Privacy Impact Assessment (PIA)

Name of Project: Archives Investigative Management System (AIMS) System

Project's Unique ID: AIMS

Legal Authority(ies):	**5 USC App 3**

Purpose of this System/Application: The Archives Investigative Management System is used by the Office of Investigations within the Office of Inspector General to manage, track, and report on all aspects of complaints and investigations reported to and initiated by the Office of Investigations.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Employees		There are numerous fields related to 'Individuals' not specifically employees. A type field indicates whether the individual is a NARA employee or private citizen, etc. These fields include first name, last name, address, telephone number, email address, organization, place of employment, and grade, (if applicable). Additionally, if the individual is the subject of a complaint or investigation, there are other fields in the system that are populated with information regarding that individual. These fields include legal action, conviction status, sentencing, etc. There are a number of fields where the user can enter textual information about the case which will include information about any individuals associated with the case.
External Users		Although there are no external users of the system, the information pertaining to volunteers, contractors or other individuals who are not employed with NARA may be the same as the elements described in the "Employees" entry above except that it will be recorded as individuals "Associated" with the investigation. The field indicating "Private Citizen" will be selected and the amount of information pertaining to the public citizen may vary based on what is made available for the investigation.
Audit trail information (including employee log-in information)		Every login/logout from the system, attempted login, or failed login to the system is captured in an audit log. Additionally every change made to an existing record in the system is captured in the audit log. Information on the user, time of use, and information added or deleted is captured.
Other (describe)		N/A

Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		Employees in the Office of Inspector General input information pertaining to the investigations are obtained from public citizens and employees.
External users		This system does not accept data from any other system.
Employees		This system does not accept data from any other system.
Other Federal agencies (list agency)		This system does not accept data from any other system.
State and local agencies (list agency)		This system does not accept data from any other system.
Other third party source		This system does not accept data from any other system.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

Yes. In order to effectively and accurately conduct an investigation the data elements defined in the system are necessary. Not all of the elements will relate to every investigation, but all of the elements will, at some time, relate to a particular investigation. Additionally, the elements in the system are required in order to support agency and Congressional reporting requirements.

2. Is there another source for the data? Explain how that source is or is not used?

The electronic case tracking system is the sole database used by the OIG to track investigative information. (FOR EXAMPLE The information is input into the system manually based on information derived from paper-based sources. Or the information is added to this databased derived from data pulled from "SYSTEM NAME" and then particular fields necessary to track the investigation are then added to this database.)

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

As a result of the investigative information the designated staff within the Office of General Counsel, which includes FOIA requests, or the Office of Inspector General are able to view the aggregate information which otherwise would not exist in this format.

2. Will the new data be placed in the individual's record?

N/A - see answer to question 1. In the event that an adverse action is taken against the employee based on information obtained in this system and requires inclusion to an individual record, the discipline process provides the employee the ability to review the information and FOIA allows for access by the public.

3. Can the system make determinations about employees/the public that would not be possible without the new data?
No.

4. How will the new data be verified for relevance and accuracy?
N/A - see answer to question 1.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
N/A - see answer to question 1.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
No processes are being consolidated in the system.

7. Generally, how will the data be retrieved by the user?
Data is retrieved via a program interface, which allows the user to query against the database for the information that they are looking for. Each user has a unique user ID and password. Different users have different access rights, which restrict their ability to edit specific types of cases.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.
The system has query capabilities, which allow the users to perform data searches. Data is retrievable by personal identifiers name, date of birth, address, telephone number, place of employment, and email address(es).

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

There are no reports in the system that are specific to an individual. Reports are based on queries linked to specific case numbers, but not individual names. The only people who have access to these reports are authorized users of the system. These reports are used to respond to Freedom of Information Act requests, Congressional requests, and other law-enforcement uses.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

No

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

No

12. What kinds of information are collected as a function of the monitoring of individuals?

N/A

13. What controls will be used to prevent unauthorized monitoring?

Every login/logout from the system, attempted login, or failed login to the system is captured in an audit log. Additionally every change made to an existing record in the system is captured in the audit log. Information on the user, time of use, and information added or deleted is captured.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

The system is not web based, but is rather housed on NARA's internal servers and systems. It is not available to users outside of the OIG.

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

System users, and contractors and developers who are authorized by contract by the OIG.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?

Access is determined by Application Administrators set within the system under the authority of the Assistant Inspector General for Investigations (AIGI). These controls are documented in the software's User Guide. Those Application Administrators can terminate access to the system as authorized by the AIGI.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

Each authorized system user is assigned a specific authorization level which determines that user's access to data. However, additional restrictions on information access can be instated as needed for individual system users.

System-level and network accounts for IO managed systems are managed according to the User Account Management SOP. This SOP identifies various account types and documents procedures for the following aspects of account management: 1) Account approval process 2) Establishing, activating, modifying, disabling, and removing accounts 3) Review and validation of accounts. Accounts are reviewed at least quarterly to make certain there are no users who have changed roles and or positions having unnecessary access and/or permissions.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?

Each authorized system user is assigned a specific authorization level which determines that user's access to data. However, additional restrictions on information access can be instated at need for individual system users. In addition, there are audit controls that track who has accessed or changed records in the system, and when they accessed them. These audit logs are available to the system administrator for review at any time period. While the administrator can review audit logs on an ad-hoc basis, typical review would be driven by suspected misuse.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, contractors are involved in the development and maintenance of the system. They have signed a non-disclosure agreement with the OIG.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.

No

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

N/A

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

N/A

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

N/A

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

Individuals submitting a complaint to the IG's office have the option of providing personal information, or having their information associated with the complaint. Individuals who are the subject of a complaint or investigation do not have an option with respect to the information collected about them in the system. This is a source system for the information collected and/or maintained in the application.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Individuals do not have direct access to AIMS, only NARA employees do. The system does not do this. This would be a process handled by the investigators and their supervisors within the OIG, who are authorized system users.

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

Since the nature of this system is to track data relating to complaints and investigations, the accuracy of the data in many cases is subjective. Information given by individuals initiating a complaint, subjects of investigations or witnesses is assumed to be accurate when it is given. Other data collected by the investigators as a result of the investigative process is also assumed to be accurate based on the information at hand. System users are mandated by the procedures outlined in the Special Agents' Handbook and the User Guide.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is only operated at one site in College Park, MD.

3. What are the retention periods of data in this system?

The maintenance and disposition of the records created by this system are directed by the applicable NARA records schedule, Chapter 12 – Investigate Case Files 1208-1, 1208-2, 1208-3

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

The disposition of the records created by this system is specified by the applicable NARA records schedule, published in The Federal Register. Records will be purged when deemed they will no longer be needed, utilizing IT scripts.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

No

6. How does the use of this technology affect public/employee privacy?

N/A

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

Yes

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

Yes - NARA IT performs monthly vulnerability and risk-assessment scans. These reports are reviewed and appropriate actions are taken based upon findings.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

NARA IT performs monthly vulnerability and risk-assessment scans. These reports are reviewed and appropriate actions are taken based upon findings.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Jason Metrick (OIG)
Assistant Inspector General for Investigations
Jason.Metrick@nara.gov
301-837-2941

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

This system operates under NARA 23, Office of Inspector General Investigative Case files.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

No

2. If so, what changes were made to the system/application to compensate?

N/A

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager

Privacy Act Officer

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
(Signature)	7/8/19 (Date)
Name: Jason Metrick	
Title: Assistant Inspector General for Investigations	
Contact information: 8601 Adelphi Road, Room 1320, College Park, MD 20740-6001 301-837-2941, jason.metrick@nara.gov	
Senior Agency Official for Privacy (or designee)	
(Signature)	6/7/19 (Date)
Name: Gary M. Stern	
Title: Senior Agency Official for Privacy	
Contact information: 8601 Adelphi Road, Room 3110, College Park, MD 20740-6001 301-837-3026, garym.stern@nara.gov	
Chief Information Officer (or designee)	
Swarnali Haldar (Signature)	8/29/2019 (Date)
Name: Swarnali Haldar	
Title: Executive for Information Services/CIO (I)	
Contact information: 8601 Adelphi Road, Room 4415, College Park, MD 20740-6001 301-837-1583, swarnali.haldar@nara.gov	