Treasury Office of Inspector General (OIG) Privacy Impact Assessment (PIA)

Name of System: OIG General Support System (OGSS)

Date of Submission: 01/07/2009

Contact:
John Czajkowski, Assistant Inspector General for Management/CIO, OIG, 202-927-5835,
czajkowskij@oig.treas.gov

Dee Thompson, Director IT, OIG, 202-927-5883
thompsond@oig.treas.gov

1. **What is the purpose of the system?**

The Office of Inspector General (OIG) General Support System (OGSS) is the system infrastructure which provides data access and the computing services for OIG's Audit and Investigations business functions and allows them to perform their mission. OGSS promotes productivity and efficiency by giving the users access to automated tools that are utilized in the performance of duties. The system consists of data extracts from various electronic systems maintained by governmental agencies and other entities. The data is used for audit and investigative purposes and is necessary to identify and prevent fraud, waste, and abuse in the programs and operations of the Department of the Treasury and related entities as well as to promote economy, efficiency, and integrity in the administration of all applicable laws and deter wrongdoing by Treasury and OIG employees or contractors.

2. What legal authority authorizes the purchase or development of this system?

The nature and scope of OIG's oversight and investigative responsibilities are established and set forth in the Inspector General Act of 1978, as Amended, 5 U.S.C.A. Appendix 3; 5 U.S.C. 301; 31 U.S.C. 321 and Treasury Order 114-01. In order to enable OIG to perform its oversight and investigative functions, the Inspector General Act of 1978 authorizes OIG to have access to "all record, reports, audits, reviews, documents, papers, recommendations, or other material" maintained by the Treasury Department.

3. Under which Privacy Act SORN does the system operate?

Treasury/DO 191: OIG Management Information System (MIS)

4. What categories of individuals are covered by the data in the system?

See attached PIAs.

5. What are the sources of information in the system?

See attached PIAs.

6. How the data is in the system verified for accuracy, timeliness, and reliability?

See attached PIAs.

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

See attached PIAs.

8. What are the retention periods and the procedures for disposition of the data in the system?

See attached PIAs.

9. Will this system provide the capability to identify, locate, and monitor individuals?

See attached PIAs.

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

OIG has various policy directives in place to ensure the integrity, availability and confidentiality of data stored in the OGSS. OIG employees should always verify that the request of accessing data has been authorized. All OIG employees are required to undergo yearly security, privacy and ethics training. System access is monitored closely and if a user or an administrator violates the organization's security policies they are subject to disciplinary action, up to and including termination of employment. OGSS users, administrators, and other personnel protect OIG from unwanted access and are on the front line in the organization's ability to respond to incidents.

11. Who will have access to the data in the system and what controls are in place to prevent misuse?

OGSS is an internal system that is not accessible by the public. The OGSS contains sensitive data that needs to be protected and guarded to the maximum extent possible. Everyone who has been granted access to the system is responsible for providing the level of protection warranted by the classification of the information and material in his or her possession or control.
The Privacy Officer, System Owners, Managers and everyone in OIG who has access to the data are responsible for assuring the proper use of the data. System access for users, developers, and administrators accounts will be restricted to the functionality needed by the employee to perform his or her job. For data files that are deemed sensitive for general access additional preventative controls have been built into applications to provide additional restrictions to user access.

The Following Officials Have Approved this Document

1. **Program Manager**

/s/ **(Signature)**

Name Dee Thompson **Title** Assistant Inspector General for Management

2. **Information Systems Security Manager**

/s/ **(Signature)**

Name Ernest Eldredge **Title** Information Systems Security Officer

3. **Privacy Act Officer**

/s/ **(Signature)**

Name R.K. Delmar **Title** Counsel to the Inspector General

4. **IT Review Official**

/s/ **(Signature)**

Name Dee Thompson **Title** Director of Information Technology

5. **Chief Information Officer Official (when necessary)**

/s/ **(Signature)**

Name John Czajkowski **Title** Assistant Inspector General for Management

Attachment I to OIG Privacy Impact Assessment (PIA)

Chapter III: Privacy Impact Assessment Template
(Derived from the Department of the Treasury Privacy Impact Assessment Manual TD P 25-07, July 2006 Advance Copy)

Once completed provide copies of the PIA to the following:

- Office of Management and Budget (OMB) Exhibit 300 Submission (when required)
- Bureau Privacy Act Officer
- Bureau Information Systems Security Manager
- Treasury's Office of the Chief Information Officer

Also refer to the signature approval page at the end of this document.

A. **Contact Information:**

Name of System, Project or Program: Office of Inspector General Office of Counsel Case Tracking System (OCCTS)
OMB Unique Identifier: (*if appropriate)*

1. **Who is the person completing this document?**

Cynthia A. Langwiser, Assistant Counsel, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-5869, LangwiserC@oig.treas.gov.

2. **Who is the system owner?**

R.K. Delmar, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, DelmarR@oig.treas.gov.

3. **Who is the system manager for this system or application?**

R.K. Delmar, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, DelmarR@oig.treas.gov.

4. **Who is the Information Systems Security Manager who reviewed this document?** (Name, organization, and contact information).

Ernest Eldredge, Information Systems Security Officer, U.S. Department of the Treasury, Office of Inspector General, Office of Information Technology, (202) 927-5753, EldredgeE@oig.treas.gov.

5. **Who is the Bureau Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).

R.K. Delmar, Counsel to the Inspector General, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, DelmarR@oig.treas.gov.

6. **Who is the IT Reviewing Official?** (Name, organization, and contact information).

Dee Thompson, Director of Information Technology, U.S. Department of the Treasury, Office of Inspector General, Office of Management, Office of Information Technology, (202) 927-5883, ThompsonD@oig.treas.gov.

B. **System Application/General Information:**

1. **Does this system contain any information in identifiable form?**

The system contains personal information about individuals, e.g., name, home and work telephone and fax numbers, e-mail addresses, and other pertinent information related to pending casework in the Office of Counsel, including the processing of Giglio requests.

2. **What is the purpose of the system/application?**

The primary purpose of this system is to facilitate the manageability and efficiency of casework handled by the Office of Counsel. The system will allow the tracking of case assignments from receipt to completion, provide valuable information to OIG staff working in the Office of Counsel provide internal reports, and improve customer service.

3. **What legal authority authorizes the purchase or development of this system/application?**

5 USCS Appx § 6

4. **Under which Privacy Act SORN does the system operate**? **Provide the number and name.**

TREASURY/DO .191: OIG Management Information System (MIS)

C. **Data in the System:**

1. What categories of individuals are covered in the system?

Individuals who make or are the subject of Giglio requests, individuals who are the complainants, appellants or the plaintiffs in EEO, MSPB or Federal Court litigation, individuals who are witnesses or contacts in litigation, OIG employees who request ethics or other legal advice.

2. What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information in this system comes primarily from the individuals who make requests for ethics or legal advice, individuals who make Giglio requests, individuals who are complainants, appellants, and plaintiffs, respectively, in EEO, MSPB, and Federal Court litigation and employees handling cases.

b. What Federal agencies are providing data for use in the system?

None other than United States Attorney Offices who make Giglio requests.

c. What State and/or local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None other than United States Attorney Offices who make Giglio requests.

e. What information will be collected from the employee and the public?

Information collected will include, but not be limited to: name, home/business address; home/business telephone number; fax and e-mail numbers; organizational affiliation; date of requests; subject of requests; other information related to processing and responding to requests, disposition of Giglio requests, requests for ethics and other legal advice, and litigation.

3. Accuracy, Timeliness, and Reliability

All staff handling case work in the Office of Counsel will be responsible for ensuring that information entered into the system is accurate and complete. Information will be entered in a timely manner and updated in the system as appropriate.

a. How will data collected from sources other than bureau records be verified for accuracy?

Information is only as reliable as provided by requestors in the case of Giglio requests and requests for legal and ethics advice.

b. How will data be checked for completeness?

Information is only as reliable as provided by requestors in the case of Giglio requests, litigation and requests for legal and ethics advice.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Information is only as reliable as provided by requestors in the case of Giglio requests and requests for legal and ethics advice.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The OCCTS is comprised of specific data fields. These fields are described in detailed in a User Guide prepared by the contractor. In addition, specific guidance regarding data entry for specific fields is included in the User Guide.

D. **Attributes of the Data:**

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

The information collected in the OCCTS is necessary and is directly related to the reason for which the system has been designed.

2. 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.

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

No.

4. Can the system make determinations about employees/public that would not be possible without the new data?

No.

5. How will the new data be verified for relevance and accuracy?

N/A

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The data in the system is not being consolidated.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Access to the OCCTS will only be granted to those persons within the Office of Counsel, OIG. Access levels and permission levels have been established by the OIG and authorized only to those persons who have a need to know the information contained in a system in order to carry out their duties. In accordance with OMB Circulars A-123, and A-130, Appendix III, the OCCTS will have controls in place to prevent the unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

8. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data will be retrieved by various fields including, case complainant, complainant address and case contacts.

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

Reports will not be produced on individuals.

E. **Maintenance and Administrative Controls:**

1. 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 user's manual and guidelines will ensure consistent use of the data in all sites.

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

The retention periods of data/records in the system are covered by General Records Schedules (GRS) 14 and 20. The OIG also follow guidance on permanent and

temporary records disposition issued by the National Archives Records Administration (NARA).

3. 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?

Procedures for eliminating the data at the end of the retention are established in accordance with GRS 14 and 20 or NARA guidance.

4. Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

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

There is no new use of technology that would affect privacy.

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

While some data will allow the identification of individuals, the system is not configured to monitor any individuals.

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

N/A.

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

The system is only accessible by those OIG employees who have been assigned usernames and passwords.

9. Under which Privacy Act SORN does the system operate? Provide number and name.

TREASURY/DO .191: OIG Management Information System (MIS)

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

The changes made to this system does not require amendment or revision to the Privacy Act SORN.

F. **Access to Data:**

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

Users of the system will include: system managers, attorneys and other employees of the OIG who have a need to know the information contained in this system in order to carry out their duties. The System Administrator will have access to the data in the system as necessary to carry out his/her responsibilities. The routine use section of the Privacy Act system of records notice, TREASURY/DO .191, identifies those parties that can gain access to the information when the use is compatible with that identified in the notice.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

For the most part, access to the data by a user is determined by the "need-to-know" requirements of the Privacy Act, the users profile based on the user's job requirements, managerial decisions, etc. and dependent on a compatible purpose for which the data was collected.

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

Access to records in the system is limited to authorized personnel whose official duties require such access, i.e., all in a "need to know" basis. Electronic data is protected through user identification, passwords, database permissions and software controls.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

In accordance with OMB Circulars A123, and A-130, Appendix III, the electronic OCCTS system will have controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All users have a password and ID that is issued by the OIG's Office of Information Technology. All users received training on the OCCTS.

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, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

Yes, contractors were involved with the design and development of the system and were involved with the initial maintenance of the system. As far as I can tell a Privacy Act clause was not included as part of the statement of work. I do not know if the contractor was provided with copies of the Department's Privacy Act regulations. As of 1 October 2008 the contractor is no longer involved in the maintenance or development of the system. Any upgrades will be handled by the OIG IT staff.

6. Do other systems share data or have access to the data in the system? If yes, explain.

No, the OCCTS is a closed system.

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

There is no interface. Although all employees who have access to information in a Privacy Act system have responsibility for protecting personal information covered by the Privacy Act (see 31 CFR 1.28**,** Training, rules of conduct, penalties for non-compliance), the information owner and system manager share overall responsibility for protecting the privacy rights of individuals by following Treasury Directive 71-10 along with the Department of the Treasury Security Manual.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

Other agencies will not share or have access to the data in the system.

9. How will the data be used by the other agency?

N/A

10. Who is responsible for assuring proper use of the data?

The Counsel to the Inspector General.

The Following Officials Have Approved this Document

1. Program Manager

/s/ **(Signature)**

Name R. K. Delmar **Title** Counsel to the Inspector General

2. System Manager

/s/ **(Signature)**

Name R. K. Delmar **Title** Counsel to the Inspector General

3. Information Systems Security Manager

/s/ **(Signature)**

Name Ernest Eldredge **Title** Information Systems Security Officer

4. Privacy Act Officer

/s/ **(Signature)**

Name R.K. Delmar **Title** Counsel to the Inspector General

5. IT Review Official

/s/ **(Signature)**

Name Dee Thompson **Title** Director of Information Technology

6. Chief Information Officer Official (when necessary)

/s/ **(Signature)**

Name John Czajkowski **Title** Assistant Inspector General for Management

Attachment II to OIG Privacy Impact Assessment (PIA)

Chapter III: Privacy Impact Assessment Template
(Derived from the Department of the Treasury Privacy Impact Assessment Manual TD P 25-07, July 2006 Advance Copy)

Once completed provide copies of the PIA to the following:

- Office of Management and Budget (OMB) Exhibit 300 Submission (when required)
- Bureau Privacy Act Officer
- Bureau Information Systems Security Manager
- Treasury's Office of the Chief Information Officer

Also refer to the signature approval page at the end of this document.

A. **Contact Information:**

Name of System, Project or Program: Office of Inspector General Electronic FOIA Tracking System (EFTS)
OMB Unique Identifier: (*if appropriate)*

1. **Who is the person completing this document?**

Deborah E. Butler, Paralegal Specialist, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-5012, ButlerD@oig.treas.gov.

2. **Who is the system owner?**

R.K. Delmar, Counsel to the Inspector General, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, DelmarR@oig.treas.gov.

3. **Who is the system manager for this system or application?**

Deborah E. Butler, Paralegal Specialist, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-5012, ButlerD@oig.treas.gov.

4. **Who is the Information Systems Security Manager who reviewed this document?**

Ernest Eldredge, Information Systems Security Officer, U.S. Department of the Treasury, Office of Inspector General, Office of Information Technology, (202) 927-5753, EldredgeE@oig.treas.gov.

5. **Who is the Bureau Privacy Act Officer who reviewed this document?**

R.K. Delmar, Counsel to the Inspector General, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, DelmarR@oig.treas.gov.

6. **Who is the IT Reviewing Official?**

Dee Thompson, Director of Information Technology, U.S. Department of the Treasury, Office of Inspector General, Office of Management, Office of Information Technology, (202) 927-5883, ThompsonD@oig.treas.gov.

B. **System Application/General Information:**

1. **Does this system contain any information in identifiable form?**

The system contains personal information about individuals, e.g., name, home address, home telephone and fax numbers, personal e-mail address, and other pertinent information related to processing and responding to their FOIA and Privacy Act requests.

2. **What is the purpose of the system/application?**

The primary purpose of this system is to facilitate the manageability and efficiency of the FOIA and Privacy Act (PA) process in the Office of Inspector General, Office of Counsel. The system will allow the tracking of FOIA/PA requests from receipt to completion, provide valuable information to OIG staff working with the FOIA/PA programs, help to identify duplicate requests, action taken on FOIA/PA requests, appeals, and litigation, provide internal reports, and improve customer service.

3. **What legal authority authorizes the purchase or development of this system/application?**

5 U.S.C. 552; 5 U.S.C. 552a

4. **Under which Privacy Act SORN does the system operate**? **Provide the number and name.**

Treasury .004 – Freedom of Information Act/Privacy Act Request Records—Treasury.

C. **Data in the System:**

1. What categories of individuals are covered in the system?

Individuals who have submitted FOIA/PA requests and administrative appeals; individuals whose requests or records have been referred to the OIG by other agencies; and in some instances attorneys representing individuals submitting such requests, appeals and litigation; individuals who are the subject of such requests, appeals, litigation, and/or the OIG personnel assigned to handle such requests, appeals and litigation.

2. What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information in this system comes primarily from the individuals who submit FOIA/Privacy Act requests, internally generated documents, and employees processing the requests.

b. What Federal agencies are providing data for use in the system?

None other than those which may be in the FOIA case files.

c. What State and/or local agencies are providing data for use in the system?

None other than those which may be in the FOIA case files.

d. From what other third party sources will data be collected?

None other than those which may be in the FOIA case files.

e. What information will be collected from the employee and the public?

Information collected will include, but not be limited to: name, home/business address; home/business telephone number; fax and e-mail numbers; organizational affiliation; the name and grade of the employee processing and reviewing the FOIA requests; the number of hours the employee spent in processing and reviewing the FOIA requests; date of requests; subject of requests; pertinent information associated with Bureau contact information when referring documents to other agencies; other information related to processing and responding to requests, e.g., disposition of requests.

3. Accuracy, Timeliness, and Reliability

All staff processing FOIA requests will be responsible for ensuring that information entered into the system is accurate and complete. Information will be entered in a timely manner and updated in the system as appropriate.

a. How will data collected from sources other than bureau records be verified for accuracy?

Information is received from individual FOIA/PA requesters and is only as reliable as that provided by the requester.

b. How will data be checked for completeness?

Information is first received from the Departmental Disclosure Office from individual FOIA/PA requesters and is only as reliable as that provided by the requester.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Information is received from individual FOIA/PA requesters and is only as reliable and current as that provided by the requester.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The EFTS is comprised of specific data fields. These fields are described in detail in a User Guide prepared by the contractor. In addition, specific guidance regarding data entry for specific fields is included in the User Guide.

D. **Attributes of the Data:**

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

The information collected in the EFTS is necessary and is directly related to the reason for which the system has been designed. The majority of the data elements are required for preparation and submission of the FOIA annual report to Congress (5 U.S.C. 552(e)).

2. 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?

Yes. The system will allow users through reports to aggregate information about requesters with regard to the number and nature of the FOIA/PA requests they have submitted to the OIG in the year of submission.

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

No. The data will be maintained in the EFTS.

4. Can the system make determinations about employees/public that would not be possible without the new data?

Yes, through the use of the system, the OIG will be able to determine what records have been created and completed by users in the system.

5. How will the new data be verified for relevance and accuracy?

Information is received from individual FOIA/PA requesters and is only as reliable as that provided by the requester.

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The system consolidates the information provided by requesters and users for the express purpose of providing computerized reports. No privacy information is consolidated in this system or reports from the system, only general statistical information pertaining to FOIA activities, i.e., number of days spent processing requests.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Access to the EFTS will only be granted to those persons within the OIG involved in working on FOIA requests. Access levels and permission levels have been established by the OIG and authorized only to those persons who have a need to know the information contained in a system in order to carry out their duties. In accordance with OMB Circulars A-123 and A-130, Appendix III, the electronic FOIA tracking system will have controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

8. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data that will be retrieved by various fields including, name of requester, date of request, subject of request, FOIA number and/or the organizational affiliation of the requester, etc.

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

The system will be able to produce reports using various parameters determined by the user limited to only the information that has been provided by the requester. The reports will enable the user to determine certain information regarding the request submitted including types of requests, categories of requests, numbers of requests, dates pertinent to requests, number of hours used to process requests, etc. This information will only be accessible to the users of the EFTS.

E. **Maintenance and Administrative Controls:**

1. 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 user's manual and guidelines will ensure consistent use of the data in all sites.

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

The retention periods of data/records in the system are covered by General Records Schedules (GRS) 14 and 20. The OIG also follow guidance on permanent and temporary records disposition issued by the National Archives and Records Administration (NARA).

3. 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?

Procedures for eliminating the data at the end of the retention period are established in accordance with GRS 14 and 20 or NARA guidance.

4. Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

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

There is no new use of technology that would affect privacy.

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

While some data will allow the identification of individuals, the system is not configured to monitor any individuals.

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

N/A.

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

The system is only accessible by those OIG employees who have been assigned usernames and passwords.

9. Under which Privacy Act SORN does the system operate? Provide number and name.

Treasury .004, Freedom of Information Act/Privacy Act Requests Records – Treasury.

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

The changes made to this system do not require amendment or revision to the Privacy Act SORN.

F. **Access to Data:**

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

Users of the system will include: FOIA/PA officers and coordinators, system managers, attorneys and other employees of the OIG who have a need to know the information contained in this system in order to carry out their duties. The System Administrator will have access to the data in the system as necessary to carry out his/her responsibilities. In certain instances, the contractor performing the work on the OIG's behalf may have access to records in the system. The routine use section of the Privacy Act system of records notice, Treasury .004, identifies those parties that can gain access to the information when the use is compatible with that identified in the notice.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

For the most part, access to the data by a user (i.e., OIG employees who are designated as FOIA/Privacy Act personnel and, as such, require access to the database to administer the laws) is determined by the "need-to-know" requirements of the Privacy Act, the users profile based on the user's job requirements, managerial decisions, etc. and dependent on a compatible purpose for which the data was collected. The criteria, procedures, controls and responsibility regarding access are documented by audit trials and system logs.

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

Access to records in the system is limited to authorized personnel whose official duties require such access, i.e., all in a "need to know" basis. Electronic data is protected through user identification, passwords, database permissions and software controls. Counsel employees working on FOIA cases will have access to all data.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

In accordance with OMB Circulars A-123, and A-130, Appendix III, the electronic FOIA tracking system will have controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All users have a password and ID that is issued by the OIG's Office of Information Technology. All users received training on the EFTS. In addition, the contractor developed a user's manual to provide guidance to the FOIA personnel who will be regular users of the system.

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, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

Yes, contractors are involved with the design and development of the system and were involved with the maintenance of the system contract. As far as I can tell a Privacy Act clause was not included as part of the statement of work. I do not know if the contractor was provided with copies of the Department's Privacy Act regulations. As of October 1, 2008 the contractor is no longer involved in the maintenance or development of the system. Any upgrades will be handled by the OIG IT staff.

6. Do other systems share data or have access to the data in the system? If yes, explain.

No, the EFTS is a closed system.

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

There is no interface. Although all employees who have access to information in a Privacy Act system have some responsibility for protecting personal information covered by the Privacy Act (see 31 CFR 1.28**,** Training, rules of conduct, penalties for non-compliance), the information owner and system manager share overall responsibility for protecting the privacy rights of individuals by following Treasury Directive 71-10 along with the Department of the Treasury Security Manual.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

Information from this system will only be shared with other agencies consistent with the FOIA/PA statutory exceptions in the routine uses set forth in the privacy act system of records notice, Treasury .004, Freedom of information act/privacy act requester records—Treasury.

9. How will the data be used by the other agency?

Access will only be provided to those parties identified in the routine use section of the privacy act system of records notice, Treasury .004, Freedom of Information Act/Privacy Act requester records—Treasury.

10. Who is responsible for assuring proper use of the data?

The Counsel to the Inspector General and FOIA/PA coordinators.

The Following Officials Have Approved this Document

1. Program Manager

/s/ **(Signature)**

Name R. K. Delmar **Title** Counsel to the Inspector General

2. System Manager

/s/ **(Signature)**

Name Deborah E. Butler **Title** Paralegal Specialist

3. Information Systems Security Manager

/s/ **(Signature)**

Name Ernest Eldredge **Title** Information Systems Security Officer

4. Privacy Act Officer

/s/ **(Signature)**

Name R. K. Delmar **Title** Counsel to the Inspector General

5. IT Review Official

/s/ **(Signature)**

Name Dee Thompson **Title** Director of Information Technology

6. Chief Information Officer Official (when necessary)

/s/ **(Signature)**

Name John Czajkowski **Title** Assistant Inspector General for Management

Attachment III to OIG Privacy Impact Assessment (PIA)

Chapter III: Privacy Impact Assessment
(Derived from the Department of the Treasury Privacy Impact Assessment Manual TD P 25-07, July 2006 Advance Copy)

Once completed provide copies of the PIA to the following:

- Office of Management and Budget (OMB) Exhibit 300 Submission (when required)
- Bureau Privacy Act Officer
- Bureau Information Systems Security Manager
- Treasury's Office of the Chief Information Officer

Also refer to the signature approval page at the end of this document.

A. **Contact Information:**

Name of System, Project or Program: Office of Investigations, Case Management System

OMB Unique Identifier: (*if appropriate)*

1. **Who is the person completing this document?**

David S. Smith, Special Agent in Charge, U.S. Department of the Treasury, Office of Inspector General, Office of Investigations, (202) 927-0315, smithd@oig.treas.gov.

2. **Who is the system owner?**

Matthew Issman, Assistant Inspector General for Investigations, U.S. Department of the Treasury, Office of Inspector General, Office of Investigations, (202) 927-5260, issmanm@oig.treas.gov.

3. **Who is the system manager for this system or application?**

David S. Smith, Special Agent in Charge, U.S. Department of the Treasury, Office of Inspector General, Office of Investigations, (202) 927-0315, smithd@oig.treas.gov.

Who is the Information Systems Security Manager who reviewed this document?

Ernie Eldredge, Information Systems Security Office, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-5753, eldredgee@oig.treas.gov.

4. Who is the Bureau Privacy Act Officer who reviewed this document?

Richard K. Delmar, Counsel to the Inspector General, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, delmarr@oig.treas.gov.

5. Who is the IT Reviewing Official?

Dee Thompson, Director of Information Technology, U.S. Department of the Treasury, Office of Inspector General, Office of Management, (202) 927-5883, thompsond@oig.treas.gov.

B. **System Application/General Information:**

1. Does this system contain any information in identifiable form?

The system contains personal information about individuals, e.g., name, home address, home telephone and fax numbers, personal e-mail address, and other pertinent information related to processing and responding to receipt of, investigations of allegations pertaining to the Department of Treasury.

2. What is the purpose of the system/application?

The records and information collected and maintained in this system are used to (a) receive allegations of violations of the standards of ethical conduct for employees of the Executive Branch (5 CFR part 2635), the Treasury Department's supplemental standards of ethical conduct (5 CFR part 3101), the Treasury Department's rules of conduct (31 CFR part 0), the Office of Personnel Management merit system principles, or any other criminal or civil law; and to (b) prove or disprove allegations which the OIG receives that are made against Department of the Treasury employees, contractors and other individuals associated with the Department of the Treasury.

3. What legal authority authorizes the purchase or development of this system/application?

The Inspector General Act of 1978, as Amended, 5 U.S.C.A. App.3; 5 U.S.C. 301; 31 U.S.C. 321.

4. Under which Privacy Act SORN does the system operate? Provide the number and name.

TREAS/DO .190; to be amended to reflect the title change of the database only.

C. **Data in the System:**

1. What categories of individuals are covered in the system?

(A) Current and former employees and contractors of the Department of the Treasury and persons whose association with current and former employees relate to the alleged violations of the rules of ethical conduct for employees of the Executive Branch, the Department's supplemental standards of ethical conduct, the Department's rules of conduct, merit system principles, or any other criminal or civil misconduct, which affects the integrity or facilities of the Department of Treasury. The names of individuals and the files in their names may be: (1) Received by referral; or (2) initiated at the discretion of the Office of the Inspector General in the conduct of assigned duties.

(B) Individuals who are: Witnesses; complainants; confidential or non-confidential informants; suspects; defendants; parties who have been identified by the Office of the Inspector General, constituent units of the Department of Treasury, other agencies, or members of the general public in connection with the authorized functions of the Inspector General.

(C) Current and former senior Treasury and bureau officials who are the subject of investigations initiated and conducted by the Office of the Inspector General.

2. What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information in this system comes primarily from the individuals who submit hotline and other allegations, internally generated documents, and from employees processing the requests. There is also integration with data from the Treasury Human Resources Information System (HRIS), the Treasury Integrated Management Information System (TIMIS), the Treasury Enforcement Communications System (TECS) and AutoTrackXP.

b. What Federal agencies are providing data for use in the system?

Treasury offices and bureaus, Homeland Security and Justice Departments, and OPM.

c. What State and/or local agencies are providing data for use in the system?

Varies depending on particulars of case, but primarily state and local police and investigative agencies, and personnel agencies.

d. From what other third party sources will data be collected?

Varies depending on particulars of case, but generally private employers, schools, and other entities and individuals with knowledge of subjects and incidents under investigation.

Integration with data from HRIS/TIMIS, TECS and AutoTrackXP.

e. What information will be collected from the employee and the public?

(A) Letters, memoranda, and other documents citing complaints of alleged criminal or administrative misconduct.

(B) Investigative files which include: (1) Reports of investigations to resolve allegations of misconduct or violations of law with related exhibits, statements, affidavits, records or other pertinent documents obtained during investigations; (2) transcripts and documentation concerning requests and approval for consensual (telephone and consensual non-telephone) monitoring; (3) reports from or to other law enforcement bodies; (4) prior criminal or non-criminal records of individuals as they relate to the investigations; and (5) reports of actions taken by management personnel regarding misconduct and reports of legal actions resulting from violations of statutes referred to the Department of Justice for prosecution.

3. Accuracy, Timeliness, and Reliability

All staff processing allegations will be responsible for ensuring that information entered into the system is accurate and complete. Information will be entered in a timely manner and updated in the system as appropriate.

a. How will data collected from sources other than bureau records be verified for accuracy?

Information is received from individuals and is only as reliable as that provided.

b. How will data be checked for completeness?

Information is received from individuals and is channeled to the Office of Investigations' Complaint Management Branch and is only as reliable as that provided.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Information is received from individuals and is channeled to the Office of Investigations' Complaint Management Branch and is only as reliable and current as that provided.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The Office of Investigations Case Management System is comprised of specific data fields. These fields are described in detail in a User Guide prepared by the system developer. In addition, specific guidance regarding data entry for specific fields is included in the User Guide.

D. **Attributes of the Data:**

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

The information collected in the Office of Investigations Case Management System is necessary and is directly related to the reason for which the system has been designed. The majority of the data elements are required for preparation and submission of the Semi Annual report to Congress required by the Inspector General Act, 5 U.S.C. App. 3, § 5.

2. 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?

Yes. The system will allow users through reports to aggregate information about the subjects of investigations with regard to the nature of the allegations received or initiated by the OIG.

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

No. The data will be maintained in the Office of Investigations Case Management System.

4. Can the system make determinations about employees/public that would not be possible without the new data?

Yes, through the use of the system, the OIG will be able to determine what records have been created and completed by users in the system.

5. How will the new data be verified for relevance and accuracy?

Information is received from individuals and is only as reliable as that provided.

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The system consolidates the information provided by complainants and users for the express purpose of providing reports. Paper records and word processing disks are maintained in locked safes and all access doors are locked when offices are vacant. Automated records are controlled by computer security programs which limit access to authorized personnel who have a need for such information in the course of their duties. The records are available to Office of Inspector General personnel who have an appropriate security clearance on a need-to-know basis.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Access to the Office of Investigations Case Management System will only be granted to those persons within the OIG with a need to know. Access levels and permission levels have been established by the OIG and authorized only to those persons who have a need to know the information contained in a system in order to carry out their duties. In accordance with OMB Circulars A-123, and A-130, Appendix III the electronic Office of Investigations Case Management System will have controls in place to the prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

8. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Paper. Yes. Alphabetically by name of subject or complainant, by case number, and by special agent name and/or employee identifying number.
Electronic: by complainant, subject, victim, or witness case number, and by special agent name.

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

These records may be used to:

(1) Disclose information to the Department of Justice in connection with actual or potential criminal prosecution or civil litigation;

(2) Disclose pertinent information to appropriate Federal, State, local, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or

implementing a statute, rule, regulation, order, or license, or where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(3) Disclose information to a Federal, State, or local agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an employee, or the issuance of a security clearance, license, contract, grant, or other benefit;

(4) Disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations in response to a subpoena or in connection with criminal law proceedings;

(5) Provide information to a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(6) Provide information to the news media in accordance with guidelines contained in 28 CFR 50.2 which relate to an agency's functions relating to civil and criminal proceedings;

(7) Provide information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation.

E. <u>Maintenance and Administrative Controls:</u>

1. 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 user's manual and guidelines will ensure consistent use of the data in all sites.

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

The retention periods of data/records in the system are covered by General Records Schedules (GRS) 14 and 20. The OIG also follow guidance on permanent and temporary records disposition issued by the National Archives Records Administration (NARA).

3. 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?

Procedures for eliminating the data at the end of the retention are established in accordance with GRS 14 and 20 or NARA guidance.

Investigative files are stored on-site for 3 years at which time they retired to the Federal Records Center, Suitland, Maryland, for temporary storage. In most instances, the files are destroyed when 10 years old. However, if the files have significant or historical value, they are retained on-site for 3 years, then retired to the Federal Records Center for 22 years, at which time they are transferred to the National Archives and Records

Administration for permanent retention. In addition, an automated investigative case tracking system is maintained on-site; the case information deleted 15 years after the case is closed, or when no longer needed, whichever is later.

4. Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

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

There is no new use of technology that would affect privacy.

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

While some data will allow the identification of individuals, the system is not configured to monitor any individuals.

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

N/A.

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

The Office of Investigations Case Management System utilizes audit logs and has user levels to prevent unauthorized access to the system. The system is only accessible by those OIG employees who have been assigned usernames and passwords.

9. Under which Privacy Act SORN does the system operate? Provide number and name.

TREAS/DO.190; to be amended to reflect the title change of the database only.

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

"Yes" because of the need to change the name from IDMS to IMIS or generally to cover all future systems, the Office of Investigations Case Management System.

F. **Access to Data:**

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

Users of the system will include: Office of Investigations Special Agents, Supervisors and IT Staff, system managers, attorneys and other employees of the OIG who have a need to know the information contained in this system in order to carry out their duties. The System Administrator will have access to the data in the system as necessary to carry out his/her responsibilities. In certain instances, the contractor performing the work on the OIG's behalf may have access to records in the system. The routine use section of the Privacy Act system of records notice, TREASURY/DO .190, identifies those parties that can gain access to the information when the use is compatible with that identified in the notice.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

For the most part, access to the data by a user (i.e., OIG employees who are designated as Office of Investigations personnel and, as such, require access to the database to administer the laws) is determined by the "need-to-know" requirements of the Privacy Act, the users profile based on the user's job requirements, managerial decisions, etc. and dependent on a compatible purpose for which the data was collected. The criteria, procedures, controls and responsibility regarding access are documented in the Special Agent Handbook, and in the SORN.

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

Access to records in the system is limited to authorized personnel whose official duties require such access, i.e., all in a "need to know" basis. Electronic data is protected through user identification, passwords, database permissions and software controls. For example, in the Office of Investigations Case Management System Supevisors have access to all the data.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

In accordance with OMB Circulars A123, and A-130, Appendix III, the electronic Case Management System will have controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All users have a password and ID that is issued by either the OIG's Office of Information Technology or Office of Investigations, System Administrator. All users received training on the Office of Investigations Case Management System. In addition, the System Developer created a user manual to provide guidance to the OIG personnel who will be regular users of the system.

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, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

Yes, contractors are involved with the design and development of the system and were involved with the maintenance of the system contract. As far as I can tell a Privacy Act clause was not included as part of the statement of work. I do not know if the contractor was provided with copies of the Department's Privacy Act regulations. As of October 1, 2008 the contractor is no longer involved in the maintenance or development of the system. Any upgrades will be handled by the OIG IT staff.

6. Do other systems share data or have access to the data in the system? If yes, explain.

No, the Office of Investigations, Case Management System is a closed system.

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

There is no interface. Although all employees who have access to information in a Privacy Act system there are some responsibility for protecting personal information covered by the Privacy Act (see 31 CFR 1.28**,** Training, rules of conduct, penalties for non-compliance), the information owner and system manager share overall responsibility for protecting the privacy rights of individuals by following Treasury Directive 71-10 along with the Department of the Treasury Security Manual.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

Information from this system will only be shared with other agencies consistent with the FOIA/PA statutory exceptions in the routine uses set forth in the privacy act system of records notice, Treasury .004, Freedom of information act/Privacy act requester records—Treasury.

The Following Officials Have Approved this Document

1. Program Manager

/s/ **(Signature)**

Name David S. Smith **Title** Special Agent in Charge

2. System Manager

/s/ **(Signature)**

Name Matthew Issman **Title** Assistant Inspector General for Investigations

3. Information Systems Security Manager

/s/ **(Signature)**

Name Ernest Eldredge **Title** Information Systems Security Officer

4. Privacy Act Officer

/s/ **(Signature)**

Name Richard K. Delmar **Title** Counsel to the Inspector General

5. IT Review Official

/s/ **(Signature)**

Name Dee Thompson **Title** Director of Information Technology

6. Chief Information Officer Official (when necessary)

/s/ **(Signature)**

Name John Czajkowski **Title** Assistant Inspector General for Management

Attachment IV to OIG Privacy Impact Assessment (PIA)

Chapter III: Privacy Impact Assessment Template
(Derived from the Department of the Treasury Privacy Impact Assessment Manual TD P 25-07, July 2006 Advance Copy)

Once completed provide copies of the PIA to the following:

- Office of Management and Budget (OMB) Exhibit 300 Submission (when required)
- Bureau Privacy Act Officer
- Bureau Information Systems Security Manager
- Treasury's Office of the Chief Information Officer

Also refer to the signature approval page at the end of this document.

A. **Contact Information:**

Name of System, Project or Program: Office of Inspector General Correspondence Management System (CMS)

OMB Unique Identifier: (*if appropriate)*

1. **Who is the person completing this document?**

Debra L. McGruder, Deputy Assistant Inspector General for Management, U.S. Department of the Treasury, Office of Inspector General, Office of Management , (202) 927-5229, mcgruderd@oig.treas.gov..

2. **Who is the system owner?**

Dennis Schindel, Deputy Inspector General, U.S. Department of the Treasury, Office of Inspector General, (202) 622-1090; schindeld@oig.treas.gov.

3. **Who is the system manager for this system or application?**

Debra L. McGruder, Deputy Assistant Inspector General for Management, U.S. Department of the Treasury, Office of Inspector General, Office of Management, (202) 927-5229, mcgruderd@oig.treas.gov.

4. Who is the Information Systems Security Manager who reviewed this document? (Name, organization, and contact information).

Ernest Eldredge, Information Systems Security Officer, U.S. Department of the Treasury, Office of Inspector General, Office of Management, Office of Information Technology, (202) 927-5753, EldredgeE@oig.treas.gov.

5. Who is the Bureau Privacy Act Officer who reviewed this document? (Name, organization, and contact information).

Richard K. Delmar, Counsel to the Inspector General, U.S. Department of the Treasury, Office of Inspector General, Office of Counsel, (202) 927-3973, DelmarR@oig.treas.gov.

6. Who is the IT Reviewing Official? (Name, organization, and contact information).

Dee Thompson, Director of Information Technology, U.S. Department of the Treasury, Office of Inspector General, Office of Management, Office of Information Technology, (202) 927-5883, ThompsonD@oig.treas.gov.

B. **System Application/General Information:**

1. Does this system contain any information in identifiable form?

The system contains personal information about individuals, e.g., name, home and work telephone and fax numbers, e-mail addresses, and other pertinent information related to Correspondence received from individuals, Congress or other Government Offices. The information is then entered in to the CM with whatever contact information is provided from the sender.

2. What is the purpose of the system/application?

The primary purpose of this system is to facilitate the manageability and efficiency of correspondence received from individuals, Congress or other Government Offices. A short synopsis of the content is entered into the CM; then the correspondence is forwarded to appropriate OIG Program Office or other Government agency.
The system will allow the tracking of correspondence from receipt to completion.

3. What legal authority authorizes the purchase or development of this system/application?

The Inspector General Act of 1978, as Amended, 5 U.S.C.A. App. 3; 5 U.S.C. 301; 31 U.S.C. 321.

4. **Under which Privacy Act SORN does the system operate**? **Provide the number and name.**

TREASURY/DO .191: OIG Management Information System (MIS).

C. **Data in the System:**

1. **What categories of individuals are covered in the system?**

Correspondence is received from individuals, businesses, Congress or other Government Offices.

2. **What are the sources of the information in the system?**

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information in this system comes primarily from the individuals who make requests.

b. What Federal agencies are providing data for use in the system?

None.

c. What State and/or local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

Information collected will include, but not be limited to: name, home/business address; home/business telephone number; fax and e-mail numbers; organizational affiliation; date of requests; subject of requests; other information related to responding to requests.

3. **Accuracy, Timeliness, and Reliability**

The OIG staff assigned to reply will be responsible for ensuring that information entered into the system is accurate and complete. Information will be entered in a timely manner and updated in the system as appropriate.

a. How will data collected from sources other than bureau records be verified for accuracy?

Information is only as reliable as provided by requestors.

b. How will data be checked for completeness?

Information is only as reliable as provided by requestors.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Information is only as reliable as provided by requestors.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The CMS is comprised of specific data fields. These fields are described in detailed in a User Guide prepared by the contractor. In addition, specific guidance regarding data entry for specific fields is included in the User Guide.

D. **Attributes of the Data:**

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

The information collected in the CMS is necessary and is directly related to the reason for which the system has been designed.

2. 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.

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

No.

4. Can the system make determinations about employees/public that would not be possible without the new data?

No.

5. How will the new data be verified for relevance and accuracy?

N/A

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The data in the system is not being consolidated.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Access to the CMS will only be granted to those persons within the Office of Inspector General. Access levels and permission levels have been established by the OIG and authorized only to those persons who have a need to know the information contained in a system in order to carry out their duties. In accordance with OMB Circulars A-123, and A-130, Appendix III, the CMS has controls in place to prevent the unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

8. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved by searching various fields such as: name, address, phone number, email address, type of request or complaint, Treasury office or bureau at issue, type of action needed, and OIG function assigned.

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

Reports will not be produced on individuals.

E. **Maintenance and Administrative Controls:**

1. 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 user's manual and guidelines will ensure consistent use of the data in all sites.

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

The retention periods of data/records in the system are covered by General Records Schedules (GRS).

3. 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?

Procedures for eliminating the data at the end of the retention are established in accordance with the GRS.

4. Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

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

There is no new use of technology that would affect privacy.

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system is capable of identifying individuals by name, phone number, home address, etc. While this data would allow for the identification of individuals, the system is not configured to monitor any individual.

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

Individuals will not be monitored.

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

The system is only accessible by those OIG employees who have been assigned usernames and passwords. In addition, the system has audit logs which will allow administrators to see who accesses the system.

9. Under which Privacy Act SORN does the system operate? Provide number and name.

TREASURY/DO .191: OIG Management Information System (MIS)

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

System has not been modified since inception of the database.

F. **Access to Data:**

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

Users of the system will include: system managers and other employees of the OIG who have a need to know the information contained in this system in order to carry out their duties. The System Administrator will have access to the data in the system as necessary to carry out his/her responsibilities. The routine use section of the Privacy Act system of records notice, TREASURY/DO .191, identifies those parties that can gain access to the information when the use is compatible with that identified in the notice.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

For the most part, access to the data by a user is determined by the "need-to-know" requirements of the Privacy Act, the users profile based on the user's job requirements, managerial decisions, etc. and dependent on a compatible purpose for which the data was collected.

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

Yes. However, electronic data is protected through user identification and passwords. In addition, any changes in the database will create audit logs which can be accessed by the administrators.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

In accordance with OMB Circulars A123, and A-130, Appendix III, the electronic CMS system will have controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All users have a password and ID that is issued by the OIG's Office of Information Technology. All users received training on the CMS.

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, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

Yes, contractors were involved with the design and development of the system and were involved with the initial maintenance of the system. As far as I can tell a Privacy Act clause was not included as part of the statement of work. I do not know if the contractor was provided with copies of the Department's Privacy Act regulations. As of 1

October 2008 the contractor is no longer involved in the maintenance or development of the system. Any upgrades will be handled by the OIG IT staff.

6. Do other systems share data or have access to the data in the system? If yes, explain.

No, the CMS is a closed system.

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

There is no interface. Although all employees who have access to information in a Privacy Act system have responsibility for protecting personal information covered by the Privacy Act (see 31 CFR 1.28**,** Training, rules of conduct, penalties for non-compliance), the information owner and system manager share overall responsibility for protecting the privacy rights of individuals by following Treasury Directive 71-10 along with the Department of the Treasury Security Manual.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

Other agencies will not share or have access to the data in the system.

9. How will the data be used by the other agency?

N/A

10. Who is responsible for assuring proper use of the data?

The Deputy Inspector General.

The Following Officials Have Approved this Document

1. Program Manager

/s/ **(Signature)**

Name John Czajkowski **Title** Assistant Inspector General for Management

2. System Manager

/s/ **(Signature)**

Name Debra L. McGruder **Title** Deputy Assistant Inspector General for Management

3. Information Systems Security Manager

/s/ **(Signature)**

Name Ernest Eldredge **Title** Information Systems Security Officer

4. Privacy Act Officer

/s/ **(Signature)**

Name R.K. Delmar **Title** Counsel to the Inspector General

5. IT Review Official

/s/ **(Signature)**

Name Dee Thompson **Title** Director of Information Technology

6. Chief Information Officer Official (when necessary)

/s/ **(Signature)**

Name John Czajkowski **Title** Assistant Inspector General for Management