ADAMS ML20161A187

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.

Access Denial Record (ADR)

Date: June 9, 2020

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Access Denial Record is located on the office of Administration's (ADM) SharePoint site, internal to the Nuclear Regulatory Commission (NRC) and tracks Information about NRC employees, contractors and visitors regarding denial of access to NRC facilities as a result of COVID-19 screening. This information is used only internally.

2. What agency function does it support?

Due to COVID19, to support the chairman by providing data on how many staff are being turned away and to determine how long the agency should continue screening. Also, to support OCHCO in the event that someone files a grievance in reference to access denial.

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

Not applicable.

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

Not applicable.

What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.

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

The chairman needs to have data on how many staff are being turned away in order to determine how long contact screening should continue.

OCHCO would like to have a record of staff that are turned away in the event that they file a grievance.

6. Points of Contact:

Name	Role	Office/Division/Branch	Telephone
Denis Brady	Business Project Manager	ADM/DFS/FSB	301-415-5768
Tamar Katz	IT Specialist; ACCESS ISSO	ADM/PMDA/ITT	301-415-2500
Jennifer Golder	Executive Sponsor	ADM	301-415-0741

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

a. ____ New System

____ Modify Existing System

_X_ Other Data stored in a SharePoint list

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

Not Applicable

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

N/A

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

N/A

8. **Do you have an NRC system Enterprise Architecture (EA)/Inventory number?**

   Yes

   a. **If yes, please provide Enterprise Architecture (EA)/Inventory.**

      20200053

   b. **If, no, please contact EA Service Desk to get Enterprise Architecture (EA)/Inventory number.**

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 (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).**

      Information about NRC employees, contractors, and visitors regarding denial of access to NRC facilities as a result of COVID-19 screening

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

   b. **What information is being maintained in the system about an individual (be specific – e.g. SSN, Place of Birth, Name, Address)?**

      Information includes name, email, badge number, date, time and location of screening, screening question responses and temperature at time of screening.

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?

Information includes name, email, badge number, date, time and location of screening, screening question responses and temperature at time of screening.

d. Will the information be collected from individuals who are not Federal employees?

Yes

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

Not Needed.

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

N/A

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

No

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

N/A

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 ADR relies on the operators of the system to verify the accuracy or completeness of the information that the system retains.

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

The information is collected via SharePoint list.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

No

(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 NRC will use the information as documentation as to when, where and why an individual was denied access to the facility.

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 ADR system relies on the operators of the system to verify the accuracy or completeness of the information that the system retains. They sign a "notification of responsibilities regarding the use, disclosure, and protection of privacy act information."

The information is protected under Privacy Act Systems of Records Notice (SORN) - NRC 40, Facility Security Access Control Records

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

The data elements are available in the settings of the SharePoint list.

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

N/A

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

No

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?

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 (name, unique number or symbol)? (Be specific.)

Information will be retrieved by employee name and or Email

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Information about individuals will be retrievable by personal identifier in the system.

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes

a. If "Yes," provide name of SORN and location in the Federal Register.

Privacy Act Systems of Records - NRC-40, Facility Security Access Control Records

8. If the information system is being modified, will the SORN(s) require amendment or revision?

No

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

No

a. If yes, explain.

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

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

List of individuals denied access

a. What are the reports used for?

Provide documentation of those denied access to the facility

b. Who has access to these reports?

Access to the reports in the ADR is limited to authorized users. Persons must have a need-to-know to become authorized users and they can only access reports appropriate for their job responsibility. They undergo a rigorous background screening process and their need- to-know and access privileges are reviewed annually.

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
- 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
- Technical Training Center, Division of Resource Management and Administration

(1) For what purpose?

Due to COVID19, to support the chairman by providing data on how many staff are being turned away and to determine how long the agency should continue screening. Also, to support OCHCO in the event that someone files a grievance in reference to access denial.

(2) Will access be limited?

Yes

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

No

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

N/A

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

N/A

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 AND INFORMATION MANAGEMENT (RIM) - 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 NARA statutes (44 U.S.C., 36 CFR). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management (RIM) and NARA's Universal

Electronic Records Management (ERM) requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule(NUREG-0910), or NARA's General Records Schedules?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).

See GRS Schedule 5.6 Item 090 and table below which will be used for the retention of the information. If information does not fall into the items listed in GRS 5.6, then data 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.

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

Records	Citation	Temporary/ Permanent	Disposition Instructions	Notes/Comments
Security Records	GRS 5.6 item 090	T	Records of routine security operations. Records about detecting potential security risks, threats, or prohibited items carried onto Federal property or impacting assets, including records documenting access control, screening, patrol and response, and control center operations. Temporary: Destroy when 30 days old, but longer retention is authorized if required for business use.	BASED ON NRC SORN 40 NARA Schedule: DAA-GRS 2017-0006-0012

b. If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

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

Access to information will be restricted using SharePoint permissions

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 person's identity by strict identification and authentication protocols. Access will be controlled by the use of SharePoint permissions. The information will not be accessible by unauthorized users.

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

Yes

(1) If yes, where?

It is part of the SharePoint security infrastructure.

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

Yes. Designated ADM users may access SharePoint remotely via the NRC VPN or Citrix environments.

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

All persons in the same role, go through the same training, sign the same agreements, have the same access restrictions, and are subject to the same oversight independent of their physical location. Users are required to adhere to NRC's policies for computer use.

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

Access to the data is strictly controlled and limited to those with an operational

need to access the information. This is controlled through SharePoint provided access permissions.

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

Yes

a. If yes, what will be collected?

The Versioning feature in SharePoint will capture the user and timestamp associated with any changes and will list values of modified fields.

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

No

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?

SharePoint permissions will ensure that only approved users have access to the data. The Versioning feature in SharePoint will capture the user and timestamp associated with any changes and will list values of modified fields.

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

Yes

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

Since ADR is stored in SharePoint and SharePoint is accredited please refer to the FISMA boundary that NRC SharePoint resides.

ADAMS ML20161A187

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

System Name: Access Denial Record (ADR)

Submitting Office: ADM

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
The information is protected under Privacy Act Systems of Records Notice (SORN) - NRC 40, Facility Security Access Control Records

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	6/11/2020

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:
No OMB clearance is required but the information being collected from NRC staff and contractors is related to their regular duties. For non-Federal visitors, the information collection meets the exemption criteria in 5 CFR 1520.3(h)(1) and (3).

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	6/9/2020

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

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

Comments:

See GRS Schedule 5.6 Item 090 which will be used for the retention of the information. If information does not fall into the items listed in GRS 5.6, then data 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	06/09/2020

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 11, 2020

Clarissa L. Evans Brown, Chief
Computer Security Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Jennifer Golder, ADM**	
Name of System: **Access Denial Record (ADR)**	
Date CSB received PIA for review: **June 9, 2020**	Date CSB completed PIA review: **June 11, 2020**
Noted Issues:	
Clarissa L. Evans Brown, Chief Computer Security Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ June 11, 2020**
Copies of this PIA will be provided to: *Tom Ashley, 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*	