Privacy Impact Assessment

Name of Project: Inspector General Case Management & Tracking System
Project's Unique ID: IGCMTS

Legal Authority(ies): 5 U.S C App. 3

Purpose of this System/Application:

The IG Case Management and Tracking 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:

a. Employees

There are numerous fields related to 'Individuals' not specifically employees. A type field indicates if the individual is a NARA employee or public citizen, etc. These fields include first name, last name, address, phone number, email address, organization, grade. (if applicable). Additionally, if the individual is the subject of a complaint or investigation, there are other areas of the system that are populated with information regarding the individual. These fields include legal action, conviction status, sentence, etc. There are a number of fields where the user can enter textual information about the case which will include information about the individual associated with the case.

b. External Users

There are no external users of the system.

c. 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. These logs are kept indefinitely.

d. Other (describe)

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

a. NARA operational records
b. External users
c. Employees
d. Other Federal agencies (list agency)

e. State and local agencies (list agency)
f. Other third party source

This system does not accept data from any other system, however it does allow authorized users to upload documents of any kind (Word, Excel, PDF, Text, etc.) into the system and associate them with a complaint or an investigation.

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?**
   Paper files are kept for each case in the system.

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?
No, this does not happen in the system.

2. Will the new data be placed in the individual's record?
N/A – see answer to question 1.

3. Can the system make determinations about employees/the public that would not be possible without the new data?
N/A – see answer to question 1.

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, and they are required to change their password every 90 days. Different users have different access rights, which restrict their ability to either edit or see 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 extensive query capabilities, which allow the users to perform data searches on any data element in the system. Typically, searches are performed on a name or case number.

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 Cases (Complaints or Investigations) which have individuals tied to them. The only people that have access to theses reports are authorized users of the system. The system audit logs are not specific reports, but can be printed if desired. These logs track all activity in the system including logins and logouts, attempted logins, cases viewed, cases updated and the before and after data. The reports are used to provide statutorily required information and data to Congress.

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?

NA

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

NA

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

The system is web based, but does not use persistent cookies or other tracking devises to identify web visitors. The system is not available outside of NARA, in fact, the system is not available outside of the OIG's physical office space, it is restricted to a specific subnet.

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)?

The only people that access the system are members of the OIG's office. The system administrator is the AIGI who is part of the OIG's office.

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.).

User access is determined and granted by the Assistant Inspector General for Investigations (AIGI). These controls are documented in the System Requirements Specification document.

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

There are some cases that are restricted and will be labeled as such. Based on user access some users will not be able to see these cases, or know that they even exist Additionally access to the system user information is restricted to the system administrator. If cases are marked 'OIG Sensitive', only the primary investigator and the AIGI will have access to them. Additionally there is a user role that is used by the receptionist to enter complaints received into the system. This role only has access to Complaint data, but not investigations.

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)?

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. 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. The have signed a non-disclosure agreement with the OIG, and have security clearances. While contractors are involved in the development and maintenance of the system, they do not have access to the production system or the data. They have a copy of the system at their office that does not contain any NARA data which they use to troubleshoot the system.

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?

NA

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

NA

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.

NA

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. Granting consent is verbal. 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.

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

The system does not do this. This would be a process handled by the investigators within the OIG.

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. There is a requirement that complaints and investigations be closed within a specific number of days from the time that they were opened. The system tracks these dates and reports are generated to determine the status of open cases.

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?

System is only used at one site.

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

Records are divided into Complaints and Investigations. Nearly all investigative case files are temporary records and are destroyed in accordance with the disposition instructions in the

NARA records schedule contained in FILES 203, the NARA Files Maintenance and Records Disposition Manual. However, the retention and disposal of significant investigative case files, such as those that result in national media attention, congressional investigation, and/or *substantive changes in agency policy or procedure, are determined on a case-by-case basis..*

1208	**Investigative Case Files**	
	Case files developed during investigations of known or alleged fraud and abuse and irregularities and violations of laws and regulations Cases relate to agency personnel, programs, and operations administered or financed by the agency, including contractors and others having a relationship with the agency This includes investigative files relating to employee and hot line complaints and other miscellaneous complaint files Files consist of investigative reports and related documents, such as correspondence, notes, attachments, and working papers	
1208-1	Files containing information or allegations which are of an investigative nature but do NOT relate to a specific investigation They include anonymous or vague allegations not warranting an investigation, matters referred to constituents or other agencies for handling, and support files providing general information which may prove useful in investigations	Cut off annually Destroy when 15 years old (N1-64-00-4, item 2a)
1208-2	All other investigative case files EXCEPT those that are unusually significant for documenting major violations of criminal law or ethical standards by agency officials or others (see "NOTE")	Place in inactive file when case is closed Cut off inactive file at the end of the fiscal year Destroy 15 years after cutoff (N1-64-00-4, item 2b)
	NOTE Significant case files (i e , those that result in national media attention, congressional investigation, and/or substantive changes in agency policy or procedure) are NOT covered by Schedule #N1-64-00-4 Cut off inactive file at end of fiscal year, hold 5 years, and submit an SF 115 to the Lifecycle Management Division (NWML), via the NARA Records Officer (NARA will determine the disposition on a case-by-case basis.)	
1209	**Indexes to Case Files**	
	Indexes and registers used as references to investigative and audit case files	Destroy or delete with the related records (GRS 23, item 9)

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.

Removing records from the system at the end of the retention period is performed by running scripts against the database that will delete records based on a specific case number or date range, whichever is specified. These instructions are part of the System Requirements Specification (CMTS-SRS final v2.doc). System generated reports are destroyed when no longer needed.

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?

NA

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?

An analysis of the system threat environment was completed in September 2007 as part of the NARA IT Contingency Plan. This analysis identified boilerplate threat sources (natural, environmental/physical, and human), however, since the CMTS is not a mission critical system, no additional controls or procedures were enacted and none are presently deemed necessary.

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

A system security plan was conducted on this system in July 2006. Under the plan, risk assessments are done subsequent to any significant modification or every three years at a minimum.

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

Tom Bennett, Computer Forensic Analyst, OIG, 301-837-0364

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?

NA

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

______________ (Signature) 8/29/08 (Date)
System Manager, (Please include name, title and contact information)

for Leo Scanlon

______________ (Signature) 9/5/08 (Date)
IT Security Officer, (Please include name, title and contact information)

______________ (Signature) 9/3/08 (Date)
Senior Agency Official for Privacy, (Please include name, title and contact information)

______________ (Signature) 9/5/08 (Date)
Chief Information Officer, (Please include name, title and contact information)