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.

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

Date: April 5, 2022

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system: (*Use plain language, no technical terms.*)

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 AINS eCase Platform. AINS eCase Platform is provided to the U.S. Nuclear Regulatory Commission (NRC) as a Software-as-a-Service (SaaS) cloud solution by AINS, Inc. The AINS eCase Platform is authorized by the Federal Risk and Authorization Management Program (FedRAMP).

AINS 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. AINS 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.

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

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.

2. What agency function does it support? (*How will this support the U.S. Nuclear Regulatory Commission's (NRC's) mission, which strategic goal?)*)

Utilizing the AINS eCase SaaS, OIG-ICAMS supports investigations, correspondence, and audits performed by the OIG for the NRC and the Defense Nuclear Facilities Safety Board (DNFSB).

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

AINS eCase contains the following modules:

- eCase Audit - Provides a collaborative workflow-driven solution to support audit and compliance processes. 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 and 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, requires 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 agency-wide tracking, document version control, retention management, and real-time reporting of statistical data. eCase Correspondence.

a. Provide ADAMS ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.

N/A – OIG-ICAMS does not have any subsystems nor components.

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.*)

Inspector General Act of 1978 (as amended).

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

Information is collected to support the OIG's mission to (1) independently and objectively conduct and supervise audits and investigations relating to NRC and 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.

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**
Rick Grancorvitz	OIG/RMOS	301-287-0805
Business Project Manager	**Office/Division/Branch**	**Telephone**
Rick Grancorvitz Kristean Marchant	OIG/RMOS OIG/AIGI	301-287-0805 301-415-5890
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Rick Grancorvitz Kristean Marchant	OIG/RMOS OIG/AIGI	301-287-0805 301-415-5890
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Ziad Buhaissi	OIG	301-415-1983
ISSO	**Office/Division/Branch**	**Telephone**
Consuella Debnam Luc Phuong	OCIO/GEMSD/CSB/IAT OCIO/GEMSD/CSB/IAT	301-287-0834 301-415-1103
System Owner/User	**Office/Division/Branch**	**Telephone**
Thomas Ashley	OCIO/ITSDOD	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

__X__ 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.

June 26, 2020 – ML20150A436.

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

Migration of the legacy Office of the Inspector General Management Information System (OIGMIS) from an on-premise solution hosted in the NRC data center to a FedRAMP authorized cloud-based Software-as-a-Service solution hosted by a commercial vendor AINS.

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

Yes.

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

20050018.

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.)).

Investigation information includes individuals and entities referred in complaints or actual investigative cases, reports, accompanying documents, and correspondence prepared by, compiled by, or referred to the OIG. Subjects of the complaints and investigative cases include Federal employees and contractors. Information about the persons making the complaints could include Federal employees and contractors, licensees, interveners, or the general public.

Audit information includes names, titles, and work contact information for NRC and DNFSB employees and contractors associated with the NRC and DNFSB activities being audited.

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

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

OIG-ICAMS could include the following information about an individual: first name, last name, home and work address, home and work phone number, employer, and email address.

Optional fields are Other Names Used, Date of birth, Place of Birth, Height, Weight, Social security number, Personal Telephone Number (Home, Mobile), Sex, Race, Marital Status, Scar/Marks/Tattoos, Prior Criminal Record and Picture.

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

Yes, 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.

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

OIG-ICAMS information could include correspondence, cases, matters, memoranda, materials, legal papers, evidence, exhibits, and data about a case and/or audit. An individual's first name, last name, address, phone number, social security number and email address could also be collected should it concern the specifics of an investigation or audit.

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?

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.

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

N/A.

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

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 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, or foreign agencies; licensees; interveners, advocacy groups, and the general public.

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

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

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

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.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

Yes. Based on the NIST Special Publication (SP) 800-60 and as documented in the OIG-ICAMS Security Categorization, the following types of Information are processed:

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

Information Type	NIST SP 800-60 Description
Program Evaluation Information Type	Program Evaluation Information is used to document, analyze and report information related to complaints, investigations, and audit work.
Program Monitoring Information Type	Program Monitoring Information is used to document, analyze and report information related to internal and external programs and the extent to which they comply with related laws, regulations, and policies.
IT Security Information Type	IT Security Information is used to configure and monitor security configurations and to restrict access to data and functions.
Record Retention	Record Retention involves the management of the official documents and records while adhering to an approved National Archives and Records Administration (NARA) records retention schedule.
Criminal Investigation and Surveillance Information Type	Criminal investigation and surveillance includes the collection of evidence required to determine responsibility for a crime and the monitoring and questioning of affected parties.
Legal Investigation Information Type	Legal Investigation Information is used to document, track and support activities

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

The information is obtained from internal and external 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.

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.

- Conducting, managing, and tracking the status and outcome of complaints, investigations, and audits
- References for aiding current OIG projects

- Routine uses identified in the Privacy Act System of Records Notices, NRC- 18, Office of the Inspector General (OIG) Investigative Records

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the data in this system?

The System Administrator and the BASS Information System Security Officer(s) (ISSO) are responsible for ensuring that the policies and procedures of the system are followed by users. The Assistant Inspector General for Investigations is responsible for ensuring that investigative records are used in accordance with the Privacy Act System of Records Notices, NRC-18, Office of the Inspector General (OIG) Investigative Records.

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

Yes.

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

The Cloud Service Provider, AINS, Inc., has provided the following documents detailing the data elements within the AINS eCase Platform.

- eCase Audit Data Models Documentation
- eCase Audit Data Dictionary
- eCase Investigation Data Models Documentation
- eCase Investigation Data Dictionary

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

No.

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

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

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

N/A.

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

N/A.

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

N/A.

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

Investigations, correspondence, and audit information will be retrieved by a folder id. In investigations the unique folder id will correspond to a complaint, preliminary, or investigation. Correspondence this will correspond to a unique correspondence number. Audit the folder id will correspond to a unique audit number. Contact information will have the options of be retrieved by First Name, Last Name, email, or address.

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

Contact information will have the options of be retrieved by First Name, Last Name, email, or address.

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.

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

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

Yes.

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.

A variety of reports are available to authorized users, such as:

- Performance measure reports
- Training activity reports
- Audit recommendation reports
- Hotline activity reports
- Complaint and Case reports
- Pending follow-up reports
- Referral reports
- Legal outcome and prosecution reports
- Law Enforcement Availability Pay (LEAP) reports
- Time and Expense by Activity reports

a. What are the reports used for?

Reports are used to track and manage investigation and audit activities, to assess progress in meeting OIG performance measures, to provide statistics for inclusion in OIG's Semi-Annual Report to Congress, and to respond to requests for information from external entities such as the Federal Bureau of Investigation.

b. Who has access to these reports?

Authorized OIG users.

D. ACCESS TO DATA

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

OIG.

(1) For what purpose?

Daily work activities that support OIG investigations, correspondence, and audit processing.

(2) Will access be limited?

Yes, access to information is limited to OIG through least privilege and separation of duties principles.

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

No.

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

N/A.

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

N/A.

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

No.

(1) If yes, who?

N/A.

(2) Will access be limited?

N/A.

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

N/A.

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

N/A.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 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).

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

A records retention and disposition schedule (N1-431-10-002) for OIG records, including OIG-ICAMS, was approved by the Archivist of the United States on September 16, 2014. Additional information is scheduled under the General Records Schedules (GRS) below:

IT Security Information Type (found under PIA Section B.2.a(1)	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.

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).

Users must be logged in to the NRC LAN using their NRC authorized computer before attempting to connect to the OIG-ICAMS system hosted by AINS. Through a secure (https) Uniform Resource Locator (URL), users must first authenticate with their PIV card and PIN followed by an id and password to login and access OIG-ICAMS in the cloud. Once users successfully connect to the system, the roles and permissions of each module limit what they can see and do. Additional access within the investigations and audit modules allows for additional security for items label as sensitive or for grand jury.

OIG-ICAMS data is available only to authorized personnel who have a need to know and whose duties require access to the information. The application utilizes separation of duties to determine login abilities. Separate login accounts with different access privileges are used by personnel who have multiple roles, such as an auditor who also serves as a backup system administrator.

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

Access to data within AINS eCase is restricted to authorized personnel who have a need to know and whose duties require access to the information. Users are assigned roles based on their responsibilities limited their access and preventing misuse. Action History Log also shows when information was access and updated. Access permissions are promptly removed when users leave the OIG.

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

Yes.

(1) If yes, where?

The OIG-ICAMS Technical Guidelines is maintained by the OIG within their SharePoint site.

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

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

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

Security controls implemented within the OIG-ICAMS apply to all users and sessions regardless of their location.

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

- OIG special agents
- OIG investigative analysts
- OIG auditors and management analysts
- OIG team leaders and managers
- OIG General Counsel
- OIG administrative support staff
- System administrators

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

Yes.

a. If yes, what will be collected?

The OIG-ICAMS username and date/time of successful login is recorded. OIG-ICAMS also logs user activity including the username, and the date/time records were access, created, or modified.

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

Yes, the cloud service provider, AINS, contractors will be involved with the design and development of the system. As this is a SaaS solution they will also be involved with the maintenance of the system in terms of hardware and software updates.

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?

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.

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

Yes, FIPS 140-2 compliant encryption and the other required FISMA security controls have been implemented.

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

OIG-ICAMS is using an external IT service, AINS eCase Platform. AINS eCase Platform is provided to the NRC as a SaaS cloud solution by AINS, Inc. The AINS eCase Platform is authorized by the Federal Risk and Authorization Management Program (FedRAMP).

The AINS eCase Platform completed its latest FedRAMP Security Assessment in February 2022.

OIG-ICAMS will undergo an Authorization System Cybersecurity Assessment (ASCA) in CY 2022 to obtain an ongoing authorization.

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

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

Submitting Office: Office of Inspector General (OIG)

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
Covered by 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 04/28/22	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:

Reviewer's Name	Title
Signed by Cullison, David on 04/19/22	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

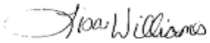
____ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

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

Comments:

Reviewer's Name	Title
 Signed by Williams, Lisa on 04/21/22	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.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

 Signed by Partlow, Benjamin on 05/04/22

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: Ziad Buhaissi, Office of Inspector General (OIG)	
Name of System: Office of the Inspector General - Investigations, Correspondence, and Audit Management System (OIG-ICAMS)	
Date CSB received PIA for review: April 5, 2022	**Date CSB completed PIA review:** April 27, 2022
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 05/04/22
Copies of this PIA will be provided to: *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*	