U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Physical Access Control System (PACS)

Subsystem of Automated Access Control and Computer Enhanced Security System (ACCESS)

Office of Administration (ADM)

EA Number H0008

Version 1.3

02/01/2024

Document Revision History

Date	Version	PIA Name/Description	Author
02/01/2024	1.3	Updated document based on assessor feedback and questions	ADM
1/10/2023	1.2	Updated document based on assessor feedback and questions	ADM
09/12/2023	1.1	Updated document to reflect current environment and data collection methods	ADM Oasis Systems, LLC
08/15/2023	1.0	PACS PIA - Initial Release	ADM Oasis Systems, LLC
07/26/2023	DRAFT	PACS PIA Draft Release	ADM Oasis Systems, LLC

Table of Contents

The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: Physical Access Control System (PACS).

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): NRC campus and buildings.

Date Submitted for review/approval: January 10, 2024.

1 Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

The NRC uses the PACS system to control access to the NRC campuses and buildings.

Please mark appropriate response below if your project/system will involve the following:

☐	PowerApps	☐	Public Website
☐	Dashboard	☐	Internal Website
☐	SharePoint	☒	None
☐	Other		

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response:

	Status Options
☐	New system/project
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.*
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☒	Other (explain) The PACS subsystem PIA was part of the Consolidated ACCESS PIA and was split out into its own document per NRC's Privacy Officer request.

1.3 Points of Contact:

	Project Manager	System Owner /Data Owner /Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Denis Brady	Jennifer Golder	Tamar Katz	Michael England	Mark Daniels	Jennifer Golder
Office /Division /Branch	Office of Administration (ADM) /Division of Facilities & Security (DFS) /Security Management and Operations Branch (SMOB)	Office of Administration (ADM)	Office of Administration (ADM) /Division of Resource Management & Administration (DRMA)	Office of Administration (ADM) /Division of Facilities and Security (DFS) /Security Management & Operations Branch (SMOB)	Office of Administration (ADM) /Division of Facilities and Security (DFS) /Security Management & Operations Branch (SMOB)	Office of Administration (ADM)
Telephone	301-415-5768	301-287-0741	301-415-2500	301-415-0178	301-415-5772	301-287-0741

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	Authority	Citation/Reference
☒	**Statute**	• 10 CFR parts 10, 11, 14, 25, 50, 73, 95 • 42 U.S.C. 2011 et seq. • 42 U.S.C. 2165 and 2201(i) • 42 U.S.C. 2165–2169, 2201, 2201a, and 2284 et seq. • 42 U.S.C. 5801 et seq. • 44 U.S.C. 3501, 3504, and 3541 • 44 U.S.C. 36 • 5 CFR parts 731, 732 • 5 U.S.C. 301 • E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) • Electronic Government Act of 2002, 44 U.S.C. 36
☒	**Executive**	• Executive Order 10450, as amended

Mark with an "X" on all that apply.	Authority	Citation/Reference
	Order	• Executive Order 10865, as amended • Executive Order 13462, as amended by Executive Order 13516 • Executive Order 13467 • Executive Order 13526 • Executive Order 9397, as amended by Executive Order 13478
☒	Federal Regulation	• 10 CFR parts 10, 11, 14, 25, 50, 73, 95
☐	Memorandum of Understanding/ Agreement	
☒	Other (summarize and provide a copy of relevant portion)	• Federal Information Security Management Act of 2002 (Pub. L. 107-296, Sec. 3544) • Homeland Security Presidential Directive 12 (HSPD–12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004 • Interagency security committee standards "Physical Security Criteria for Federal Facilities," April 2010 • OMB Circular No. A–130, Revised

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*).

The PACS system contains names, facial image, badge number, campus, clearance level, and information about people who have access to the NRC campus and buildings. The NRC uses the access control information in the PACS system to control access to the NRC campus and buildings.

If the project collects Social Security numbers, state why this is necessary and how it will be used.

N/A.

3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

	Category of individual
☒	Federal employees
☒	Contractors
☐	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☒	Licensees
☐	**Other**

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table 2023.

	Categories of Information		
☒	Name	☐	Resume or curriculum vitae
☐	Date of Birth	☐	Driver's License Number
☐	Country of Birth	☐	License Plate Number
☐	Citizenship	☐	Passport number
☐	Nationality	☐	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☐	Home Address	☐	Credit/Debit Card Number
☐	Social Security number (Truncated or Partial)	☐	Medical/health information
☐	Gender	☐	Alien Registration Number
☐	Ethnicity	☐	Professional/personal references
☐	Spouse Information	☐	Criminal History
☐	Personal e-mail address	☒	Biometric identifiers (facial images, fingerprints, iris scans)
☐	Personal Bank Account Number	☐	Emergency contact e.g., a third party to contact in case of an emergency
☐	Personal Mobile Number	☐	Accommodation/disabilities information
☐	Marital Status	☐	**Other:**
☐	Children Information		
☐	Mother's Maiden Name		

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

The USAccess System collects the information. (USAccess is a federal shared service that provides Personal Identity Verification credentialing services.) The PACS system pulls the information from NRC Active Directory. (For details on how this information is passed from the USAccess system to NRC Active Directory, see ITI ICAM documentation.)

3.2 If using a form to collect the information, provide the form number, title and/or a link.

N/A.

3.3 Who provides the information? Is it provided directly from the individual or a third party.

The USAccess System collects the information. The PACS system pulls the information from NRC Active Directory. (For information on how this information is passed from the USAccess system to NRC Active Directory, see ITI ICAM documentation.)

3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.

The PACS system relies on the operators of the USAccess system to verify the accuracy and completeness of the information.

3.5 Will PII data be used in a test environment? If so, explain the rationale.

No.

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

N/A - The PACS system relies on the USAccess system to allow the subject individual to correct inaccurate or erroneous information.

4 Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

Access to the reports in the PACS system is limited to authorized users from DFS/SMOB, and authorized contractors. Persons must have a need-to-know to become authorized users and they can only access reports appropriate for their job responsibility. They undergo a rigorous background screening process and their need-to-know and access privileges are reviewed yearly.

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

PACS does not pass on any information to other systems.

4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

N/A.

Identify what agreements are in place with the external non-NRC partner or system in the table below.

	Agreement Type
☐	Contract Provide Contract Number:
☐	License Provide License Information:
☐	Memorandum of Understanding Provide ADAMS ML number for MOU:
☐	Other
☒	None

4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

The PACS system can generate reports which contains the data:

- Credential history reports
- Alarm history reports
- Operator history reports
- Device reports (number of card readers, number of alarm points, and so forth)

Logical access to the PACS system is limited to authorized users. Physical access to equipment displaying information is limited to the same authorized users.

Persons must have a need-to-know to become authorized users. They can only access information and features of the system appropriate for their job responsibility. They undergo a rigorous background screening process. Their need-to-know and access privileges are reviewed yearly.

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

Communication is encrypted.

4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).

The data is stored at the NRC.

4.7 Explain if the project can be accessed or operated at more than one location.

Information can only be accessed from the NRC network.

4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?

Yes, all contractors with access to the PACS system are badged by NRC.

4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.

Logical access to the PACS system is limited to authorized users. Physical access to equipment displaying information is limited to the same authorized users.

Persons must have a need-to-know to become authorized users. They can only access information and features of the system appropriate for their job responsibility. They undergo a rigorous background screening process. Their need-to-know and access privileges are reviewed yearly.

4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.

Yes, the PACS system stores PII and physical access information about individuals.

4.11 Define which FISMA boundary this project is part of.

The PACS system is a part of the ACCESS Federal Information Security Management Act (FISMA) boundary.

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
☐	Unknown
☐	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track*.
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity-Moderate Availability-Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

The ACCESS EA Number is H0008.

5   Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

	Response
☒	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)**
☐	**List the identifiers that will be used to retrieve the information on the individual.**
☐	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.**

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

	Response
☒	*Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)* *Provide the SORN name, number, (List all SORNs that apply):* • *Privacy Act Systems of Records* • *SORN NRC-40, "Facility Security Access Control Records"* • *SORN NRC-45, "Digital Certificate for Personal Identity Verification Records"*
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☐	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?

> *A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.*

Mark the appropriate response.

Options	
☐	**Privacy Act Statement**
☒	**Not Applicable**
☐	**Unknown**

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

N/A – The PII information is not collected by the PACS System. (For details on how the source information is collected, see ITI ICAM documentation.)

6   Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for NARA's Universal Electronic Records Management (ERM) requirements, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,

- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule
☒	NARA's General Records Schedules
☐	Unscheduled

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	ACCESS PACS
Records Retention Schedule Number(s)	GRS Schedule 5.6 – Security Management Records (see attached list for itemized schedules; please consult this link to determine if additional items are applicable to PACS)
Approved Disposition Instructions	See details below in table: GRS 5.6 item 111 GRS 5.6 item 190 GRS 5.6 item 090 GRS 5.6 item 120 GRS 5.6 item 170 GRS 5.6 item 171
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	Yes

Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Yes, the records are automatically deleted at the end of the retention period.
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	No permanent records are created.

GRS SCHEDULE NUMBER	SCHEDULE TITLE	DISPOSITION
GRS 5.6 item 090	Facility security management operations records	**Temporary.** Destroy when 30 days old, but longer retention is authorized if required for business use.
GRS 5.6 item 111	Visitor process records. All other facility security areas.	**Temporary.** Destroy when 2 years old, but longer retention is authorized if required for business use.
GRS 5.6 item 120	Personal identification credentials and cards. Application and activation records.	**Temporary**. Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use.
GRS 5.6 item 121	Personal identification credentials and cards. Cards.	**Temporary**. Destroy after expiration, confiscation, or return.
GRS 5.6 item 120	Temporary and local facility identification and card access records.	**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 5.6 item 170](#)	Personnel security investigative reports. Personnel suitability and eligibility investigative reports.	**Temporary**. Destroy in accordance with the investigating agency instruction.
[GRS 5.6 item 171](#)	Personnel security investigative reports. Reports and records created by agencies conducting investigations under delegated investigative authority.	**Temporary**. Destroy in accordance with delegated authority agreement or memorandum of understanding.
[GRS 5.6 item 190](#)	Index to the personnel security case files.	**Temporary**. Destroy when superseded or obsolete.

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

N/A – The PACS system does not collect information from persons. (For details on how the source information is collected, see ITI ICAM documentation.)

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

No.

7.3 Is the collection of information required by a rule of general applicability?

N/A.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: [https://intranet.nrc.gov/ocio/33456.](https://intranet.nrc.gov/ocio/33456)

8 Privacy Act Determination

Project/System Name: Physical Access Control System (PACS)
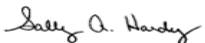
Submitting Office: Office of Administration (ADM)

Privacy Officer Review

	Review Results	Action Items
☐	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
☐	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☒	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

Covered by System of Record Notices: SORN NRC-40, "Facility Security Access Control Records" and SORN NRC-45, "Digital Certificate for Personal Identity Verification Records

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 02/21/24	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results
☒   No OMB clearance is needed.
☐   OMB clearance is needed.
☐   Currently has OMB Clearance. Clearance No._____

Comments:

Reviewer's Name	Title
[signature] Signed by Cullison, David on 02/21/24	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
☐	No record schedule required.
☐	Additional information is needed to complete assessment.
☐	Needs to be scheduled.
☒	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
Signed by Dove, Marna on 01/25/24	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

	Review Results
☐	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☒	This project/system **does** collect, maintain, or disseminate information in identifiable form.

I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Feibus, Jonathan
on 02/21/24

_____

Chief information Security Officer
Cyber Information Security Division
Office of the Chief Information Officer

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Physical Access Control System (PACS) Subsystem of Automated Access Control and Computer Enhanced Security System (ACCESS)

Date CSB received PIA for review:	**Date CSB completed PIA review:**
January 10, 2024	February 21, 2024

Action Items/Concerns:

Copies of this PIA will be provided to:

Gwendolyn Hayden
Acting Director
IT Services Development and Operations Division
Office of the Chief Information Officer

Jonathan Feibus
Chief Information Security Officer (CISO)
Office of the Chief Information Officer