U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Regional Applications – Region I (RAPP-RI)

Subsystem of Business Application Support System (BASS)

Office of the Chief Information Officer (OCIO)

Version 1.0

10/02/2023

Instruction Notes:
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

Template Version 2.0 (08/2023)

Document Revision History

Date	Version	PIA Name/Description	Author
10/02/2023	1.0	Regional Applications - Region I (RAPP-RI) Initial Release	OCIO Oasis Systems, LLC
09/13/2023	DRAFT	Regional Applications - Region I (RAPP-RI) Draft Release	OCIO Oasis Systems, LLC

Table of Contents

The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: Regional Applications - Region I (RAPP-RI).

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

Date Submitted for review/approval: October 30, 2023.

1 Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

Regional Applications (RAPP) is a subsystem of BASS, and RAPP is comprised of 3 sets of applications: Region I (RAPP-RI), Region II (RAPP-RII), Region IV (RAPP-RIV)

The RAPP-RI, RAPP-RII, and RAPP-RIV applications reside on BASS virtual servers. Regional system administrators are only responsible for their applications. BASS provides centralized services and database administration.

Region I descriptions are provided below:

The Region I office oversees Resident Inspector Site Expansion (RISE) locations throughout the Northeastern United States. Applications that support the business functions are hosted on BASS.

RAPP-RI applications include*:*

Region I Data Warehouse: consolidates all Regional I databases into a single warehouse which will host all RI modernized databases.

Staff Profile Request System (SPRS): manages Emergency Response Staff information and the staff reporting system.

Request Tracking System (RTS): provides a purchase tracking system that tracks all of the RI form 30 purchase activities.

Government Vehicle Reservations System (GVRS)*:* provides the interface for users to reserve government vehicles. This system allows users to interact with the vehicle management team to report and to maintain vehicle condition.

Emergency Responsibility Scheduling System (EROAS): provides a web access system that allows all emergency response members to log their availability through the ERO system. In addition to the logged availability, the system can generate EROAS reports based on management needs.

Ask Management Feedback System (AMFS): provides a web access system that regional staff use to communicate with the management team through a question-and-answer format. The AMFS implements role-based security to provide question privacy (anonymous submission) and automates the AMS publication processes.

SPRS is the application that stores PII information. The other applications are fed from SPRS which is under the development of the Region I Enterprise Database Application Modernization (EDAM) project. The purpose of the SPRS is multifold. First, it replaces the Region I intranet legacy system, which used obsolete technologies and tools. SPRS has implemented many new features to automate and replace the manual processes of Region I staff information updated from HQ ICAM nightly jobs. SPRS provides Region I staff information with functions for searching, updating local profiles, and integrating with the HQ ICAM system. SPRS also generates specific staff contact reports for organizational needs. The SPRS is a subset of the EDAM application developed by using the Microsoft C# and ASPNet MVC frameworks with Microsoft SQL server as the backend data store.

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

☐ PowerApps	☐ Public Website
☒ Dashboard	☐ Internal Website
☐ SharePoint	☐ None
☐ Other	

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response.

Status Options	
☒	New system/project
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.*
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below*
☐	Other (explain)

1.3 Points of Contact:

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Shihsing Chang	Gwen Hayden	Consuella Debnam	Michael Dean	Shihsing Chang	Michael Dean Mary Walsh
Office/ Division/ Branch	NRC R1 DRM IRB	OCIO	OCIO	NRC R1 DRM IRB	NRC R1 DRM IRB	NRC R1 DRM IRB
Telephone	610-337-5221	301-287-0761	301-287-0834	610-337-5079	610-337-5221	610-337-5079 610-337-5351

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	Authority	Citation/Reference
☐	**Statute**	
☐	**Executive Order**	
☐	**Federal Regulation**	
☐	**Memorandum of Understanding/Agreement**	
☒	**Other (summarize and provide a copy of relevant portion)**	TBD

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*).

Localized and centralized staff Information allows emergency responders to easily access all emergency personnel contact information. In addition, SPRS gives the management group the capability of getting employee profile reports.

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

Social Security numbers are not collected.

3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
☒	Federal employees
☒	Contractors
☐	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☐	Licensees
☐	**Other**

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table 2023.

Categories of Information			
☒	Name	☐	Resume or curriculum vitae
☐	Date of Birth	☐	Driver's License Number
☐	Country of Birth	☐	License Plate Number
☐	Citizenship	☐	Passport number
☐	Nationality	☐	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☒	Home Address	☐	Credit/Debit Card Number
☐	Social Security number (Truncated or Partial)	☐	Medical/health information
☐	Gender	☐	Alien Registration Number
☐	Ethnicity	☐	Professional/personal references
☐	Spouse Information	☐	Criminal History
☒	Personal e-mail address	☐	Biometric identifiers (facial images, fingerprints, iris scans)
☐	Personal Bank Account Number	☒	Emergency contact e.g., a third party to contact in case of an emergency

Categories of Information			
☒	Personal Mobile Number	□	Accommodation/disabilities information
□	Marital Status	☒	**Other:** Emergency contact name, phone number and address.
□	Children Information		
□	Mother's Maiden Name		

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

SPRS does one-way pulling (data transfer) with read-only access by Region I employees unless a user has specific role with specific access rights.

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

There is no hard paper form used to feed the SPRS.

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

Information is pulling only from the HQ ICAM view.

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

The data comes directly from HQ ICAM where it is validated, and any updates would be made directly in HQ ICAM.

3.5 Will PII data be used in a test environment? If so, explain the rationale.

No.

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

The registrant/applicant cannot access their information once the form is submitted to OCIO management. If there needs to be a change to the information, the individual must notify the manager. The incorrect data must be corrected through the NRC ICAM interface.

4 Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

Region I applications implement a least-privilege RBAC that restricts data access to only authenticated personnel who have a need-to-access to perform their job function for the subsystem.

SPRS is role-based security application. Below is the matrix of role permissions.

Role Name	Description	Module Access
RI EDAM System Admin	This is an administrative access, which provides full right to manage the EDAM applications.	ALL EDAM systems and Admin Modules
SPRS - User	Access rights to his/her own profile and view-only rights to the work information of other staff.	SPRS view module and Edit/Save his/her own local fields
SPRS - Manager	Access rights to all staff profile information and certain reports.	All SPRS modules including the reporting module
SPRS - Admin	Access rights to all staff profile information and certain reports. Access rights to the SPRS non-staff reference data.	Full access to all the SPRS modules

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

SPRS does not share any information with other NRC systems outside the Region I domain, except applications used specifically for Region I employees.

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

N/A.

Identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
□	Contract Provide Contract Number:
□	License Provide License Information:
□	Memorandum of Understanding Provide ADAMS ML number for MOU:
□	Other
☒	None

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

SPRS is accessed through the Region I intranet and uses the role-based access mechanism. All privileged domain accounts are logged and recorded by Splunk. Region I application administrators receive Splunk reports daily. Region I application administrators are also able to run a report at the application level that shows privileged user actions.

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

The staff information comes from the ICAM view and can only be accessed through internal application code. The code is also embedded with security logic to prevent unauthorized method calls. The security logics have been implemented to check the role-based access right to reveal authorized data.

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

The data is stored in the Region I SQL server.

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

The SPRS is only hosted by the Region I IIS server and the code only resides in the protected NRC server domain. It is the Region I intranet application.

4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?

Yes, all contractors have gone through the security check and have been issued valid NRC badges.

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

The Region I Data Warehouse used by the EDAM suite implements the following audit columns and is available for auditing purposes as needed.

CreatedDate, CreatedBy, LastModifiedDate, LastModifiedBy.

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

Yes, the SPRS database table has implemented auditing fields such as “CreateBy”, “ModifiedBy”, “CreateByTimestamp”, and “ModifyByTimestamp.”

4.11 Define which FISMA boundary this project is part of.

BASS.

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
□	Unknown
□	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track***.**
□	In Progress provide the estimated date to receive an ATO**.** Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity-Moderate Availability-Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

20210011.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
☒	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)**
☒	**List the identifiers that will be used to retrieve the information on the individual.** Information from the Staff Profile Request System (SPRS) is retrieved by individual names.
□	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.**

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

Response	
☒	***Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)*** ***Provide the SORN name, number, (List all SORNs that apply):*** SPRS is covered by NRC-36, Employee Locator Records.
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☐	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?

> *A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.*

Mark the appropriate response.

Options	
☐	**Privacy Act Statement**
☒	**Not Applicable**
☐	**Unknown**

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

This is not applicable because data comes from the ICAM view and has been approved and predefined.

6 Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for NARA's Universal Electronic Records Management (ERM) requirements, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding RIM - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☒	NUREG-0910, "NRC Comprehensive Records Disposition Schedule
☒	NARA's General Records Schedules
□	Unscheduled

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	Region I (RAPP-RI)
Records Retention Schedule Number(s)	See the table below for a listing of RAPP-RI modules and records retention schedules.
Approved Disposition Instructions	See the table below for a listing of RAPP-RI modules and Disposition Instructions.

RAPP-RI Module	**Module Description**	**Schedule Number**	**Disposition**
Reg I Data Warehouse	Consolidates all RI databases into a single warehouse which will host all RI modernized databases	*Reference Copy” Data collections should be retained according to the NUREG 0910 Part 25 (Regions) and NARA’s GRS	Retain until it is no longer needed for business use.
Staff Profile Request System (SPRS)	Manages Emergency Response Staff information and the staff reporting system	GRS 5.3 item 020 – Employee emergency contact information	Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employees
Request Tracking System (RTS)	Provides a purchase tracking system that tracks all of the RI Form 30 purchase activities	GRS 1.1 item 011 – Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. All other copies. Copies used for administrative or reference purposes. **(This assumes that OCFO holds the official copy.)**	Temporary. Destroy when business use ceases.

Government Vehicle Reservations System (GVRS)	Provides the interface for users to reserve government vehicles. The system allows users to interact with the vehicle management team to report and maintain vehicle condition.	GRS 5.4 item 010 – Facility, space, vehicle, equipment, stock, and supply administrative and operational records…records scheduling and dispatching vehicles…	Temporary. Destroy when 3 years old or 3 years after superseded, as appropriate, but longer retention is authorized if required for business use.
		GRS 5.4 item 090 – Land vehicle and water vessel inspection, maintenance, and service records.	Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use. Transfer of extant records to new owns at sale or donation is authorized.
		GRS 5.4 item 110 – Vehicle and heavy equipment operator records.	Temporary. Destroy 3 years after separation of employee or 3 years after rescission of authorization to operate vehicles or equipment, whichever is sooner.
Emergency Responsibility Scheduling System (EROAS)	Provides a web access system that allows all emergency response members to log their availability through the ERO system. In addition to the logged availability, the system can generate EROAS reports based on management needs.	GRS 5.3 item 020 – Employee emergency contact information	Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employees

Ask Management Feedback System (AMFS)	Provides a web access system that regional staff use to communicate with the management team through a question-and-answer format. The AMFS implements role-based security to provide question privacy (anonymous submission) and automates the AMS publication processes.	GRS 5.8 item 010 – Technical and administrative help desk operational records	Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	N/A
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	N/A
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	N/A

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an OMB approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or more members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

Yes.

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

No.

7.3 Is the collection of information required by a rule of general applicability?

No.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: https://intranet.nrc.gov/ocio/33456.

8 Privacy Act Determination

Project/System Name: Regional Applications - Region I (RAPP-RI).

Submitting Office: Office of the Chief Information Officer (OCIO).

Privacy Officer Review

Review Results		Action Items
□	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
□	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☒	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

The *Staff Profile Request System (SPRS)* is covered by NRC-36, Employee Locator Records.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 12/06/23	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
☒	No OMB clearance is needed.
☐	OMB clearance is needed.
☐	Currently has OMB Clearance. Clearance No.________________

Comments:

An OMB clearance is not needed if the collection of information from contractors is within the scope of their contract.

Reviewer's Name	Title
Signed by Cullison, David on 11/17/23	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

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

Comments:

Reviewer’s Name	Title
Marna B. Dove Signed by Dove, Marna on 11/20/23	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

Review Results	
□	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☒	This project/system **does** collect, maintain, or disseminate information in identifiable form.

I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Feibus, Jonathan
on 12/06/23

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

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Regional Applications – Region I (RAPP-RI)	
Date CISD received PIA for review: October 31, 2023	**Date CISD completed PIA review:** December 1, 2023
Action Items/Concerns:	
Copies of this PIA will be provided to: *Caroline Carusone* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Garo Nalabandian* *Deputy Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	