Privacy Impact Assessment

Allegations, Resolution, Investigation and Enforcement System (ARIES)

Subsystem of Business Application Support System (BASS)

Office of the Chief Information Officer (OCIO)

Version 1.2
11/09/2023

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

Document Revision History

Date	Version	PIA Name/Description	Author
10/13/2023	1.0	ARIES PIA Initial Draft Release	Bill Nightingale
10/25/2023	1.1	ARIES PIA Final Draft Release	OCIO/Bill Nightingale
11/9/2023	1.2	Updated ARIES PIA Final Draft	OCIO/Bill Nightingale

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: Allegation, Resolution, Investigation and Enforcement System (ARIES) - Formerly Case Management System Web (CMS-W).

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

Date Submitted for review/approval: November 9, 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.

The Allegations, Resolution, Investigation and Enforcement System (ARIES) is an overarching subsystem hosted within the Microsoft Power Platform that provides an integrated methodology for planning, scheduling, conducting, reposting, and analyzing allegation programs for the U.S. Nuclear Regulatory Commission (NRC). ARIES is the umbrella title given to three separate processes. It includes legacy functionality from the following legacy functionality. In addition to legacy functionality, improvements have been made to reflect current business owner needs.

- Allegation Process - Allows authorized users to store and retrieve key information on allegations related to NRC- regulated facilities.

- Investigation Process - Designed to assist the Office of Investigations (OI) meet their objectives by tracking all the different entities required for NRC investigations.

- Enforcement Process - Allows authorized users to enter new or updated case information, query enforcement case information and report on enforcement case information.

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.* ML23244A043
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	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	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Arathi Dommeti	Caroline Carusone	Consuella Debnam	Sandra Mendez - Allegations David Hsia – Investigations Gerald Gulla - Enforcement	Bill Nightingale	Dave Nelson Thomas Ashley David Pelton
Office /Division /Branch	OCIO/ITS DOD/ADS B/CCAT	OCIO/SDOD	OCIO	OE, OI	OCIO	OCIO OI OE
Telephone	301-415-4003	301-415-1085	301-287-0834	301-287-9426 301-415-3486 301-287-9143	703-973-3265	301-415-8700 301-415-0771 301-415-1492

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**	• Privacy Act of 1974, as amended, 5 U.S.C. §552a • Paperwork Reduction Act, as amended, 44 U.S.C. § 3501 et seq • E-Government Act of 2002, Section 208 (Public Law 107-347) • Records Management by Federal Agencies, 44 U.S.C. Chapter 31
☐	**Executive Order**	
☐	**Federal Regulation**	
☐	**Memorandum of Understanding/Agreement**	
☐	**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*).

ARIES contains sensitive allegation, enforcement action, and investigation data involving actual or alleged criminal and civil/regulatory violations. ARIES may include witness and subject names and personal identifiers as well as personal background information with address and phone numbers. These systems will contain detailed information on current and completed allegations, enforcement actions, and investigations with pre-decisional information for enforcement actions.

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	☒	Organization
☒	Date of Birth	☒	Driver's License Number
☒	Country of Birth	□	License Plate Number
☒	Citizenship	□	Passport number
☒	Nationality	□	Relatives Information
☒	Home or Cellular Number	☒	Taxpayer Identification Number
☒	Mailing Address	☒	Professional Training
☒	Social Security Number	☒	Witness and Subject Names
☒	Gender	☒	Experience
☒	Ethnicity	□	Professional/personal references
☒	License Type	☒	Education
☒	Email Address	☒	Biometric identifiers (Height, Weight, Hair Color, Eye Color, Scars, Tattoos, etc.)
☒	Title	☒	Certifications
☒	Personal Mobile Number	□	Accommodation/disabilities information
□	Marital Status	□	**Other**
□	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).

Information is initially provided in the form of a third-party contact in the form of emails, phone calls or in person contact regarding possible issues at facilities. Subsequent interviews will gather additional information regarding an Allegation, (e.g., personal information, additional witness information, facility information, etc.)

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

N/A.

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

Information is initially provided in the form of a third-party contact in the form of emails, phone calls or in person contact regarding possible issues at facilities. Subsequent interviews will gather additional information regarding an Allegation, (e.g., personal information, additional witness information, facility information, etc.)

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

The ARIES approach to data integrity, including accuracy, is multi-faceted and incorporates all of the following elements:

- There is no external portal or interface. The data are entered into ARIES by cleared NRC personnel.
- We have worked with Stakeholders and User Groups to ensure that only data elements that deliver real business value are captured within the system. All extraneous data elements from the three legacy systems have not been incorporated into the future system.
- All requests for additional data elements are scrutinized to ensure there are legitimate value propositions for inclusion.
- Each data element incorporated in ARIES is assessed and categorized. This exercise includes:
  - A determination on whether each element is mandatory or optional. If Optional, we perform an additional exercise to ensure relevance.
  - A determination of field characteristics. This includes establishing attributes such as field length, field type, and field business logic. Every effort is made to tighten the parameters for each field to restrict what can be entered and improve the validity and accuracy of the value.
  - The data element business logic will check across fields where associations exist. It will also automate the display of tier-two data elements that should only be presented based on the value selected on another related data element.
  - An additional determination is made as to the potential for incorporating lookup tables and/or drop-down lists for each data element. This is done to further restrict what can be entered/selected and improve data integrity. A significant percentage of data elements captured within ARIES are tied to formal lookup tables with

predetermined value sets.

- We have invested significantly in the sharing of data elements across the domains of Allegations, Investigations, and Enforcement. Moreover, we have focused on the movement of data across records and phases to ensure that each data value entered will not require reentry at a later point in the lifecycle.
- We have worked diligently to organize and group data elements in a manner that is logical to users. This gives much needed context for users and allows for quick population of multiple fields related to a single purpose.
- We are incorporating alt text for almost every data element to ensure users have the ability to received additional context about the purpose and requirements for data population.
- We will be developing data integrity report(s) that will track data entry patterns and raise awareness of issues related to the integrity of system data, including accuracy, completeness, and timeliness of data.

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

Yes, Production data from the legacy databases will be migrated in small data sets to Dev and Test environments to facilitate development and testing. Migration scripts are used to accomplish this need. Stakeholders performing testing can/will also add dummy data to facilitate the process. Dummy data will not be migrated forward to Staging or Production.

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

Information is initially provided in the form of a third-party contact in the form of emails, phone calls or in person contact regarding possible issues at facilities. Subsequent interviews will gather additional information regarding an Allegation, (e.g., personal information, additional witness information, facility information, etc.). Through later interactions the data can be updated by NRC personnel if necessary.

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).

Internal NRC, Administrators, Badged Contractors.

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.

ARIES does not integrate with any non-NRC partners or systems.

Identify what agreements are in place in the table below.

Agreement Type	
☐	Contract Provide Contract Number:
☐	License Provide License Information:
☐	Memorandum of Understanding Provide ADAMS ML number for MOU:
☐	Other

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

Badged system administrators will have access to the data vis the raw data table in Dataverse. All other access to the data is accomplished by interaction with ARIES by cleared NRC and contractor personnel. This access is restricted to need to know via role-based access (RBAC) based upon business rules provided by system Product Owners from all three business areas (Allegations, Investigations and Enforcements).

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 are encrypted at rest and in motion. Access to data from within ARIES is restricted to those with need to know via Role Based Access.

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

Power Platform Dataverse.

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

ARIES is a cloud based internal system accessible via Intranet URL. The system utilizes SSO and two factor authentication via PIV/PIN.

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

Yes, all team members are badged.

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

Every table and field can have auditing turned on for it. A field with auditing turned on has its change history logged based on who made the change and when. In terms of preventing misuse of data, there are authorization-based permissions applied to every user in the system that limits their abilities to see records that they are/aren't an owner of or given permission to. For PII information, field-column security is enabled, which has even more security applied as you need to both be given permissions to the record, and you need to be given the PII-specific security role to view the data.

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.

Business Application Support System (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**.**
☒	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.

N/A.

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.** Name, Organization, Date of Birth, Home or Cellular Number, Mailing Address, Professional Training, Social Security Number, Witness and Subject Names, Gender, Experience, Ethnicity, License Type, Education, Email Address, Biometric identifiers (Height, Weight, Hair Color, Eye Color, Scars, Tattoos, etc.), Title, Certifications
☐	**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):*** NRC 23, Case Management System – Indices, Files, and Associated 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?

Voluntary, system allows for anonymous contact if desired. Information is initially provided in the form of a third-party contact in the form of emails, phone calls or in person contact regarding possible issues at facilities. Subsequent interviews will gather additional information regarding an Allegation, (e.g., personal information, additional witness information, facility information, etc.)

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?

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

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)	ARIES see table below for Records Retention Schedules / Dispositions for ARIES which is based on the former Case Management System Web (CMS-W)
Records Retention Schedule Number(s)	See table below for Records Retention Schedules.
Approved Disposition Instructions	See table below for Dispositions.
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.	Manual 1. When files are uploaded to the system, they will always be association with a single record in the system. Record types include Contact, Case, Allegation, Investigation, Enforcement, Alternative Dispute Resolution, Concern, Entity, and Action. 2. In order to upload a file, a user must first be granted permission to access and edit a respective record. Most users who are granted permissions to edit a respective record will only be permitted to upload and edit files, but not delete them.

	3. In order to delete a file, a user must be given elevated permissions to the associated record. This permission will only be granted to a restricted number of users. (Elevated Roles include Admins, Supervisors, and Record Owners) 4. As authorized users will have the capability of deleting files, we intend to display a notification at the time of deletion informing users of NRC's retention policy and if it is appropriate to delete the respective document(s). Accompanying this notification, a user will be presented a secondary delete button requiring they confirm that the deletion of this file does not violate NRC policy. 5. As files are uploaded, they will be automatically tagged in accordance with the associated record they belong to. 6. Additionally, users will be given the opportunity to manually add metatags to assist them (and other users) with dispositioning. 7. Shortly after go-live, we intend to develop a report(s) to track the status of each record (and associated files), and notify users when milestones are reached requiring disposal. This report will serve as an interim means for supporting retention and disposal requirements. 8. After a series of priority enhancements are completed after go-live, we intend to develop a system component that will introduce semi-automated mechanisms supporting disposal. Although the exact nature of this envisioned component is not yet designed, it will serve as a mechanism for monitoring all closed records, calculating the requisite retention period for each record and each accompanying file (based on data captured on each record and file), and then triggering the automated disposal of records and/or files when respective retention periods are reached. Working with Stakeholders and Users, we will also explore the need for a notification to be generated prior to destruction allowing an Admin or User to

	approve the disposal or prevent it, if appropriate.
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	
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)**	

Schedule Number	Schedule Title	Disposition
NUREG 0910-2.10.2(a)(1) (page 2.10.5)	Enforcement Action Case Files. Significant Enforcement Actions	**Permanent**. Cut off files when case is closed. Transfer to NARA with indexes when 20 years. (Regions have the same retention)
NUREG 0910-2.10.2(b)(1) (page 2.10.5)	Enforcement Action Case Files. All other Enforcement Actions and Violations	**Temporary**. Cut off files when case is closed. Hold 2 years. Destroy 10 years after enforcement actions are cut off. (Regions have the same retention)
NUREG 0910- 2.16.1 (page 2.16.1)	Allegation and Inquiry Files	**Temporary**. Hold closed allegation case files in office 2 years. Destroy 10 years after cases are closed.
NUREG 0910- 2.17.1 (page 2.17.1) NUREG 0910- 2.18.1 (page 2.18.1)	Allegation Case Files	**Temporary.** Cut off files upon final resolution of allegation. Retain in office for 2 years or until no longer needed for current activities. Destroy 10 years after cutoff.
NUREG 0910-2.16.4.a (page 2.16.7)	Investigation Case Files (Significant)	**Permanent.** Cut off files when case is closed. Hold in field 6 months then forward to HQ. Hold for 2 years, Transfer in 10-year blocks which will be transferred at 10-year intervals.
NUREG 0910-2.16.4.b	Investigation Case Files	**Temporary.** Temporary. Cut off files when case is closed. Hold in field

(page 2.16.70	(Other case files that do not meet the criteria for permanent retention)	office for 6 months then forward to HQ. Hold for 2 years. Destroy 20 years after cases are closed.
GRS 5.2 item 020	Intermediary records This schedule is generally used to dispose of those records which are used to create a subsequent record, such as those manually input into a system.	**Temporary.** Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

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 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, OMB approval is not required for information collections during a Federal criminal investigation or prosecution, during a civil action to which the United States is a party, or during the conduct of intelligence activities.

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?

OMB approval is not needed for information collections made:

- During the conduct of a federal criminal investigation or prosecution, or during the disposition of a particular criminal matter.
- During the conduct of a civil action to which the United States or any official or agency thereof is a party, or during the conduct of an administrative action, investigation, or audit involving an agency against specific individuals or entities. However, the requirements of the Paperwork Reduction would apply during the conduct of general investigations or audits undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.

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.

STOP HERE - The remaining pages will be completed by the Privacy Officer, Records Management, and Information Collections Team.

8 Privacy Act Determination

Project/System Name: Allegations, Resolution, Investigation and Enforcement System (ARIES).

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:

NRC 23, Case Management System – Indices, Files, and Associated Records.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 12/14/23	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. Multi.

Comments:

ARIES itself does not need a clearance. The collections of information that is used to populate ARIES and do not fall under the exception in 5 CFR 1320.4 may be subject to the requirements of the Paperwork Reduction Act.   These collections may be covered by a number of existing OMB clearances.

Reviewer's Name	Title
Signed by Cullison, David on 12/11/23	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
Signed by Dove, Marna on 12/13/23	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 12/14/23

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

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Allegations, Resolution, Investigation and Enforcement System (ARIES)	
Date CISD received PIA for review: November 9, 2023	**Date CISD completed PIA review:** December 13, 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*	