U.S. Nuclear Regulatory Commission

Privacy Impact Assessment
Information Technology Infrastructure (ITI)
Identity, Credential, and Access Management (ICAM)
Office of the Chief Information Officer (OCIO)

Version 1.2
07/17/2025

Document Revision History

Date	Version	PIA Name/Description	Author
07/17/2025	1.2	Revised based on change to the contract, new template, and system involved	OCIO Oasis Systems, LLC
07/16/2025	DRAFT of v1.2	Revised based on change to the contract, new template, and system involved	OCIO Oasis Systems, LLC
02/01/2024	1.1	Revised based on change to the federal credentialing services USAccess	OCIO
07/25/2023	1.0	Initial Release of ITI_ICAM PIA in new template	OCIO Oasis Systems, LLC
07/13/2023	DRAFT	Draft Release - Completed ICAM PIA in new template	OCIO 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:

Identity, Credential, and Access Management (ICAM).

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform)

Database Server, SharePoint, Other Government Agency (GSA).

Date Submitted for review/approval: July 17, 2025.

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.

ICAM is a robust set of identity and credentialing services built on industry standard commercial off-the-shelf software running on the Nuclear Regulatory Commission (NRC) standard computing platforms. ICAM delivers Public Key Infrastructure (PKI) and One-Time Password (OTP) credentials to internal staff, contractors, and external partners. In addition, it provides single sign-on (SSO), identity management, and attribute synchronization services. ICAM includes processes for verifying the identity of certificate applicants, securely issuing certificates and keys and revoking certificates in a timely manner. ICAM also escrows encryption keys of employees and contractors to prevent loss of data in the event a user's data encryption key becomes unavailable. ICAM is a Privacy Act System of Records, identified as NRC-45, as defined by the Privacy Act of 1974.

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

☐ PowerApps	☐ Server/Database Design
☒ Dashboard	☐ Public Website
☒ SharePoint	☒ Internal Website
☒ Cloud Service Provider	☒ Other (General Service Administration's USAccess PIV System)

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.* The NRC has transitioned its Personal Identity Verification (PIV) card system from an internally hosted system to the General Service Administration's (GSA) USAccess PIV System.
☐	Other (explain)

1.3 Points of Contact: (Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.)

Role	Contact Information Name Office/Division/Branch Phone Number
Project Manager(s)	TBD
System Owner/Data Owner or Steward	Jonathan Feibus OCIO/ITSDOD 301-415-0717
ISSM	**Branden Jarrell** OCIO/CISD/IAOB/IAT 301-415-4074 **Zanira Khan** OCIO/CISD/IAOB/IAT 301-415-5248
Executive Sponsor	TBD
Other	**James Peyton** OCIO/CISD 301-287-0701

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**	N/A
☒	**Executive Order**	Homeland Security Presidential Directive 12
☐	**Federal Regulation**	N/A
☐	**Memorandum of Understanding/Agreement**	N/A
☒	**Other (summarize and provide a copy of relevant portion)**	OMB Memorandum M-22-09

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 purpose of **ICAM** and the data it collects is to identify applicants and verify identity information provided by those applicants in support of a request for electronic credentials for access to federal facilities, networks, computer systems, and Internet-based e-Government applications.

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

ICAM may require the use of Social Security Number (SSN) information for confirmation of applicant identity or for federal processing requirements. All SSN data is encrypted to applicable federal standards at rest and during transmission.

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 **N/A**

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/Home Number	☐	Accommodation/disabilities information
☐	Marital Status	☐	Other N/A
☐	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).

For internal staff, information is collected from the PSATS and FPPS to ensure accuracy and consistency of information used for identity credentials. Information from the PSATS and/or FPPS is a data transfer. Information is collected from online registration and paper submissions completed by the applicant. Information is also collected through the General Service Administration's USAccess PIV System.

For External Partner applicants, the provided identity information may be validated using an external service that accesses one or more authoritative repositories intended for identity verification.

In addition, External Partner company names are verified against Secretary of State business Records, and company affiliation is verified through a telephonic employment check.

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

N/A.

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

Directly from the individual. For internal staff, information is collected from the PSATS and FPPS to ensure accuracy and consistency of information used for identity credentials.

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

Directly from the individual.

3.5 Will PII data be used in a test environment? If so, explain the rationale for this and how the PII information is protected.

N/A.

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

Users have access to EIH SailPoint IdentityIQ which allows them to update personal information such as name and home contact information, office location & phone numbers, organizational information such as position and organization information, as well as the ability to update emergency contact 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).

System administrators with a need-to-know.

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.

NRC e-Government applications may have access to External Partner credential information when a controlled access mechanism is available.

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

If so, 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 Online searches for copies of an individual's public digital certificate using the Public Certificate Repository portion of the ICAM system; and Data transmitted to the Office of Personnel Management (OPM) as part of the vetting process for internal applicants. OPM has access only to the data transmitted, not to the system. The Public Certificate Repository is made available to all agencies, organizations, and the public. The Office of Personnel Management (OPM) Fingerprint Transaction System receives transmitted applicant data.
☐	None

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

Data can only be accessed through privileged accounts and a PIV card.

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).

ICAM transmits content to staff over the NRC's ITI internal network. ICAM communicates with the General Service Administration's USAccess PIV System for data transfer. The data is encrypted and so is the communication.

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

Stored at NRC database.

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

Headquarters and all Regions.

4.8 Can the project be accessed by a contractor? Have the contractors completed an IT-II investigation? Do they possess an NRC badge?

Yes, contractors possess a badge and PIV card.

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

All privileged role holders must meet qualifications and sign special Rules of Behavior for Trusted Persons which are periodically renewed. Private Key recovery requires a minimum of two authorized administrators with administrator certificates and key recovery privilege. Defined system security events trigger email alerts. Viewing audit data requires administrator privileges.

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

No.

4.11 Define which FISMA boundary this project is part of.

ICAM is a subsystem of the Information Technology Infrastructure (ITI) 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 ITI EA# is 20090005.

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, or other unique number, etc.)** **List the identifiers that will be used to retrieve the information on the individual.** Name
☐	**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):* NRC 45 - Electronic Credentials for Personal Identity Verification
☐	**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?

Mandatory via PSATS and FPPS.

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)	ICAM
Records Retention Schedule Number(s)	See Table Below:
Approved Disposition Instructions	
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.	ICAM will be assessed using the Records and Information (RIM) Certification process. The structured process will provide criteria aligned with the Suggested Rating to accurately reflect the system's ability to support records management requirements.
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	ICAM will be assessed using the Records and Information (RIM) Certification process. The structured process will provide criteria aligned with the Suggested Rating to accurately reflect the system's ability to support records management requirements.

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)**	TBD

Records Retention Schedule Number(s)	Approved Disposition Instructions
GRS 3.1 – General Technology Management Records	**See all related dispositions.**
GRS 3.2 Information Systems Security Records	**See all related dispositions.**
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 – Cards	**Temporary.** **Destroy after expiration, confiscation, or return.**
GRS 5.6 item 130 – 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.**

Note: Information in *Section 6, Records and Information Management-Retention and Disposal* does not need to be fully resolved for final approval of the privacy impact assessment.

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 more 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?

Yes.

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?

No.

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.

8 Privacy Act Determination

Project/System Name: Information Technology Infrastructure (ITI), Identity, Credential, and Access Management (ICAM)
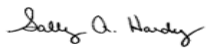
Submitting Office: Office of the Chief Information Officer (OCIO)

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 NRC 45 - Electronic Credentials for Personal Identity Verification.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 09/11/25	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. <u>3150-0267</u>

Comments:

Reviewer's Name	Title
[signature] Signed by Cullison, David on 08/21/25	Agency Clearance Officer
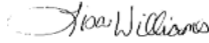
10 Records Retention and Disposal Schedule Determination

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 09/08/25	Sr. Program Analyst, Electronic Records Manager
Signed by Williams, Lisa on 09/04/25	Records and Information Management Specialist

11 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 Nalabandian, Garo
on 09/11/25

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

ADDITIONAL ACTION ITEMS/CONCERNS

<table>
<tr><td colspan="2">Name of Project/System:

Information Technology Infrastructure (ITI), Identity, Credential, and Access Management (ICAM)</td></tr>
<tr><td>Date CISD received PIA for review:

September 8, 2025</td><td>Date CISD completed PIA review:

September 10, 2025</td></tr>
<tr><td colspan="2">Action Items/Concerns:

</td></tr>
</table>