ADAMS ML17173A083

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.

Automated Access Control and Computer Enhanced Security System (ACCESS)

Date: June 5, 2017

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The automated access control and computer enhanced security system (ACCESS) is a physical security information management (PSIM) system used to continuously monitor the safety and security of agency facilities. The system consists of a personal identity verification (PIV) card issuance (ACCESS-PCI) subsystem , a physical access controls (ACCESS-PACS) subsystem, Federal visitor Kiosk subsystem, internet protocol (IP) closed circuit TV network subsystem, emergency communications (ECS) subsystem. ACCESS correlates data from all of these devices and presents it to the agency staff responsible for the security of facilities and personnel. Note:*In the PIV card creation work process personally identifiable information (PII) is collected for other agency systems but no PII is maintained or stored within this system. By office policy the agency criminal history system, though not connected to the ACCESS system, is included in its FISMA boundary.

This system is deployed across all US Nuclear Regulatory Commission (US NRC) facilities and supports the agency mission to provide security services to the US NRC workplace. This system operates under US NRC Privacy Act systems of records NRC-40 “Facility Security Access Controls Records,” and NRC-45, “Digital Certificates for Personal Identity Verification Records.”

2. What agency function does it support?

- ACCESS supports the safety and security of NRC personnel, property, information, systems and assets.

3. Describe any modules or subsystems, where relevant, and their functions. ACCESS consists of the following components:

- ACCESS Personal Identification Verification Card Issuance (ACCESS-PCI). Produces and manages the lifecycle of employee personal identification verification (PIV) cards. Under Homeland Defense Presidential Directive #12, all federal employees and contractors are required to possess a PIV card to physically access federal facilities. The cards contain sensitive information including the cardholder unique identifier (CHUID), PIN, two biometric fingerprints, PIV authentication key, card authentication key, digital signature key and a key management key. All keys are created and maintained on the card except for the key management key, with is stored by the agency to ensure the user's encrypted data can be retrieved in an emergency. The NRC information type is currently categorized under OCIO-CS-PROS-2001, March 27, 2017 as "personal identity and authentication information and security management information".

- ACCESS Physical Access Control System (ACCESS-PACS). Authenticates the identity of NRC employees, contractors holding PIV cards and enforces agency security policies to gain physical entry to NRC facilities through the use of automated barriers. Security guards also validate the identity of employees via the use of "swipe & show" software at building entries. This software displays an identification photo of employees which is compared to the employee as they swipe PIV cards against ACCESS-PACS card readers to enter facilities. The NRC information type is currently categorized under OCIO-CS-PROS-2001, March 27, 2017 as "personal identity and authentication information and security management information"

- Closed Circuit TV Network. Monitors the IP closed circuit television (CCTV) network in facilities garages, building entries, exits and common areas. The CCTV provides assessment capability and archives camera recordings of activities. Only authorized facilities security specialist can connect directly to the CCTV network to view video feed from cameras, and to review archived video to support law enforcement activities.

- Emergency Communications System. Improves physical security radio communications. The internet protocol (IP) based radio communications system extends encrypted radio signals using the information technology infrastructure (ITI) to all agency security specialists and agency personal security officers (PSO)s. The system also facilities agency communication capabilities between agency security personnel and community first responders.

- Federal Visitor Kiosk. Authenticates the identity of external Federal visitors holding PIV cards and enforces agency security policies to gain physical entry through the use of automated barriers to pre-designated common areas in NRC facilities. The NRC information type is currently categorized under OCIO-CS-PROS-2001, March 27, 2017 as "personal identity and authentication information and security management information".

- Criminal History (CH) system. The CH system is not interconnected with the ACCESS system, but by office policy it is included in the ACCESS FISMA boundary. The CH SECCAT Transmittal Package is at ML#16057A665, March 4, 2017.

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

- Title 5 United States Code Section 301, "Departmental Regulations"
- Federal Information Security Management Act (Pub. L. 107-296, Sec. 3544)
- E-Government Act of 2002 (Pub. L. 107-347)
- Paperwork Reduction Act of 1995 (44 USC 3501 et. al.)
- 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.
- Title 32 of the Code of Federal Regulations Parts 2001 and 2003, "Classified National Security Information," June 28, 2010.

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

- To ensure the safety and security of NRC personnel, contractors, federal PIV card holders and the general public.
- To allow logical access to authorized agency facilities, common areas and workspaces. To limit access to secure room workspaces by unauthorized personnel.
- To detect unauthorized activities or entry at NRC facilities.
- To monitor the safety and security of NRC employees, contractors, and visitors.

6. Points of Contact:

Business Project Manager	Office/Division/Branch	Telephone
Denis Brady	ADM/DFS/FSB	301-415-7056
Technical Project Manager	Office/Division/Branch	Telephone
John W. Garnsey	ADM/PMDA/ITT	301-415-7822
Executive Sponsor	Office/Division/Branch	Telephone
Cynthia Carpenter	ADM/FO	301-415-8747

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?

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

Approval Date: April 13, 2017, ML# 16077A027

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

This PIA includes system components identified in previous submissions. In 2017, NRC DFS will deploy a radio communications system that uses the agency network to support of the agency's safety and security mission. Additional modifications this fiscal year include deploying two automated Kiosks that authenticate the identity of federal visitors, and allows physical access to common office work spaces. Additionally, we anticipate the migration of the stand-alone NRC – OPM Fingerprint Transmission System into ACCESS-PCI subsystem.

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?

Collects information from Federal employees and contractors for the OCIO-ICAM system which it later accesses to generate and maintain HSPD-12 PIV cards. Note: The OCIO-ICAM system is outside the FISMA boundary of the ACCESS system.

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

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

NRC collects biographic and biometric information to (i) complete identity proofing and registration, (ii) create a PIV data record, and (iii) issue a PIV card. This information consists of: Name, date of birth, social security number (SSN),

organizational/employee affiliations, fingerprints, digital color photograph, work e-mail address, and phone numbers as well as additional verification and demographic information. Federal emergency response official status, results of a background check, PIV card issuance location, gender, race, country and city of birth.

The data used during lifecycle maintenance of PIV cards is stored in the OCIO Identity Credentialing & Access Management (ICAM) Authentication and Credentialing Services (ACS) SQL server that resides outside the FISMA boundary of ACCESS. ACCESS-PACS maintain information about the individual's name, cardholder unique identification (CHUID), PIV card number, clearance, access rights, and access history. The intrusion detection system maintains data about individuals IDS transactions (i.e. arming and disarming alarm panels). The IP CCTV maintains video recordings of general activities within NRC garages, entries and exits.

The hard copy fingerprint cards scanned for the processing of external NRC – OPM fingerprints will be maintained for a period of 30 days after which they are destroyed per agency directive. The records of federal visitor kiosk transactions with the federal certification authority will be maintained within the system.

c. Is information being collected from the subject individual? Yes.

To the greatest extent possible, collect information about an individual directly from the individual.

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

During PIV card enrollment, required data elements are collected directly from the individual for the ICAM system. The other components indirectly collect information from subject individuals.

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

Yes – contracted workforce.

(1) If yes, does the information collection have OMB approval?
Yes.

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

3206-0258 Questionnaire for Public Trust Positions (SF 85P)
3150-0049 NRC Form 136, Security Termination Statement
3150-0218 NRC Forms 850A, Request for NRC Contractor Building Access

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

Yes.

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

An individual's clearance or access authorization information is collected from the NRC Personnel Security Adjudication Tracking System (PSATS). An individual's personnel data (i.e. legal name, date of birth, etc.) are also confirmed in PSATS.

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

No.

(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?

The accuracy and completeness of the data is reviewed by key personnel at several stages. It is reviewed during the sponsorship process by representatives of the Office of the Chief Human Capital Officer (OCHCO). During the enrollment process and in the adjudication process by the NRC Personnel Security staff. The following technical controls also ensure the completeness of the data:

- Consistency and reasonableness checks
- Validation during data entry and processing
- Use of required fields to prevent critical data from being omitted

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

The data will be manually transcribed from the NRC Personnel Security Adjudication Tracking System (PSATS) and collected directly from PIV applicants, the individuals to whom a PIV card is issued.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

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

ACCESS-PACS maintain information on PIV card transactions, individual access rights, and access control alarm activity. The IDS component of ACCESS will maintain information about arming, disarming, alarm alerts, and signals. The IP CCTV component will maintain general video footage about individual activities occurring at NRC facilities in the form of digital video recording.

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

Internal card readers and access control devices will be the source of information maintained under ACCESS-PACS. Internal alarm panels and alarm points will be the source of information maintained under the IDS component of ACCESS. The IP CCTV network consisting of cameras and network video recorders additionally will be a source of information.

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.

- Create a record in the authentication & credentialing services (ACS) system. ACS is a component of the OCIO-ICAM information system, and not the ACCESS system. The data is used during the registration (enrollment) process to create the PIV applicant's enrollment record, manage and maintain this information throughout the PIV card lifecycle, and, verify, authenticate and revoke PIV cardholder access to federal resources. A unique identifier is assigned during registration and used to represent the individual's identity and associated attributes stored in the system.

- Complete the PIV identity proofing and registration process. (enrollment) The biographic information collected or confirmed as part of this process is used to establish the PIV applicant's identity. Biometric information is used to accurately authenticate a PIV applicant and to ensure he/she has not been previously enrolled in the PIV system. As part of this process, FIPS 201 requires that applicants provide two forms of identity source documents in an original form. The identity source documents must come from the list of acceptable documents included in Form I-9, Employment Eligibility Verification.

- Issue a PIV Card. Upon successful completion of the enrollment and background investigation process a PIV card is activated and generated.

Biometric information is used during PIV card issuance to verify PIV applicant identity and complete activation of the card. This provides much stronger security assurances than typical card activation protections such as a PIN and/or passwords. Once the individual has been issued a PIV card, the PIV Identity Database Management System is updated to reflect that the card has been issued.

- Authenticate and enforce physical access controls. To authenticate identity and allow or deny personnel including federal visitors' access to facilities when a PIV card is presented at a physical access controller (PACS) card reader. This reader uses a combination of the CHUID, PIV card status (active/suspended), associated access rights, and a PIN listed in an ACCESS SQL database to grant permission to enter facilities. The identity of federal visitors is authenticated by the federal certification authority that creates a temporary record in the PACS database that allows access to designated common work space. At each entry, security guards use a "swipe & show" workstation application to compare the PIV card against the cardholder to verify identity.

- Detect unauthorized entry at NRC facilities. To detect unauthorized entry into NRC facilities or restricted access areas. Alarm panels at sites throughout the facilities alert, or signal an alarm when unauthorized entry is detected.

- Assess alarms and suspected unauthorized activities. ACCESS IP CCTV network generates a video feed to monitors in the central alarm station that monitor general activities for suspected unauthorized activities occurring in garages, entries and exits.

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?

ACCESS administrators with defined roles/responsibilities are responsible for protecting the privacy rights of individuals and are required to sign the "notification of responsibilities regarding the use, disclosure, and protection of privacy act information" Information residing in ACCESS is protected under the agency Privacy Act Systems of Records: NRC-39 Personnel Security Files and Associated Records; NRC-40 Facility Security Access Control Records; and NRC-45 Digital Certificate for Personal Identity Verification Records.

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 Security Categorization Report for ACCESS documents the data elements used by the system. This report is an Official Agency Report (OAR) filed in ADAMS ML#16106A036, May 11, 2016.

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

Yes. I.e. the system derives new data by generating an individual's access history, compares it with an IDS alarm history and IP CCTV video recording history to derive if the individual has performed unauthorized access to the facility.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

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

The access control data is maintained in an application SQL database with a password and PIV card by the system administrators. The server is hosted behind the NRC data center firewall in a physically restricted workspace. IDS data is maintained in the restricted access Headquarters central alarm station (CAS) as well as the federal protective service (FPS) monitoring station. IP CCTV video is maintained on facility digital video recorders (DVR) or network video recorder (NVR). These recorders are password protected as well, reside behind the data center firewall, and are stored in restricted access telecommunications closets. This aggregate data will only be used to investigate alarms and unauthorized access at NRC facilities. The aggregate data will be protected in accordance with the Privacy Act Systems of Records NRC-40 "Facility Security Access Control Records."

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

Whenever possible the aggregate data from each system component will be validated against the data from other system components. For example, an individual's access history can be corroborated by their alarm or video history.

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

The ACCESS system is in compliance with organizational defined computer security controls. These controls are applied to "hardened" the system against unauthorized access, insider threat, compromise, or disaster. ACCESS complies with the NRC Information Security Policy & Oversight Branch (ISPOB) policies and procedures; and undergoes independent continuous monitoring assessment to secure the system. ACCESS complies with the Office of Chief Information Officer (OCIO) change management procedures to ensure that only authorized work is being performed on the system, following defined procedures by authorized personnel.

This data is restricted to only the system administrator and an alternate in the facilities security branch. These individuals have undergone rigorous background screening, and are trained in their administrator duties to secure the ACCESS system. Finally, ACCESS has a primary and alternate Information system security officer (ISSO) assigned to ensure that system security controls are operating as designed and intended.

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

Data in the PIV lifecycle component of ACCESS is stored in the ACS SQL server which is located outside the ACCESS system boundary. Data can be queried directly from the ACS SQL server or via a PIV creation workstation. Data can also be queried by name or CHUID from the ACCESS-PACS SQL database that is the underlying engine to the Facility Commander Wnx (FCWnx) application. Only authorized system administrators have access to these systems. Information can be used by the application that retrieves the information or can be printed as a paper copy.

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

Yes.

a. If yes, explain.

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

Facilities and equipment are secured by limiting physical access to the workspace and system, and by requiring an appropriate verification of identity for logical access to the system.

Encryption technologies are used during the electronic transfer of information to ensure unauthorized monitoring does not occur, and that

data is sent only to its intended destination and to an authorized user, by an authorized user.

A “least privilege” role-based access system restricts access to data on a “need to know” basis. System/application users have varying levels of responsibility and are only allowed to access information and features of the system appropriate for their level of job responsibility and security clearance. Only a select few administrative and privileged users will have access to all the aggregate data in the system, and these individuals undergo a rigorous background screening process. The access for these trusted personnel are reviewed on an annual basis. Access is revoked for personnel who no longer require system access.

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

- Statistical reports (# PIV cards issued, #PIV cards schedule to expire, # PIV card holders per region)
- Credential history reports
- Alarm history reports
- Operator history reports
- Device reports (# of card readers, # of alarm points, etc.)

a. What are the reports used for?

- To report NRC compliance with federal standards
- To investigate malfunctioning equipment
- To investigate unauthorized access or activity.

b. Who has access to these reports?

A “least-privilege” role based access system restricts access to data on a “need to know” basis. System/application users have varying levels of responsibility and are only allowed to access information and features of the system appropriate for their level of job responsibility and security clearance. Only a select few system administrators and privileged users will have access to all the aggregate data in the system, and these individuals undergo a rigorous personnel security screening process. Access is revoked for personnel no longer requiring access to the system.

D. ACCESS TO DATA

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

- Office of Administration, Division of Facilities and Security
- Office of Chief Information Officer, Operations Division
- Region I, Division of Resource Management
- Region II, Division of Resource Management and Administration
- Region III, Division of Resource Management and Administration
- Region IV, Division of Resource Management and Administration
- Office of the Chief Human Capital Officer, Technical Training Center

(1) For what purpose?

The Office of Administration, Division of Facilities and Security (ADM/DFS) has access to data from all four components of ACCESS as ADM/DFS is responsible for the physical security of NRC personnel, properties, information and assets.

The Office of Chief Information Officer, Operations Division (OCIO/OD) has access to data from the PIV lifecycle component of ACCESS as the information resides with the Authentication and Credentialing Services (ACS) system boundary, which is owned by OCIO-OD.

Region I Division of Resource Management (RI/DRM), Region II Division of Resource Management and Administration (RII/DRMA), Region III Division of Resource Management and Administration (RIII/DRMA), Region IV, Division of Resource Management and Administration (RIV/DRMA), and Office of the Chief Human Capital Officer, Technical Training Center (TTC) have limited access to the data from all components of ACCESS that reside at their respective facility.

(2) Will access be limited?

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).

The Identity Credentialing and Access Management (ICAM) Authentication and Credentialing Services (ACS) system will have an electronic connector to the PACS global SQL server. Data from ACS will be transmitted via the electronic connector to the PACS global server to automatically provision and deprovision PIV applicants for access to NRC facilities.

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

Using encryption and private network.

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

No.

(1) If yes, who? N/A.

(2) Will access be limited? N/A

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

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

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 ?

No, General Records Schedule 18 – Security and Protective Service Records does not address those records maintained by ACCESS.

a. 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?

b. 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.

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

The retention requirements are a minimum of five years from the date when the individual moves from an active to inactive status (month of separation).

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

Yes. The Office of Inspector General (OIG) may use the records for investigative purposes.

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?

New data is continually being added to the PIV lifecycle component of the system as new personnel enter service with the agency. New data is continually being added to the remaining system components as daily PACS transactions, IDS activity, and video is automatically logged. Data is updated in the PIV lifecycle, PACS, and IDS components of ACCESS as user information changes (i.e. Name changes, change in location, clearance upgrade/downgrade, etc.)

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?

Old data is removed from the PIV lifecycle component of the system as personnel separate from the agency. The DVRs, NVRs are the only system components that write over the archived recordings after approximately 30 calendar days.

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?

No.

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

Yes. Old data is removed from the ACCESS-PCI lifecycle component of the system as personnel separate from the agency.

F. TECHNICAL ACCESS AND SECURITY

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

The user PIV authentication, along with role-based access controls (RBAC) and application level passwords ensure that only program authorized personnel have permission to access just the data needed to perform their duties. The system information infrastructure is secured from unauthorized access by a network segmentation that allows only authorized and authenticated devices to exchange data. The system administrator on a daily basis monitors the system for unauthorized and or suspicious activities. The network administrator monitors for intrusions, and suspicious activities occurring within the secured systems infrastructure. Before data can be

retrieved, a user must positively and uniquely authenticate to the NRC Domain and subsequently to the specific ACCESS component.

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

All system transactions are tied to a specific, unique individual by strict identification and authentication protocols, and there are audit trails that document all activities performed by users.

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

Yes.

(1)If yes, where?

The procedures, controls and responsibilities regarding access to the system are detailed in the NRC PIV Card Issuance (PCI) Operations plan, the ACCESS system policies and procedures (SPP) document, February 2, 2017, ML17038A438, and the FY17 Q^3 ACCESS System Security Plan (SSP) February 15, 2017, ML17046A186. All documents are maintained, reviewed on an annual basis and declared an official agency record (OAR) in ADAMS.

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

Yes.

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

A fixed number of users in each region will be authorized access to perform duties and will have the same restricted roles in the system for their respective facility.

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

Access to the data is strictly controlled, and is limited to those with an operational need to access the information. There are two core sets of user population:

1) Federal employees and contractors with full administrative responsibilities in the PACS, IDS and IP CCTV system (i.e. System Administrator and designated alternate personnel).
2) Federal employees and contractors with restricted facility specific responsibilities in the PACS, IDS, and IP CCTV system.
3) Federal contractors (security officers) with the ability to view and acknowledge transactions in the PACS, IDS, and IP CCTV system.

4) Federal employees and contractors who are provided access to the PIV lifecycle workstations and its applications (e.g. sponsors, registrars, adjudicators, and issuers).

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

Yes.

a. If yes, what will be collected?

All operator transactions are logged within the system. Audit logs are generated for all transactions, and security events.

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

Yes.

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

All ACCESS components have role-based restrictions, and individuals with access privileges have undergone personnel security vetting, suitability screening. These users undergo mandatory user awareness, role based cybersecurity and PII training related to their specific role on the information system. Data is safeguarded in transmission using encryption and access controlled private virtual networks. NRC conducts log and cybersecurity audits on the system, it procedures and processes. The system administrator receives access audit logs each day.

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

Yes.

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

The system certification and accreditation last took place in April 2014.

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

System Name: Automated Access Control and Computer Enhanced Security System (ACCESS)

Submitting Office: Office of Administration (ADM)

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
This system contains PII. The records in this system are protected by the provisions of the Privacy Act. This system will operate under NRC Privacy Act systems of records NRC-40, "Facility Security Access Controls Records," and NRC-45, "Digital Certificates for Personal Identity Verification Records."

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	6/28/2017

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

__X__ Currently has OMB Clearance. Clearance No. 3206-0258, 3150-0049, and 3150-0218

Comments:

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	6/27/2017

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

__X__ Needs to be scheduled.

____ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:
This system will need to be scheduled; therefore, NRC records personnel will need to work with both ADM and NARA to develop a records retention and disposition schedule for records created or maintained using ACCESS and/or entered in ADAMS. 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, 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	6/28/2017

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 June 29, 2017

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

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Cynthia Carpenter, Director, Office of Administration (ADM)**	
Name of System: **Automated Access Control and Computer Enhanced Security System (ACCESS)**	
Date ISB received PIA for review: **June 22, 2017**	Date ISB completed PIA review: **June 28, 2017**
Noted Issues:	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ June 29, 2017**
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*	