ADAMS ML19029A117

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Identity, Credential, and Access Management (ICAM)

Date: January 29, 2019

A. GENERAL SYSTEM INFORMATION

1. Provide a brief description of the system:

Identity, Credential, and Access Management (ICAM) is a robust set of 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. It is used by NRC Staff, NRC Contractors, Agreement States, licensees, and members of the public that have a need to securely interact with NRC public-facing systems. ICAM is a sub-system of the Information Technology Infrastructure (ITI) system for agency inventory purposes.

2. What agency function does it support?

ICAM supports the agency's regulatory mission by enabling licensees, stakeholders, and the public to securely submit documents and data electronically. To do this, ICAM provides credential enrollment, issuance, maintenance, and transaction validation services to external and internal users of agency applications. ICAM supports the agency's facility security program through issuance and maintenance of NRC Personal Identity Verification (PIV) cards for employee and contractor identification and secure building access. ICAM supports the agency's information security program by ensuring that only persons with approval from Personnel Security get credentials for access to

networked information. ICAM credentials are used agency-wide by applications requiring strong user authentication, digital signature, and user-to-user encryption to meet agency security requirements.

3. Describe any modules or subsystems, where relevant, and their functions.

This section describes the various services the ICAM system offers to both NRC internal users and non-NRC external partners.

HSPD-12 PIV Cards

To meet the goals and objectives outlined in Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standards (FIPS) 201, the ICAM Program provides PIV Card services to NRC staff and contractors. This includes services such as issuance, cancellation, and renewal. The NRC-issued PIV Cards are used for both logical and physical access.

PIV-Derived Credentials

To support secure access to NRC remote access applications such as Broadband Remote Desktop (BRD) and Outlook Web Access (OWA), ICAM provides credential lifecycle management services for Shared Service Provider Software Certificates as well as One-Time Password (OTP) credentials.

ICAM Password Wallet (Legacy)

To reduce security risks of users having to manage many different system passwords, the agency is operating an encrypted password vault, the ICAM Password Wallet. This service stores and then supplies the user's ID and password when logging in to any supported application. A user's password wallet is encrypted and protected by his or her network login credential, the PIV card. The ICAM Password Wallet is built on Oracle's "Enterprise Single Sign-On" suite and follows the NRC's Universal Access Strategy.

The ICAM Password Wallet was retired from use in May 2018. It will be removed from future versions of this document.

OTP Credential

ICAM provides OTP credentials to enable two-factor authentication to certain public-facing web applications, such as Webmail. OTP credentials generate security codes that do not transmit personal information. NRC-hosted validation servers bind the security code to a user identifier, using Symantec hosted VIP Authentication Services to verify the security codes.

Enterprise Identity Hub

ICAM's Enterprise Identity Hub is built on the SailPoint IdentityIQ Identity Management (IdM) software product. This service provides a secure central repository for electronic identity information, and automates the creation of certain network accounts and services. Identity attributes are keyed-in once at the Self-Service Portal or authoritative system and updated automatically on interfacing systems and applications.

E-Authentication Level 1 Credentials

The NRC provides digital certificates compliant at National Institute of Standards and Technology (NIST) Electronic-Authentication (E-Authentication) Level 1 for access to NRC applications where strong identity verification is not a requirement. This access may be in the form of authentication or document submission. An NRC digital certificate is issued to the end-user based upon communication to a valid email address.

The Level 1 service is currently in use by several NRC applications and systems, including Electronic Information Exchange (EIE) General Forms, EIE Adjudicatory, EIE Criminal History, and Emergency Response Data System (ERDS).

E-Authentication Level 3 Credentials

EAuthentication Level 3 services provide credentials in a manner that establishes a strong level of assurance that the user presenting the credential is who he or she claims to be.

The credentialing workflows take user information from the ICAM repository and where appropriate populate the relying applications' identity data repository. The workflows provide for establishing the identity of the user and entering initial information about the user's role into the application system. ICAM does not establish user access privileges within the application - that is the responsibility of the application owner.

Applications and programs that may use this level of authentication include Integrated Source management Portfolio (consisting of National Source Tracking System, Web-Based Licensing, and Licensed Verification System) and EIE proprietary data and Protective Order Files, where the user is required to have a software certificate issued using in-person identity verification to meet e-authentication Level 3. Medium Assurance will also be used for the Fitness for Duty application that requires Level 2 authentication.

ICAM offers credentials under this service: One-time Password credentials.

E-Authentication Level 3, One-Time Passwords

As an alternative Level 3 credential, ICAM issues platform-independent credentials in the form of OTP.

4. What legal authority authorizes the purchase or development of this system?

5 U.S.C. 301; Electronic Government Act of 2002, 44 U.S.C. Chapter 36; the Paperwork Reduction Act of 1995, 44 U.S.C. 3501; Government Paperwork Elimination Act, 44 U.S.C. 3504; Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Executive Order 9397.

5. What is the purpose of the system and the data to be collected?

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.

6. Points of Contact:

Information System Security Officer	Office/Division/Branch	Telephone
Katie Harris	**OCIO/SDOD**	**301-287-0515**
Business Project Manager	Office/Division/Branch	Telephone
Robert Randall	**OCIO/SDOD**	**301-287-0828**
Technical Project Manager	Office/Division/Branch	Telephone
James Peyton	**OCIO/SDOD**	**301-287-0701**
Executive Sponsor	Office/Division/Branch	Telephone
Thomas Rich	**OCIO/SDOD**	**301-287-0763**

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System _X_ Modify Existing System ____ Other (Explain)

b. If modifying an existing system, has a PIA been prepared before?

Yes

(1) If yes, provide the date approved and ADAMS accession number.

The MPKI Privacy Impact Assessment was approved 03/23/2006 (Accession number: ML060580656).

The MPKI Privacy Impact Assessment was updated and converted to the ACS Privacy Impact Assessment on 08/12/2009 (Accession number: ML092370560).

The ACS Privacy Impact Assessment was updated and converted to the ICAM Privacy Impact Assessment on 07/13/2012 (Accession number: ML12248A364).

The ICAM Privacy Impact Assessment is updated on 04/08/2016.

The ICAM Privacy Impact Assessment is updated on 08/07/2018.

(2) If yes, provide a summary of modifications to the existing system.

The document is converted to a new PIA template. The system modules are updated.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

ICAM maintains information about anyone who has applied for or had a certificate or credential amended, renewed, replaced, suspended, revoked, or denied or provides information through the EIH Identity Self-Service Portal The groups of individuals include the public, Federal employees, Federal contractors, licensees, attorneys, vendors, and overseas foreign nationals.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific)?

Subscriber Digital Certificates

These are X.509 standard certificates. The electronic certificate file includes the subscriber's name, e-mail address, organizational affiliation (e.g. NRC), and the cryptographic public key that corresponds to the private key in the subscriber's possession (e.g. on their computer or smart card). Certificates are issued and labeled for different purposes, including digital signature, encryption, and authentication.

Public repository of digital certificates

To facilitate the use of digital certificates for data encryption and signature verification, a certificate lookup service is hosted on a public web site at the Shared Service Provider facility.

Subscriber Encryption Certificate private keys

This item applies to the PIV card and PIV-derived credential modules only. In order to minimize the likelihood of data loss in the event an NRC employee or contractor's encryption key becomes unavailable, the system places a copy of the key into a secure escrow, in accordance with the Federal PKI Common Policy. Recovery of the cryptographic key requires a minimum of two authorized personnel with PKI Administrator certificates. Different portions of the data needed to recover the key are maintained at NRC and at the Shared Service Provider facility.

PKI audit data

In accordance with federal PKI policy (Federal Bridge Certification Authority and Common Policy) audit data describing system transactions including applicant enrollment, identity proofing, certificate issuance, revocation, and key recovery, are maintained by the system. When the audit data is aggregated, the name of the PKI Administrator performing the action is associated with the audit event. Different portions of the audit data are maintained at NRC and at the Shared Service Provider.

Certificate revocation data

To facilitate the timely validation of certificates presented to an application, information about revoked certificates is maintained on publicly accessible web servers at the Shared Service Provider. The Certificate Revocation List (CRL) is a digitally signed list of certificate serial numbers and revocation timestamps. The certificate serial number corresponds to the digital certificate posted on the public repository site.

Ordinary signature

Certain external partner enrollment forms and subscriber agreements may require an ink signature. Signed documents are stored at an external service that is used to verify external partner identity via the use of authoritative repositories. Stored records are retained for the required retention period as determined by Federal Bridge assurance level requirements, non-publicly available, with limited access.

Subscriber Agreement

An External Partner Subscriber Agreement may include identity-proofing data such as name, home address, and date of birth. The Subscriber Agreement form is stored as explained for Ordinary Signature above.

Identity Verification Information

External Partner applicant provided identity information may be validated using an external service that accesses one or more authoritative repositories intended for identity verification. The responses from these repositories may be stored in the PKI audit data as described in that section above.

Digital Fingerprint Images (Internal Staff PIV only)

As required by FIPS 201, digital fingerprint images are taken of the applicant and stored encrypted in the Internal Staff subsystem. The fingerprint images are used to initiate the required federal background investigation process, and to confirm the identity of the applicant when picking up or replacing his or her PIV card.

Social Security Number

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.

Financial Data

To meet federal requirements, external partner applicants may be asked for financial account information for identity verification purposes. Financial account information is encrypted to applicable federal standards at rest and during transmission.

Personal Information

Personal contact information: nickname, alternate last name, home address, personal email address, and personal telephone numbers are collected and processed to reduce duplicate data entry and to facilitate NRC notifications such as closures or during emergencies.

Office Information

Work office information: affiliation, physical location, mail stop and telephone numbers are collected and processed to reduce duplicate data entry and to provide a single authoritative source for downstream systems.

Organizational Information

Organization information: Contracting Officer Representative (for contractors), supervisor, title, office, and division are collected and processed to reduce duplicate data entry and to provide a single authoritative source for downstream systems.

Emergency Contact

NRC employees or contractors may opt to provide emergency contact information on a relative or friend, such as name, home address, email address and personal telephone numbers. This information is collected and processed to facilitate NRC notifications during emergencies.

c. Is information being collected from the subject individual?

Yes

(1) If yes, what information is being collected?

From internal staff: name, date of birth, social security number, organization, job function, e-mail address, telephone number, NRC badge number, ordinary signature, security clearance level, emergency responder role, photograph, fingerprints, height, eye color, and hair color.

From external partners: name, date of birth, social security number, home address, home telephone number, organizational affiliation, business address, business telephone number, driver's license number or photocopy, other government-issued ID number or photocopy, ordinary signature, financial account number.

In the case of emergency contact information, NRC employees or contractors may provide the name, address, email, and phone number of a desired contact not directly affiliated with the NRC.

d. Will the information be collected from 10 or more individuals who are <u>not</u> Federal employees?

Yes

(1) If yes, does the information collection have Office of management and Budget (OMB) approval?

No, the collection of this type of information is considered exempt under the Paperwork Reduction Act of 1995.

(a) If yes, indicate the OMB approval number:

N/A

e. Is the information being collected from existing NRC files, databases, or systems?

Yes, for internal staff only, information is collected to ensure accuracy and consistency of information used for identity credentials.

(1) If yes, identify the files/databases/systems and the information being collected.

ICAM collects PII information from the following NRC systems:
Personnel Security Adjudication and Tracking System (PSATS) – staff member name, organization, SSN, date of birth, citizenship, birth country and state, and security clearance level
Federal Personnel/Payroll System (FPPS) – staff member name, SSN, and organization
Intercede MyID - Photo

f. Is the information being collected from external sources (any source outside of the NRC)?

No. Information provided by external partner applicants is only verified against authoritative repositories for accuracy.

(1) If yes, identify the source and what type of information is being collected?

N/A

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

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

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.

h. How will the information be collected (e.g. form, data transfer)?

Information from the PSATS and/or FPPS is a data transfer. Otherwise, information is collected from online registration and paper submissions completed by the applicant.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

N/A

(1) If yes, identify the type of information (be specific).

N/A

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

N/A

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

The information is used to verify the identity, organizational affiliation, identity credentials presented, and other attributes that may be asserted by an applicant for the issuance or renewal of an electronic identity credential. In the event of possible misrepresentation or misuse of an NRC-issued credential, the

information will be used to reconstruct identity proofing and registration events and may be turned over to law enforcement.
Information is also used to provision accounts for network and email access.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes

3. Who will ensure the proper use of the data in this system?

The system owner, assisted by the Information System Security Officer, will ensure the proper use of the information.

4. Are the data elements described in detail and documented?

Yes

a. If yes, what is the name of the document that contains this information and where is it located?

The ICAM System Architecture Design document, in ICAM files

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

a. If yes, how will aggregated data be maintained, filed, and utilized?

N/A

b. How will aggregated data be validated for relevance and accuracy?

N/A

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

N/A

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific.)

The public can retrieve certificates by name and by e-mail address from (https://pki-search.symauth.com) the Symantec Digital ID Center. This service is available to anyone on the Internet.

Internal agency access to information in ICAM will be by name, email address or ICAM ID (established by the ICAM Program). The Personnel Security Branch, Office of Administration (ADM), may retrieve information using name or an agency-specific identifier.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No

a. If yes, explain.

N/A

(1) What controls will be used to prevent unauthorized monitoring?

8. List the report(s) that will be produced from this system.

The CRL

a. What are the reports used for?

The CRL is used to verify that a certificate is still valid.

b. Who has access to these reports?

The public has access to this report.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Currently the NRC offices with access to the information are the NMSS, ADM, and OCIO. Eventually this will include all NRC offices when a central identity repository is in place.

(1) For what purpose?

OCIO accesses the information to manage the applicant enrollment and validation process leading to issuing a credential. Other offices will access the information to provide Program Sponsor approval of a credential application, and to verify an application user's credential status.

(2) Will access be limited?

Yes

2. Will other NRC systems share data with or have access to the data in the system?

Yes

(1) If yes, identify the system(s).

Physical and logical access systems implemented at the NRC as part of the federal HSPD-12 program, have access to information concerning internal staff credentials for validation purposes only. NRC e-Government applications may have access to external partner credential information when a controlled access mechanism is available.

(2) How will the data be transmitted or disclosed?

Non-public information is only disclosed to an approved Program Sponsor within the secure workflow when the Sponsor is notified of an application pending his or her review.

3. Will external agencies/organizations/public have access to the data in the system?

Yes. There are two scenarios in which information is shared or made available: 1) Online searches for copies of an individual's public digital certificate using the Public Certificate Repository portion of the ICAM system; and 2) data is 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 and not to the system.

(1) If yes, who?

Public Certificate Repository is made available to all agencies, organizations, and the public.

OPM Fingerprint Transaction System receives transmitted applicant data.

(2) Will access be limited?

Public Certificate Repository has no access restrictions.
OPM related data is available to authorized OPM individuals performing the vetting process.

(3) What data will be accessible and for what purpose/use?

Public Certificate Repository: The public certificates are accessible to foster secure communication, and the CRL to allow those relying on the certificates to check the revocation status.

OPM Fingerprint Transaction System: identity information including internal applicant social security number and biometrics.

(4) How will the data be transmitted or disclosed?

Public Certificate Repository: Access to certificates is by web site using the Hyper Text Transfer Protocol Secure (HTTPS) Internet protocol and requiring search criteria to retrieve a certificate. Access to the digitally signed CRL is freely available by HTTP and Lightweight Directory Access Protocol Internet protocols (IP).

OPM Fingerprint Transaction System: The interconnection originates at the Internal Staff Registration Authority Application Server in the NRC Data Zone via the SMTP Internet protocol to the NRC Virtual Private Network (VPN) Gateway. The NRC VPN Gateway translates (Network Address Translation) the destination IP address to the IP address of the OPM's VPN Gateway. The OPM VPN Gateway translates the IP address to the IP address of the OPM Simple Mail Transfer Protocol (SMTP) server. Once the connection is established an electronic submission is made using data within the SMTP communication. No personal computers or human users participate in the interconnection.

E. RECORDS 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). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs?

Yes

(1) If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved

retention or exported to a file for transfer based on their approved disposition?

Most of the data/information in the system is covered by several GRS schedules below. However, some records in the system will need to be scheduled as they do not follow under a current GRS; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are Permanent. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.

General Records Schedules (GRS) available for use are the following:

GRS 5.6 – Security Records, items 120, 121, and 130

GRS 3.1 – General Technology Management Records

GRS 3.2 Information Systems Security Records

Records	Citation	Retention	Comments
System Access Records, includes **User Identification, Profiles, Authentications and Password Files** EXCLUDING records relating to electronic signatures.	GRS 3.2 item 031	Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.	Formerly GRS 24 item 6. a
System Access Records, includes **Routine systems**, ie, those not covered above.	GRS 3.2 item 030	Temporary. Destroy when business use ceases.	Formerly GRS 24 item 6. b
PKI administrative records. FBCA CAs.	GRS 3.2 item 060	Temporary. Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on maximum level of operation of the CA, or when no longer needed for business, whichever is later.	Formerly GRS 24 item 13.a(1)

PKI administrative records. Other (non FBCA et al) CAs	GRS 3.2 item 061	Temporary. Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.	Formerly GRS 24 item 13.a(2)
PKI Transaction-specific records. ****Not sure if these records are created/maintained in ICAM; I included it as part of "PKIs"**	GRS 3.2 item 062	Temporary. Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the **case of permanent records**, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.	Formerly GRS 24 item 13. b
External records such as -Digital Fingerprint Images -Financial data -Identify Verification Data			TBD
ICAM System Architecture Design Document	GRS 3.1 item 051	Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.	

(2) If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

N/A

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

N/A

3. Would these records be of value to another organization or entity at some point in time? Please explain.

N/A

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

N/A

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

N/A

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

N/A

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

N/A

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

The Symantec Digital ID Center requires no password as its purpose is to make certificates available to the public as widely as possible to facilitate secure

communication. Separate components of the ICAM system that are not linked to the Digital ID Center store more information related to the subscriber (date certificate was issued and by whom, if the certificate was revoked - date and by whom). These components are restricted to a small number of qualified ICAM Administrators and a special digital certificate is required for access.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

All privileged role holders within ICAM must meet qualifications and sign special Rules of Behavior for Trusted Persons. Private Key recovery requires a minimum of two authorized administrators with administrator certificates and key recovery privilege. Viewing audit data requires administrator privileges.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

(1) If yes, where?

Trusted Access Requirements	(Accession Number: ML081360011)
Trusted Person Agreement	(Accession Number: ML11081A011)
System Security Plan	(Accession Number: ML11207A214)

4. Will the system be accessed or operated at more than one location (site)?

Yes, at NRC offices and at Shared Service Provider facilities.

a. If yes, how will consistent use be maintained at all sites?

Use and operation of the ICAM system regardless of location is governed by the Symantec Shared Service Provider Certification Practice Statement for internal staff services, and the Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement for external partner services.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

Users, managers, system administrators, ICAM administrators, and the public.

6. Will a record of their access to the system be captured?

All access is audited and stored in logs of the respective modules and components.

a. If yes, what will be collected?

User ID, full name, and time for all login events are collected. Audit information for security-related events also includes system activity performed.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

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

9. Are the data secured in accordance with FISMA requirements?

Yes

a. If yes, when was Certification and Accreditation last completed?

September 17, 2017. See parent system information for ITI.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO Staff)

System Name: ICAM (for NRC-45, "Electronic Credentials for Personal Identity Verification")

Submitting Office: OCIO

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
This system is maintained as part of the NRC's Privacy Act System of Records NRC-45, Electronic Credentials for Personal Identify Verification and NRC-36, Employee Locator Records.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	02/08/2019

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:
OGC has concluded that the information required to obtain a Level 3 Credential is "necessary to identify" the individual seeking the credential under NIST 800-63-2, which is required under OMB and captured in the exclusion from the PRA in 5 CFR § 1320.3(h)(1).

Any changes to the system to collect information from other than government employees beyond that required for a Level 1 and Level 3 Credential may require OMB approval.

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	01/29/19

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

__X__ Needs to be scheduled – External records such as
-Digital Fingerprint Images
-Financial data
-Identify Verification Data

__X__ Existing records retention and disposition schedule covers the system for all other data - no modifications needed.

Comments:

Some data/information in the system will need to be scheduled; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are **Permanent**. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	2/1/19

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date February 12, 2019

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise
Management Services Division
Office of the Chief Information Office

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT /
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Thomas Rich, Office of the Chief Information Officer (OCIO)**	
Name of System: **ICAM (for NRC-45, "Electronic Credentials for Personal Identity Verification")**	
Date ISB received PIA for review: **January 29, 2019**	Date ISB completed PIA review: **February 8, 2019**
Noted Issues:	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ February 12, 2019**
Copies of this PIA will be provided to: *Tom Rich, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Services Division* *Office of the Chief Information Officer*	