
U.S. Nuclear Regulatory Commission



Privacy Impact Assessment
Office of the Inspector General - Investigations,
Correspondence, and Audit Management System
(OIG-ICAMS)
Subsystem of Business Application Support System
(BASS)
Office of the Chief Information Officer (OCIO)

Version 1.1
04/29/2024

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

Document Revision History

Date	Version	PIA Name/Description	Author
04/29/2024	1.1	Minor edits- Updated Project Manager, added SSN collection category of information	Rick Grancorvitz, OIG
09/12/2023	1.0	Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS) – Initial Release	OCIO Oasis Systems, LLC
08/17/2023	DRAFT	Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS) - Draft Release	OCIO Oasis Systems, LLC

Document Review History

Date Reviewed	Comments	Reviewed By
MM/DD/YYYY	Annual Review Certification	<Insert Reviewer Name>

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

Table of Contents

1	Description	1
2	Authorities and Other Requirements	3
3	Characterization of the Information	4
4	Data Security	6
5	Privacy Act Determination	9
6	Records and Information Management-Retention and Disposal	10
7	Paperwork Reduction Act	13
8	Privacy Act Determination	14
9	OMB Clearance Determination	15
10	Records Retention and Disposal Schedule Determination	16
11	Review and Concurrence	17

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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: Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS).

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

Date Submitted for review/approval: April 29, 2024

Note: When completing this PIA do not include any information that would raise security concerns or prevent this document from being made publicly available.

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.

OIG-ICAMS is a subsystem of the Office of the Chief Information Officer (OCIO) Business Application Support System (BASS) and includes the external Information Technology (IT) service OPEXUS eCase Platform. The OPEXUS eCase Platform is provided to the U.S. Nuclear Regulatory Commission (NRC) as a Software-as-a-Service (SaaS) cloud solution by OPEXUS, Inc. The OPEXUS eCase Platform is authorized by the Federal Risk and Authorization Management Program (FedRAMP).

OPEXUS eCase is a low-code digital process automation (DPA) platform built for dynamic case management (DCM). Their innovative platform empowers agile workflow-driven tasking and decision making across diverse business areas. eCase’s architecture is ideal for investigative case processing, audit management, and correspondence tracking as it enables simple configuration of case types with associated approval workflows, rules, permissions, reports, and more. The OPEXUS solution provides a native document management module to enable attachment of documents to tasks, document approval workflows, retention, and full text search. eCase provides real-time tracking and reporting on all tasks and documents within the system, collaboration tools for communication with internal and external contacts, configurable task approval workflows, and configurable rules, roles, and permissions to ensure consistent and secure processing across the enterprise.

OPEXUS maintains a FedRAMP-moderate data center, certified at the infrastructure-as-a-service (IaaS) level and the eCase Platform is certified at the SaaS and platform-as-a-service (PaaS) levels. The NRC solution is to utilize the SaaS solution for eCase. OPEXUS’ data center services are provided from their Top Secret cleared facility, which is compliant with FedRAMP, Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), and Federal Information Processing Standard (FIPS) security provisions.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

The data center provides system monitoring and redundant infrastructure via the implementation of clustered servers, uninterruptable power supplies, redundant networks, equipment, and other devices and methods to ensure data is fully protected. Data at rest and in transit, including connections to the database, utilize encrypted TLS protocols.

OPEXUS eCase contains the following modules:

- **eCase Audit** - Provides a collaborative workflow-driven solution to support audit and compliance processes. The eCase Audit solution spans the complete audit lifecycle: from audit planning, audit performance, and audit follow-up to recommendation tracking and reporting. It tracks the workflow of audit events, artifacts, reports, recommendations, and corrective actions. eCase Audit features include risk-based audit planning and scoping, workpaper management, configurable workflows, audit management toolkit, team-based collaborations, time tracking, issue tracking and resolution management, role-based access and views, reports dashboards, and Key Performance Indicators.
- **eCase Investigations** – Provides a configurable, Commercial off-the-shelf collaborative workflow-driven solution designed to automate, track, and report on the complete investigations process from hotline complaint receipt to case closure. The Hotline Portal allows public users to submit hotline complaints and assigns complaints to NRC OIG users within the eCase Investigation’s system. Key stages of the investigative process automated by eCase Investigations include initial processing, review, assignment, investigation, case closure, and generating the final report of investigation. Additional features include time management, inventory management, and integrity briefings management for internal and external briefings.
- **eCase Correspondence** – Provides a configurable, workflow-driven application designed to meet a variety of correspondence needs, from basic correspondence tracking and tasking to complex case management. eCase Correspondence includes robust document management out-of-the-box which captures correspondence in a case folder and adds associated attributes for future use/retrieval to provide agencywide tracking, document version control, retention management, and real-time reporting of statistical data.

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

<input type="checkbox"/> PowerApps	<input type="checkbox"/> Server/Database Design
<input type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Public Website
<input type="checkbox"/> SharePoint	<input type="checkbox"/> Internal Website
<input checked="" type="checkbox"/> Other The NRC OIG-ICAMS is in a FedRAMP-authorized cloud. This is a Software-as-a-Service (SaaS) solution.	

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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	
<input type="checkbox"/>	New system/project
<input type="checkbox"/>	Modification to an existing system/project. <i>If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.</i> <Insert response here >
<input checked="" type="checkbox"/>	Annual Review <i>If making minor edits to an existing system/project, briefly describe the changes below.</i> Change PM and to include the SSN categorization of information that Investigations may track based on the case.
<input type="checkbox"/>	Other (explain)

1.3 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	System Owner/Data Owner/Steward	ISSM	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Kris Marchant	Gwen Hayden	Consuella Debnam	Ziad Buhaiissi	N/A	N/A
Office /Division /Branch	Office of the Inspector General (OIG)	Office of the Chief Information Officer (OCIO)	Office of the Chief Information Officer (OCIO)	Office of the Inspector General (OIG)		
Telephone	301-415-5980	301-287-0761	301-287-0834	301-415-1983		

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.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

Mark with an "X" on all that apply.	Authority	Citation/Reference
<input checked="" type="checkbox"/>	Statute	Inspector General Act of 1978 (as amended).
<input type="checkbox"/>	Executive Order	
<input type="checkbox"/>	Federal Regulation	
<input type="checkbox"/>	Memorandum of Understanding/Agreement	
<input type="checkbox"/>	Other (summarize and provide a copy of relevant portion)	

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).

Information is collected to support the OIG’s mission to (1) independently and objectively conduct and supervise audits and investigations relating to NRC and Defense Nuclear Facilities Safety Board (DNFSB)’s programs and operations; (2) prevent and detect fraud, waste, and abuse, and (3) promote economy, efficiency, and effectiveness in NRC and DNFSB’s programs and operations.

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

OIG-ICAMS uses social security numbers for the purpose of conducting the investigations. The SSN is collected to verify the subject. Collection can be from the agency or the subject themselves.

3 Characterization of the Information

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

Category of individual	
<input checked="" type="checkbox"/>	Federal employees
<input checked="" type="checkbox"/>	Contractors
<input type="checkbox"/>	Members of the Public (any individual other than a federal employee, consultant, or contractor)
<input type="checkbox"/>	Licensees
<input type="checkbox"/>	Other <Insert response here>

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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			
<input checked="" type="checkbox"/>	Name	<input checked="" type="checkbox"/>	Resume or curriculum vitae
<input checked="" type="checkbox"/>	Date of Birth	<input checked="" type="checkbox"/>	Driver's License Number
<input checked="" type="checkbox"/>	Country of Birth	<input type="checkbox"/>	License Plate Number
<input checked="" type="checkbox"/>	Citizenship	<input checked="" type="checkbox"/>	Passport number
<input checked="" type="checkbox"/>	Nationality	<input type="checkbox"/>	Relatives Information
<input checked="" type="checkbox"/>	Race	<input type="checkbox"/>	Taxpayer Identification Number
<input checked="" type="checkbox"/>	Home Address	<input type="checkbox"/>	Credit/Debit Card Number
<input checked="" type="checkbox"/>	Social Security number (Truncated or Partial)	<input type="checkbox"/>	Medical/health information
<input checked="" type="checkbox"/>	Gender	<input checked="" type="checkbox"/>	Alien Registration Number
<input checked="" type="checkbox"/>	Ethnicity	<input type="checkbox"/>	Professional/personal references
<input type="checkbox"/>	Spouse Information	<input checked="" type="checkbox"/>	Criminal History
<input checked="" type="checkbox"/>	Personal e-mail address	<input type="checkbox"/>	Biometric identifiers (facial images, fingerprints, iris scans)
<input type="checkbox"/>	Personal Bank Account Number	<input type="checkbox"/>	Emergency contact e.g., a third party to contact in case of an emergency
<input checked="" type="checkbox"/>	Personal Mobile Number/Home Number	<input type="checkbox"/>	Accommodation/disabilities information
<input type="checkbox"/>	Marital Status	<input type="checkbox"/>	Other: Work address, employer, height, weight, scars/tattoos, picture.
<input type="checkbox"/>	Children Information		
<input type="checkbox"/>	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).

The information is obtained from a variety of sources including, but not limited to, the individual record subject; NRC officials and employees; and NRC contractors. It could contain information obtained from any NRC sensitive but unclassified files or systems. It does not contain Classified or Safeguards information.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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

No, information is collected in OIG-ICAMS by authorized users only. Reference documents in electronic format are attached in the system using built-in electronic data transfer mechanisms of Windows.

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

The information is obtained from a variety of sources including, but not limited to, the individual record subject; NRC and DNFSB officials and employees; employees of Federal, State, local, and foreign agencies; and other persons.

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

OIG staff that input and update information in the system are responsible for ensuring that the data entered is current, accurate, and complete. OIG-ICAMS also utilizes a variety of automated mechanisms to verify the information, including:

- Mandatory fields that must be completed before a document can be saved.
- Configurable pick lists for selecting values for key fields to ensure data consistency.
- Required management review and approval of documents, and record locking to prevent changes once documents are approved.
- Validation checks to verify that prerequisite activities were completed.

3.5 Will PII data be used in a test environment? If so, explain the rationale for this and how the PII information is protected.

No.

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

Any information deemed to be inaccurate can be relayed to OIG staff working the case. OIG staff are responsible for ensuring the data is current, accurate, and complete.

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).

Access to information is limited to OIG through least privilege and separation of duties principles. The roles that have access to the data are OIG special agents, OIG investigative analysts, OIG auditors and management analysts, OIG team leaders and managers, OIG General Counsel, OIG administrative support staff, and system administrators.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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.

N/A

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	
<input type="checkbox"/>	Contract Provide Contract Number:
<input type="checkbox"/>	License Provide License Information:
<input type="checkbox"/>	Memorandum of Understanding Provide ADAMS ML number for MOU:
<input type="checkbox"/>	Other
<input checked="" type="checkbox"/>	None

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

Logical access controls have been implemented to prevent misuse of data (i.e., unique username and password requirements). OIG-ICAMS logs user activity including the username and the date/time records were accessed, created, or modified. Access logs are reviewed by the system administrators and Subsystem ISSOs for anomalies. Attempts to access OIG-ICAMS by unauthorized users are also logged.

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).

Data in transit and at rest utilize encrypted TLS security protocols.

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

Data is stored at the OPEXUS FedRAMP-moderate data center.

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

Users who have an NRC mobile desktop computer can access the OIG-ICAMS remotely through NRC's Virtual Private Network (VPN).

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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

OIG-ICAMS data is available only to authorized personnel who have a need to know and whose duties require access to the information.

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

Logical access controls have been implemented to prevent misuse of data (i.e., unique username and password requirements). OIG-ICAMS logs user activity including the username and the date/time records were accessed, created, or modified. Access logs are reviewed by the system administrators and subsystem ISSOs for anomalies. Attempts to access OIG-ICAMS by unauthorized users are also logged.

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

No.

4.11 Define which FISMA boundary this project is part of.

OIG-ICAMS is a subsystem of the Office of the Chief Information Officer (OCIO) Business Application Support System (BASS).

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

Authorization Status	
<input type="checkbox"/>	Unknown
<input type="checkbox"/>	No <i>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.</i>
<input type="checkbox"/>	In Progress provide the estimated date to receive an ATO. Estimated date: <insert appropriate response>

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

Authorization Status	
<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	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.

20050018.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
<input type="checkbox"/>	Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, or other unique number, etc.)
<input type="checkbox"/>	List the identifiers that will be used to retrieve the information on the individual.
<input checked="" type="checkbox"/>	No, the PII is not retrieved by a personal identifier. If no, explain how the data is retrieved from the project. Investigations, correspondence, and audit information will be retrieved by a folder id. In investigations, the unique folder id will correspond to a complaint, or an investigation. In correspondence, the unique folder id will correspond to a unique correspondence number. In audit information, the folder id will correspond to a unique audit number. There will be options to retrieve contact information by First Name, Last Name, email, or address.

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.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

Response	
<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)</p> <p>Provide the SORN name, number, (List all SORNs that apply):</p> <p>NRC 18 – Office of the Inspector General (OIG) Investigative Records – NRC and Defense Nuclear Facilities Safety Board (DNFSB) located at https://www.nrc.gov/docs/ML2002/ML20022A239.pdf</p>
<input type="checkbox"/>	SORN is in progress
<input type="checkbox"/>	SORN needs to be created
<input type="checkbox"/>	Unaware of an existing SORN
<input type="checkbox"/>	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	
<input checked="" type="checkbox"/>	<p>Privacy Act Statement</p> <ul style="list-style-type: none"> - <i>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.</i> <p><i>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.</i></p>
<input type="checkbox"/>	Not Applicable
<input type="checkbox"/>	Unknown

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

Providing PII is Mandatory.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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 Records and Information Management - 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?

<input checked="" type="checkbox"/>	NUREG-0910, “NRC Comprehensive Records Disposition Schedule
<input checked="" type="checkbox"/>	NARA’s General Records Schedules
<input type="checkbox"/>	Unscheduled

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

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)	OIG-ICAMS
Records Retention Schedule Number(s)	A records retention and disposition schedule (N1-431-10-002) – Records of the Office of the Inspector General for OIG records , including OIG-ICAMS, was approved by the Archivist of the United States on September 16, 2014. There are multiple items associated with this schedule containing both Permanent and Temporary items. GRS 3.2 item 010 – Systems and data security records
Approved Disposition Instructions	I See N1-431-10-002 – Records of the Office of the Inspector General for OIG records , including OIG-ICAMS. GRS 3.2 Item 010 : Systems and data security records Temporary . Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
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

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

<p>Disposition of Permanent Records</p> <p>Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions?</p> <p>If so, what formats will be used?</p> <p>NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</p>	<p>N/A</p>
---	------------

Note: Information in *Section 6, Records and Information Management-Retention and Disposal* does not need to be fully resolved for final approval of the privacy impact assessment.

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (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?

The Inspector General Empowerment Act of 2016 amended the Inspector General Act of 1978 to exempt Inspector General information collection activities related to an audit, investigation, or other review from Paperwork Reduction Act requirements.

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)?

N/A

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

The Paperwork Reduction Act does not apply to the conduct of a federal criminal investigation or during the conduct of an administrative action, investigation, or audit involving an agency or specific individuals or entities.

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>.

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

8 Privacy Act Determination

Project/System Name: Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS).

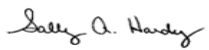
Submitting Office: Office of the Chief Information Officer (OCIO)

Privacy Officer Review

Review Results		Action Items
<input type="checkbox"/>	This project/system does not contain PII .	No further action is necessary for Privacy.
<input type="checkbox"/>	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.
<input checked="" type="checkbox"/>	This project/system does contain PII ; the Privacy Act does apply .	SORN is required- Information is retrieved by a personal identifier.

Comments:

NRC 18 – Office of the Inspector General (OIG) Investigative Records – NRC and Defense Nuclear Facilities Safety Board (DNFSB)

Reviewer's Name	Title
 Signed by Hardy, Sally on 06/06/24	Privacy Officer


Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
<input checked="" type="checkbox"/>	No OMB clearance is needed.
<input type="checkbox"/>	OMB clearance is needed.
<input type="checkbox"/>	Currently has OMB Clearance. Clearance No. _____

Comments:

Reviewer's Name	Title
 Signed by Cullison, David on 06/05/24	Agency Clearance Officer


Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
<input type="checkbox"/>	No record schedule required.
<input type="checkbox"/>	Additional information is needed to complete assessment.
<input type="checkbox"/>	Needs to be scheduled.
<input checked="" type="checkbox"/>	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 06/05/24	Sr. Program Analyst, Electronic Records Manager

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

11 Review and Concurrence

Review Results	
<input type="checkbox"/>	This project/system does not collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	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 06/06/24

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

Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	Version 1.1
Privacy Impact Assessment	04/29/2024

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System:	
Office of the Inspector General - Investigations, Correspondence, and Audit Management System	
Subsystem of Business Application Support System	
Date CISD received PIA for review:	Date CISD completed PIA review:
April 29, 2024	June 6, 2024
Action Items/Concerns:	
<i>Copies of this PIA will be provided to:</i>	
<p><i>Gwen Hayden Acting Director IT Services Development and Operations Division Office of the Chief Information Officer</i></p> <p><i>Katie Harris Acting Deputy Chief Information Security Officer (CISO) Office of the Chief Information Officer</i></p>	