenel OnGuard version 7.0. This system is specific to the AII location. PIV cards and physical access at other NARA locations are administered through separate systems.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Employees		The Badging System collects the name of the person seeking a NARA badge. The system also assigns each user an identification number. The Access System collects the following information concerning NARA employees, contractors and volunteers: name, date of birth, height, weight, hair and eye color, and assigned card number. Lenel client software is installed on applicable workstations to provide an interface for administrators, badge personnel and security staff to support entry of cardholder information as well as alarm monitoring activities.
External Users		N/A
Audit trail information (including employee log-in information)		PACS allows authorized personnel to review individuals' access history using name and/or card number. Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Currently, audit logs are not checked to trace actions of users.

Other (describe)		None

Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

NARA operational records		None
External users		None
Employees		Legal Name; Date of Birth; Height; Weight; Hair color; Eye Color
Other Federal agencies (list agency)		N/A
State and local agencies (list agency)		N/A
Other third party source		Lenel OnGuard utilizes Intelligent System Controllers (ISCs) to grant or deny access to the facilities using information on access cards and stored on the Lenel OnGuard Database. The ISCs are responsible for transferring PACS head-end information back to the main Lenel server.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes, each data element is necessary to positively identify the individual and to provide a badge giving the individual access to the building.

2. **Is there another source for the data? Explain how that source is or is not used?**
No

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?
No

2. Will the new data be placed in the individual's record?
N/A

3. Can the system make determinations about employees/the public that would not be possible without the new data?
N/A

4. **How will the new data be verified for relevance and accuracy?**
N/A

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
N/A

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
N/A

7. **Generally, how will the data be retrieved by the user?**
Authentication to the PACS is controlled by the user logging onto the specific workstation that is connected to NARANet. This access is via individual username/password pairs. Authentication to PACS involves logging into the individual workstation.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.
Yes, information in PACS can be retrieved by an individual's name and/or unique identification card number. The identification number is generated by the system.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
The system allows for the creation of access history reports on individuals who have been assigned a NARA access badge. That report provides information concerning the movement of the badge holder within the building. It provides information concerning the areas the individual entered and the time of such entry. This information is usually used by security and Insider Threat personnel or the Inspector General for investigative purposes. Lists of individuals having access are extracted for use by program offices to validate individual's access to specific areas, particularly stacks, records holding and processing areas, to validate access authority or identify those no longer needing access. Lists are returned, with changes, to the Security Management unit to be purged.

Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Currently, audit logs are able to check trace actions of users and administrators.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
Yes. PACS can be used to allow NARA to treat the public, employees, or others differently. By granting a badge, we allow employees varying degrees of access to locations within the building. That access is determined based on the individual job related duties of the employee and the approvals granted by management and the physical security staff. By denying a badge, the system restricts public access to restricted or employee only areas.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.
Yes, the system tracks individual badge holders when they enter a location via access control card. The system contains the ability to trail the actions of users and administrators that trace security-relevant events to an individual, ensuring accountability.

12. What kinds of information are collected as a function of the monitoring of individuals?
Name, card number, location(s) entered, and time of such entry.

13. What controls will be used to prevent unauthorized monitoring?
Various level Access to PACS is restricted to Security, System Maintenance and Insider Threat Personnel. All servers and client workstations are maintained in limited access, high security areas or under 24x7 armed security presence. Monitors are equipped with privacy screens. Authentication to

PACS is controlled at (# number) layers. The user must log onto the specific workstation that is connected to PACS. This access is via individual username / password pairs. Moreover, authorized users of PACS are subject to the NARA wide personnel security controls. NARA personnel security controls are described in Section 1 of NARA IT Security Handbook. Please refer to NARA IT Security Handbook, Operations Controls for more information.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

N/A

Section 4: Sharing of Collected Information

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

The system administrator and authorized users have access to PACS. Please reference question 7 and question 8 in Section 3 as well.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.)? Are safeguards in place to terminate access to the data by the user?

The system administrator determines the user's access to the system based on the user's job and their need for access to the system in order to perform that job. Responsibilities are outlined in the Concept of Operations document for the PACS as well as the System Security Plan (SSP).

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

Access to information in the system is restricted by the system administrator based on job duties and need to know.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?

Authorized users of PACS are subject to the NARA wide personnel security controls. NARA personnel security controls are described in Section 1 of NARA IT Security Handbook, Operations Controls. This protocol reminds users to only use the system for the purpose for which it was created and consistent with their authorized duties. This message is reinforced in annual security training and is reinforced with issuance of NARA policy guidance on this topic.

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

Yes. Contractors installed the system, however, input is performed by NARA staff with physical security duties. Maintenance is performed by the integrator during the warranty period and by NARA contractors under the NARA Consolidated Facilities Maintenance (CFM) contract commencing when the warranty ends.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.

No

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

N/A

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The System Administrator for PACS is responsible for protecting the privacy rights of the public and employees affected by the interface. NARA's Senior Agency Official for Privacy is responsible for ensuring compliance with the privacy rights of the public and NARA employees.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

No

Section 5: Opportunities for Individuals to Decline Providing Information

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

Submission of the requested information is voluntary; however, refusal to provide such information will result in the 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. Also, without a PIV card it may not be possible to log on to NARA computers or IT resources, impacting the ability to accomplish assigned tasks.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A

Section 6: Security of Collected Information

1. **How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).**

Information in the system is provided by the individual seeking a NARA access badge (employee, contractor or volunteer). The individual provides documentation (driver's license, employment form SF-50, etc.) that is needed to verify their identity. We assume the individuals are providing accurate, timely and complete information regarding themselves. Secondary documents are assumed correct if they have not expired.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Client workstations are connected to the primary server housing the data and the primary and secondary servers are connected via NARANet. Data transfer/backup from the primary to offsite secondary server is managed by script every 24 hours.

3. What are the retention periods of data in this system?
Credentials and passes are temporary records and are destroyed in accordance with the disposition instructions in the NARA records schedule contained in FILES 203, the NARA Files Maintenance and Records Disposition Manual.

Identification credentials, including cards, badges and photographs are destroyed *three (3)* months after return to the issuing office.

Receipts, indices, listings, and accountable records are destroyed after all listed credentials are accounted for.

Visitor control files are not maintained in this system.

Visitor Control Files Registers or logs used to record names of outside contractors, service personnel, visitors and employees admitted to areas, and reports on automobiles and passengers are not maintained in this system.

Visitor Control Files For areas under maximum security, records are not maintained in this system.

Visitor Control Files For other areas, records are not maintained in this system.

Badges are renewed every five (5) years for employees and access every two (2) years for volunteers. Badges issued to contractors expire every five (5) years and access is shut off at the end of contract.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.
See records disposition schedule above. Obsolete information is deleted at the end of the disposition period. For renewals, outdated information is replaced with current information.

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA	
System Owner	
Will Fletcher (Signature)	7/5/17 (Date)
Name: Will Fletcher	
Title: Facility Security Chief Lead Security Specialist	
Contact information: ARC II 8601 Adelphi Road, Room 2310 College Park, MD 20740-6001 301-837-1491	
Senior Agency Official for Privacy (or designee)	
(Signature)	6/30/17 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 8601 Adelphi Road, Room 3110 College Park, MD 20740-6001 301-837-1750	
Chief Information Officer (or designee)	
Swarnali Haldar (Signature)	7/10/17 (Date)
Name: Swarnali Haldar	
Title: Information Services Executive/CIO	
Contact information: ARC II	

8601 Adelphi Road, Room 2310
College Park, MD 20740-6001
301-837-1583