

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.

Please do not enter the PIA document into ADAMS. An ADAMS accession number will be assigned through the e-Concurrence system which will be handled by the Privacy Team.

Reactor Program System

Date: May 17, 2022

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The NRC's Reactor Program System (RPS) is an enterprise workload management platform that supports the effective execution of business processes associated with the reactor inspections and licensing programs. RPS was designed to provide a planning, scheduling, reporting, and analysis tool for inspection activities at nuclear power reactor and fuel facilities in the United States (U.S.). This system is used to implement the policy and inspection guidance for programs assigned to the NRC regional offices and assesses the effectiveness and uniformity of the implementation of those programs through detailed reporting processes.

The RPS is administered by the Office of Nuclear Reactor Regulation (NRR) and users include NRR, the Office of Nuclear Material Safety and Safeguards (NMSS), the Office of Nuclear Security and Incident Response (NSIR), the Office of Nuclear Regulatory Research (RES), the Office of Enforcement (OE), the Office of the Chief Information Officer (OCIO), and NRC Regional offices.

2. What agency function does it support?

RPS supports the following functions associated with the reactor inspections and licensing programs:

- track licensing of reactor operators,
- plan, schedule, and track power and research test reactors' inspections,
- plan and track workload for facility licensing activities,
- allows NRC staff and contractors to manage the Reactor Oversight Process, including Human Factors,
- monitors operational experience and manage operational workload,
- allows NRC staff and contractors to review and publish event status reports.

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

The modules of RPS are as follows:

- RPS - Inspection Scheduling and Tracking (Inspections) and Inspections Reporting tool (ISTAR) – *Manages all the scheduling and tracking for inspection activities and findings; generates inspection reports.*
- RPS - Licensing/Workload Management (LWM) – *Manages and tracks reactor licenses, milestones, and workload review process; assigns reviewers to projects; generates LWM reports.*
- RPS - Oversight – *Manages and tracks safety and security performance assessments.*
- RPS - Operator License (OL) – *Manages and tracks updates for operator licensing activities and licenses.*
- RPS - Reactor Oversight Process (ROP) – *Manages data from all RPS modules and makes the appropriate information available for the public webpage.*
- Read - only RPS – Allow limited access to Inspections and Licensing.

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

United States Code, 2006 Edition, Supplement 4, Title 42 - THE PUBLIC HEALTH AND WELFARE – 42 U.S.C. 2201(d), 2201(p) (1996) and 42 U.S.C. 2137 and 2201(i) (1996).

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

RPS includes inspection and licensing information, plant performance indicators, inspection follow-up items, safety issue data, NRC staff data, facility characteristics, and other reactor regulatory data which is used to support the following functions:

- Manage all the scheduling and tracking for inspection activities and findings.
- Manage and track reactor licenses, milestones, and workload review process.
- Manage and track safety and security performance assessments.
- Manage and track updates for operator licensing activities and licenses.
- Generate events status reports.

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

Project Manager	Office/Division/Branch	Telephone
Victor Kochuba	OCIO/SDOD/ADSB/PAT	301-415-6270
Business Project Manager	Office/Division/Branch	Telephone
Ikeda Betts	NRR/DRO/IOLB	301-415-1959
Andy Imboden	NRR/DORL/LPMB	301-287-9055
Manuel Crespo	NRR/DRO/IRIB	301-415-0298
Jason Carneal	NRR/DRO/IOEB	301-415-1451
Dan Merzke	NRR/DRO/IRAB	301-415-1457
Backup Technical Project Manager	Office/Division/Branch	Telephone
Jordon Alston / Melissa Ash	OCIO/SDOD/ADSB/PAT	301-415-4085 301-415-7251
Executive Sponsor	Office/Division/Branch	Telephone
Andrea Veil, Director	NRR	301-415-1270
ISSO	Office/Division/Branch	Telephone
Consuella Debnam (Primary)	OCIO/GEMSD/CSB/IAT	301-287-0834
Luc Phoung (Alternate)	OCIO/GEMSD/CSB/IAT	301-415-1103
System Owner/User	Office/Division/Branch	Telephone
Tom Ashley, Director	Information Technology Services Development and Operations Division	301-415-0771

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
 Other

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

Yes.

- (1) **If yes, provide the date approved and the Agencywide Documents Access and Management System (ADAMS) accession number.**

ML19260E480.

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

The RPS instance currently hosted and operating in a steady state in the NRC Data Center owned by NRR and is in the continuous authorization state within the Business Application Support Services (BASS) FISMA boundary. RPS' host machines in the Three White Flint North (3WFN) NRC Data Center will be decommissioned once it is fully stood up and authorized for use in the Information Technology Infrastructure (ITI) Azure Cloud Services (ACS) US East 2 region. (Expected go-live date is July 2022).

Please note that no change will be made to the RPS system data as part of this re-hosting effort that effects or creates new privacy risks.

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

Yes.

- a. **If yes, please provide the EA/Inventory number.**

20150003.

- b. **If, no, please contact [EA Service Desk](#) to get the 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.)).**

Federal employees, Federal Contractors, Reactor Operator Candidates and Operator Licensees.

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

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

To track licensing of reactor operators, the RPS OL module maintains applicants/operators name, date of birth, home address, citizenship, education, employment history, medical information, employer name and address, examination test scores, license type, fitness for duty and violations information.

The RPS Licensing module database maintains information on licensee name, licensee business address, email, phone number, license number, NRC employee id, employee LanID, employee name, role id, role name, office/division/branch information.

The RPS Inspection module database maintains information on licensee name, address, email address, reactor point of contact (PoC) name, email, phone, address, NRC employee (Enterprise Project Identifier (EPID) requestor, approver, etc.) LanID, office, division, and branch.

RPS is an internally facing system. It receives Operator License (OL) data, EPID and Cost Activity Code System (CACs), staff assignment time, and cost account code (CAC) from operator digitized docket (ODD) and CACS through database views, application program interfaces (API), and file transfers. RPS receives, docket, organizational, employee and contractor data from the Enterprise Data Management System (EDMS).

c. **Is information being collected from the subject individual? (To the greatest extent possible, collect information about an individual directly from the individual.)**

Yes.

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

Information being collected is name, home address, birth date, citizenship, education, employment history, medical information, and employer name and address, examination test scores, license type, fitness for duty and violations information.

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

Yes.

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

Yes.

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

3150-0090 (NRC Form 398); 0024 (NRC Form 396) with additional information covered by 3150-0018 (10 CFR Part 55).

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.

The candidate/operator provides information to the NRC that has been certified by an authorized representative of the facility licensee as required by 10 CFR Part 55 on NRC Form 398 (10 CFR Part 55.31(4) "Personal Qualification Statement-Licensee," and NRC Form 396 (10 CFR 55.23) "Certification of Medical Examination."

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

Yes.

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

The facility and the employee together supply the requested information as named in question 1c (1) above. The employee and the facility managers must certify as to the accuracy of the information.

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

Collected information is certified by facility management before it is submitted. The information is verified during the business processes associated with the reactor inspections and licensing programs, which is conducted by the Office of Nuclear Reactor Regulation (NRR), the Office of Nuclear Material Safety and Safeguards (NMSS), the Office of Nuclear Security and Incident Response (NSIR), and NRC Regional offices.

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

Operator licensing information is collected by hard copy or electronically transferred forms and letters. And through database views, web application programming interface (API) and database access.

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).

Planning, scheduling, inspecting, and reporting for facility licensees is maintained by the system.

Workload records related to licensing and inspecting facility licensees are also maintained.

Organization data, EPID & CAC/Staff Assignment data.

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

Facility licensee licensing and inspection activity is a workload plan developed internally by staff and entered into RPS.

It receives EPID and CACS/staff assignment time and cost account code (CAC) from operator digitized docket (ODD) and CACS through database views, application program interfaces (API), and file transfers.

RPS receives docket and organizational data from the Enterprise Data Management System (EDMS).

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 RPS modules data is used to:

- Manage all the scheduling and tracking for inspection activities and findings.
- Manage and track reactor licenses, milestones, and workload review processes.
- Manage and track safety and security performance assessments.
- Manage and track updates for operator licensing activities and licenses.
- Generate events status reports such as operator licensing status reports, inspection reports, safety evaluation reports, and performance/action matrix reports.

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 control for RPS components is administered by Active Directory (AD) at the OS level to manage user access to shared resources.

RPS employs an access control mechanism that regulates access to content based on the user's role and the permissions associated with that role (e.g., such as view, create, or modify).

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 data elements are documented in the "Prod DD_CombinedDS Current.xlsx" spreadsheet which represents the current view of the RPS database and is located in the Confluence File list called "RRPS Technical Artifacts" (<https://confluence.edte.nrc.gov/x/2AAzBg>). Confluence is part of the Application Lifestyle Management (ALM) toolset.

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

No, the derived or aggregation of data occurs outside of the system.

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.)

The end users consume inspections, licensing, OL, ROP, etc. data to support the business processes associated with the reactor inspections and licensing programs by connecting to the RPS via secure web server through the HTTPS port 443.

The Reactor Program Application Suite (RPAS) Data Warehouse connects to RPS via SQL server connection (TCP/IP port 1433) to pull operator licensing, licensing, inspections, and oversight data.

Licensing project data is pulled from RPS into the MAP-X Web-based Relief Request (WRR) data via RPS applications, and changes made within the interface are then reflected across the RPS database.

Yes.

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

Operator licensing records are retrieved by name and docket number. All other records are retrieved by name, docket, or report number.

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.**

System NRC-16 “Facility Operator Licensees Record Files (10 CFR Part 55),” republished in the Federal Register Vol. 81, No. 222 on Thursday, November 17, 2016.

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.**

N/A.

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

N/A.

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

The following reports may be produced, but not limited to:

Inspections -

- CAC to IP Crosswalk
- EPID Request List
- Examination FTE Estimates
- Examiner On-Site and Training Commitments
- Inactive Inspection Procedures
- Individual Examiner Schedules
- IP 1 Site Activity Timeline
- IP 10 Examiner Availability
- IP 10 Staff Assignment CAC Errors
- IP 21(A) OLES
- IP 21 Operator Licensing Exam Schedule
- IP 22 Site Inspection Activity Plan
- IP 22A Inspection Activity Table for Export to Spreadsheet for Data Analysis
- IP 22B Detailed Site Inspection Activity
- IP 24 Security Activity Plan Report
- IP 28 Inspection Procedure Analysis
- IP 29 Procedure Scope Sample Ghost Text

- IP 4 Outage_INPO Activity Timeline
- IP 5 Team Inspection Timeline
- IP 7A Organization Schedule (8.5X11)
- IP 7B Organization Schedule (11X17)
- IP 9 Vendor Inspection Schedule
- IPAS 1 Change Notice Report
- IPAS 2 List Manuel Chapters
- IPAS 3 List Procedures
- IPAS 8-9 IP-MC History
- IR 1 Item List
- IR 10 ROP Sample Completion by Inspection Report
- IR 10B Previous Completed Samples
- IR 11 Inspection Report-EPID Tracking
- IR 12 Cross Cutting Aspect
- IR 13 Inspection Activity Type Hours Distribution per EPID
- IR 2 Item List Advanced Search
- IR 3 PIM
- IR 4 Advanced Findings Violations Search
- IR 5 Inspection Performance Hours Charged
- IR 5A Inspection Performance Samples Completed
- IR 5B Inspection Performance Samples Completed at Procedure Level
- IR 6 ROP Sample Completion Hours Charged – Min Nom Max
- IR 7 Overview of Hours Charged
- IR 8 Baseline Inspection Completion
- IR 8A Baseline Inspection Completion by Site
- IR 9 TI Completion
- IRTS 1 Currently Overdue Inspection Reports by Organization
- IRTS 2 Issued Report
- IRTS 3 List of Inspection Reports
- IRTS 4 Inspection Reports Due – no ML Number
- Samples Tied to Inactive IPs
- Scheduled Inspections Linked to Inactive Organizations
- Staff Assignment List
- TABLES 3 Staff in Office
- TABLES 4 Docket List

Licensing -

- Assignment Tally Report
- Branch Chief List
- Completed RAIs
- DMLR Assignment Tally Report
- DMLR Completed Acceptance Reviews
- DMLR Completed RAIs
- DMLR Milestone Validation Dashboard
- DMLR Open Acceptance Reviews

- DMLR Open RAI Requests
- DMLR Project Hours
- DMLR Status of License Renewal and Subsequent License Renewals Applications- Environmental Review
- DMLR Status of License Renewal and Subsequent License Renewals Applications- Safety Review
- DMLR Technical Division Input Status
- Decommission Report
- Employee List
- Generic Communication Projects
- Milestone Change History
- Milestone Validation Dashboard
- Office Project Hours
- Open Acceptance Reviews – new TAM
- Open Inventory by Activity Type
- Open QPR Schedule Metrics
- Open QPR Schedule Metrics X
- Open RAI Requests
- PM Project Prioritization
- Process and Milestones
- Project Hours Report
- Project Hours Report XX
- Project Hours Title EPID Search
- Project Wildcard Search
- QPR Schedule Metrics
- QPR Schedule Metrics X
- RB Competed RAIs
- RB Completed RAIs 1
- RB Completed RAIs 2
- RB Completed RAIs 3
- RB Open RAI Requests
- RB Open RAI Requests 1
- Reviewer Milestone Status Report
- Reviewer Project Prioritization
- Technical Division Open Inventory
- Technical Reviewer Branch Hours
- Technical Reviewer Milestone Status
- CAC Employee Labor Report
- Legacy Employee Labor Report
- Licensing Dashboards

RPS- OL-

- 01- Formatted Print of the Master File
- 02- Examination of Grade Average
- 03- Activity

- 04- Exam Information
- 06a- Activity Status-Examination Results
- 06b- Activity Status-Licensing Actions
- 09- Active Operators Count
- 10- Active Applications
- 11- Licenses Due Within 60 Days
- 12- RO and SRO Summary
- 13- 3 Month 6 Month 1 Year Restriction
- 14- License Restriction
- 16- Number of Anticipated Renewals
- 18- Proposed Denial Appeal Status
- 19- Waiver Tracking
- 21- Formatted Print of GFEs File
- 22- Expired Licenses
- 25- Fitness for Duty
- 26- Amended Licenses Tracking
- Batch License Certificates
- Batch License Letter

Oversight-

- Daily Event Notification Report
- Event Notification
- HFIS Detailed Report
- IR 12 Cross Cutting Aspect
- IR 4 Advanced Findings Violations Search
- IR_LER Details by Docket
- Power Reactor Status
- SCRAM

a. What are the reports used for?

The reports are used for tracking licensing of operators, planning, scheduling, reporting, and analyzing inspection and facility licensing activities at nuclear power and research and test reactor facilities in the United States. They are used to monitor implementation of the policy and inspection guidance for programs assigned to the NRC headquarters and regional offices, and to assess the effectiveness and uniformity of agency-wide implementation of those programs.

b. Who has access to these reports?

Only Authorized users of RPS have access to the reports. Access to RPS accounts is granted on a need-to-know basis and is based on defined roles and responsibilities using the principle of least privilege.

D. ACCESS TO DATA

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

Office of Nuclear Reactor Regulation (NRR), Office of Nuclear Material Safety and Safeguards (NMSS), Office of Nuclear Security and Incident Response (NSIR), Region I, Region II, Region III, and Region IV. NMSS is included for ISFSI/Fuel Cycle and NSIR for security inspections.

Operator licensing data, access is limited to NRR and Regional Operator Licensing staff only.

The RPS Workload management data access is defined by system roles.

The Office of the Chief Information Officer (OCIO's) Reactor Program Application Suite (RPAS) Data Warehouse connects to RPS to pull operator licensing, licensing, inspections, and oversight data.

(1) For what purpose?

The NRC office(s) access the RPS data to:

- Manage all the scheduling and tracking for inspection activities and findings.
- Manage and track reactor licenses, milestones, and workload review processes.
- Manage and track safety and security performance assessments.
- Manage and track updates for operator licensing activities and licenses.
- Generate events status reports such as operator licensing status, inspection reports, safety evaluation reports, and performance/action matrix reports.

(2) Will access be limited?

Only Authorized users of RPS have access to the reports. Access to RPS accounts is granted on a need-to-know basis and is based on defined roles and responsibilities using the principle of least privilege.

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).

Enterprise Data Management System (EDMS), CACS, Agencywide Document Access and Management System (ADAMS), Operator Digitized Dockets (ODD), Headquarters Operations Officer Database (HOO), RPAS Datawarehouse (DW), and Mission Analytics Portal (MAP-X) Web-based Relief Request (WRR).

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

RPS pulls docket, employee, and organization data from EDMS via an Application Programming Interface (API). RPS pulls EPID and CAC/Staff Assignment data from CACS via API.

RPS pulls inspections and licensing accession numbers and meta data from ADAMS via database views. RPS pulls operator licensing data from ODD via API.

RPS pulls event notification (EN)/ license event reports (LER) data and part 21 creation data from HOO via a flat file drop.

The Reactor Program Application Suite (RPAS) Data Warehouse connects to RPS via SQL server connection (TCP/IP port 1433) to pull operator licensing, licensing, inspections and oversight data.

Licensing project data is pulled from RPS into the MAP-X Web-based Relief Request (WRR) data via RPS applications, and changes made within the interface are then reflected across the RPS database.

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 United States Code (U.S.C.), 36 Code of Federation Regulations (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 and NARA's Universal Electronic Records Management 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 \(GRS\)](#)?

Yes.

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

RPS retention schedule, N1-431-08-18, ML092390130.

GRS 5.2: 020 Intermediary Records (DAA-GRS-2017-0003-0002) - Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

10 CFR Part 55 Docket Files - NUREG 0910 2.18.6.a – Temporary. Cut off files upon latest license expiration/revocation/termination, application denial or withdrawal, or issuance of denial letter. Destroy when 10 years old.

Examination Package - NUREG 0910 2.18.6.b – Temporary. Cut off file upon receipt of the facility's next exam. Destroy 4 years after cutoff.

General Correspondence - NUREG 0910 2.18.6.c – Cut off at close of fiscal year. Destroy 10 years after cutoff.

If identified, any additional information/data/records kept in this system may 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 not otherwise noted. 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.

b. If no, please contact the [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 control for RPS components is administered by Active Directory (AD) at the OS level to manage user access to shared resources. All RPS users must use their PIV card to logon to their workstation prior to connecting to RPS servers. RPS relies on ITI to manage hardware token-based authentication. Access authorization is limited by user roles.

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

The security controls recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, are applied to RPS to prevent the misuse of information. Access to specific information is restricted to only individuals and/or user groups who have a need to know and have authorized access.

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

Yes.

- (1) If yes, where?**

Details of access authorization are described in the BASS RPS Subsystem Security Plan.

- 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?**

RPS is currently operational at the NRC data center in Rockville, MD and is supported by a failover backup center in Region IV.

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

As of January 2021, RPS has a new Read-Only role that allows any NRC active employee LAN ID to access all the modules. This Read-Only role only provides browsing and limited access at a very high level. For detailed access and additional functionality, each module provides additional roles as described below:

There are 3 privileged groups at the operating system level:

- RPS Remote Desktop Users,

- RPS Administrators,
- RPS APPadmins.

There are 5 roles within the RPS-OL module of the application:

- OLA (Operator Licensing Assistant)-Has permissions to view all dockets in RPS-OL and edit any dockets in their region.
- Branch Chief- Has permissions to generate and be connected to letters. Also has permissions to view RPS-OL.
- Administrator- Has permissions to view and edit all dockets in RPS-OL and manage users.
- Examiner- Has permissions to view only in RPS-OL.
- Viewer- Has permissions to view only in RPS-OL.

There are 5 roles within the RPS-Licensing module of the application:

- Project Manager – Has permissions to generate and edit projects in their branch. Also has view only permissions to all other projects.
- Branch Chief – Has permissions to designate staff to projects that they have been assigned to. Also has view only permissions to all other projects.
- Technical Reviewer – Has permissions to comment and edit milestones for projects that they have been assigned to. Also has view only permissions to all other projects.
- Administrator – Has permissions to create, view, and edit all projects in the system. Also has the ability to create and change user roles.
- Escalation Executive – Has view only permissions to all projects.

There are no temporary or emergency accounts for RPS. Additionally, there are no shared or local accounts.

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

Yes.

a. If yes, what will be collected?

RPS relies on Active Directory GPOs (default domain policy) to record certain auditable events at the operating system level. An event in the Windows Security log is either type Success or type Failure. At the RPS operating system level, the following events are recorded in the local policies:

- Audit account logon events: Success, Failure.
- Audit account management: Success, Failure.
- Audit directory service access: Failure.
- Audit logon events: Success, Failure.
- Audit object access: Failure.
- Audit policy change: Success, Failure.
- Audit privilege use: Failure.
- Audit system events: Success, Failure.

In addition, the RPS system administrator has configured the following additional auditable events:

- Security System Extension: Success and Failure.
- System Integrity: Success and Failure.
- IPsec Driver: Success and Failure.
- Other System Events: Success and Failure.
- Security State Change: Success and Failure.
- Account Lockout: Success.
- Special Logon: Success.
- Network Policy Server: Success and Failure.
- File System Object Access: Failure.
- Registry Access: Failure.

The RPS application maintains all event logging data within the database. All updates to any of RPS's tables are logged. Any time a record is inserted, updated, or deleted; a log record is created that stores all of the field values for that record. Logs are not accessible through the RPS application interface, but standard reports can be created using the RPS Business Intelligence (BI) tool. Additionally, all log data can be queried directly by system administrators. Audit logs for RPS are captured by ITI's Splunk.

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 Personally Identifiable Information (PII) contract clauses are inserted in their contracts.

- *Federal Acquisition Regulation (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?

The RPS application audit mechanism captures end users and application administrators access to the application. Splunk is in place in the NRC data center for auditing purposes.

The RPS application implements role-based authentication, granting access to users based on their assigned roles. All RPS servers have host-based intrusion prevention software, anti-virus software and appropriate firewalls installed and configured. Network protections include layered firewall design that implements rule sets to deny all and permit by exception. The security controls recommended by NIST SP 800-53 are implemented in RPS to prevent misuse of the data.

9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed? And what FISMA system is this part of?

FY19 Q3 Periodic System Cybersecurity Assessment (PSCA) Report on May 13, 2019. This PSCA was for Public Meeting Feedback System (PMFS), Drupal Web Content Management System (DWCMS), Replacement Reactor Program System (RRPS), and Office of Inspector General Management Information System (OIGMIS).

b. If no, is the Certification and Accreditation in progress and what is the expected completion date? And what FISMA system is this planned to be a part of?

N/A.

c. If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.

N/A.

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

System Name: Reactor Program System

Submitting Office: OCIO

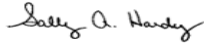
A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

Covered by NRC -16, Facility Operator Licensees Record Files (10 CFR Part 55).

Reviewer's Name	Title
 Signed by Hardy, Sally on 05/27/22	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION


No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No.3150-0018, 0024, & 0090 _____

Comments:

While the PIA only mentions how the information of Operator Licensees is collected, the other information related to licensees was collected by the NRC through other approved collections


Reviewer's Name	Title
 Signed by Cullison, David on 05/23/22	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

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

Comments:


If identified, any additional information/data/records kept in this system may 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 not otherwise noted. 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
 Signed by Dove, Marna on 05/24/22	Sr. Program Analyst, Electronic Records Manager

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.
- 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:

 Signed by Partlow, Benjamin on 06/16/22

Acting Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: (Sponsor name and office)	
Name of System: Reactor Program System	
Date CSB received PIA for review:	Date CSB completed PIA review:
Noted Issues:	
Acting Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date:  Signed by Partlow, Benjamin on 06/16/22
<i>Copies of this PIA will be provided to:</i> Thomas G. Ashley, Jr. Director IT Services Development and Operations Division Office of the Chief Information Officer Garo Nalabandian Acting Chief Information Security Officer (CISO) Office of the Chief Information Officer	