

Federal Communications Commission
Office of the Managing Director



**Privacy Impact Assessment¹ (PIA) for the
Criminal Investigative Files**

October 19, 2009

FCC Bureau/Office: Office of Inspector General (OIG)

Privacy Analyst: Leslie F. Smith
Telephone Number: (202) 418-0217
E-mail Address: Leslie.Smith@fcc.gov

¹ This questionnaire is used to analyze the impacts on the privacy and security of the personally identifiable information (PII) that is being maintained in these records and files.

The *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, requires Federal agencies to take special measures to protect personal information about individuals when the agencies collect, maintain, and use such personal information.

Having established through the **Privacy Threshold Analysis (PTA)** that this information system contains information about individuals, *e.g.*, personally identifiable information (PII), it is important that when the FCC makes changes to such an information system, the FCC then analyzes:

- (a) What changes are being made to the information that the system presently collects and maintains; and/or
- (b) What new information will be collected and maintained to determine the continuing impact(s) on the privacy of the individuals.

The Privacy Impact Assessment template's purpose is to help the bureau/office to evaluate the changes in the information in the system and to make the appropriate determination(s) about how to treat this information, as required by the Privacy Act's regulations.

Section 1.0 Information System's Contents:

1.1 Status of the Information System:

- New information system—Implementation date:
- Revised or upgraded information system—Revision or upgrade date: April 2009

If this system is being revised—what will be done with the newly derived information:

- Placed in existing information system—Implementation Date: April 2009
- Placed in new auxiliary/ancillary information system—Date:
- Other use(s)—Implementation Date:

Please explain your response:

The Office of Inspector General (OIG) is making various revisions to the Criminal Investigative Files information system, including the system of records notice (SORN) FCC/OIG-1, "Criminal Investigative Files," that covers the personally identifiable information (PII) used by this information system. OIG has upgraded parts of this information system, which includes the addition of secured servers to hold information related to the OIG's audits and investigations. OIG has also added one routine use, "breach notification," as required by OMB Memorandum M-07-16 (May 22, 2007).

1.2 Has a Privacy Threshold Analysis (PTA) been done?

- Yes
Date:
- No

If a Privacy Threshold Analysis has not been done, please explain why not:

The Criminal Investigative Files information system, including the personally identifiable information (PII) that is covered by the system of records notice (SORN), FCC/OIG-1, "Criminal Investigative Files" SORN, pre-dates the OMB requirements contained in OMB Memorandum M-03-22 (September 22, 2003).

If the Privacy Threshold Analysis (PTA) has been completed, please skip to Question 1.15

1.3 Has this information system, which contains information about individuals, *e.g.*, personally identifiable information (PII), existed under another name, *e.g.*, has the name been changed or modified?

- Yes
 No

If yes, please explain your response:

This information system has never existed under another name, nor has the name been changed since the SORN was published in the *Federal Register* on April 5, 2006.

1.4 Has this information system undergone a “substantive change” in the system’s format or operating system?

- Yes
 No

If yes, please explain your response:

The OIG staff has made only minor changes to the Criminal Investigative Files information system.

If there have been no such changes, please skip to Question 1.6.

1.5 Has the medium in which the information system stores the records or data in the system changed from paper files to electronic medium (computer database); or from one electronic information system to another, *i.e.*, from one database, operating system, or software program, *etc.*?

- Yes
 No

If yes, please explain your response:

1.6 Has this information system operated as part of another information system or was it linked to another information system:

- Yes
 No

If yes, please explain your response:

The Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is a "stand alone" information system, except that information is collected, used, and stored from other FCC information systems, *i.e.*, payroll and time and attendance data, *etc.*, but there is no electronic transfer of information between other FCC or non-FCC information systems.

The OIG is adding secured servers that will contain information, including PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, which is used in the conduct of audits and investigations. These servers are owned and used exclusively by OIG, although the Information Technology Center (ITC) staff will maintain and manage the operation of these servers. .

If the information system is not part of, nor linked to another information system, please skip to Question 1.8

1.7 If so, was it operated by another bureau/office or transferred from another Federal agency to the FCC?

- Yes
- No

Please explain your response:

1.8 What information is the system collecting, analyzing, managing, storing, transferring, *etc.*:

Information about FCC Employees:

- No FCC employee information
- FCC employee's name
- Other names used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- SSN
- Race/Ethnicity
- Gender
- U.S. Citizenship
- Non-U.S. Citizenship
- Biometric data
 - Fingerprints
 - Voiceprints
 - Retina scans/prints
 - Photographs
 - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/age
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information
- Home address
- Home address history
- Home telephone number(s)
- Personal cell phone number(s):
- Personal fax number(s)
- Personal e-mail address(es):
- Emergency contact data:
- Credit card number(s)
- Driver's license
- Bank account(s)
- FCC personal employment records
- Military records
- Financial history
- Foreign countries visited
- Law enforcement data
- Background investigation history
- National security data
- Communications protected by legal privileges

- Digital signature
- Other information: The information system contains data on individuals, including present and former FCC employees, who are or have been the subjects of criminal investigations conducted by the Office of Inspector General (OIG), which relate to allegations raised pertaining to fraud, waste, and abuse of the FCC's programs and operations.

Information about FCC Contractors:

- No FCC contractor information
- Contractor's name
- Other name(s) used, *i.e.*, maiden name, *etc.*
- FCC Contractor badge number (Contractor ID)
- SSN
- U.S. Citizenship
- Non-U.S. Citizenship
- Race/Ethnicity
- Gender
- Biometric data
 - Fingerprints
 - Voiceprints
 - Retina scans/prints
 - Photographs
 - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/Age
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information
- Home address
- Home address history
- Home telephone number(s)
- Personal cell phone number(s):
- Personal fax number(s)
- Personal e-mail address(es):
- Emergency contact data:
- Credit card number(s)
- Driver's license number(s)
- Bank account(s)
- Non-FCC personal employment records
- Military records
- Financial history
- Foreign countries visited
- Law enforcement data
- Background investigation history
- National security data
- Communications protected by legal privileges
- Digital signature
- Other information: The information system contains data on individuals, including contractors who work at the FCC, who are or have been the subjects of criminal

investigations conducted by the Office of Inspector General (OIG), which relate to allegations raised pertaining to fraud, waste, and abuse of the FCC's programs and operations.

Information about FCC Volunteers, Visitors, Customers, and other Individuals:

- Not applicable
- Individual's name:
- Other name(s) used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- SSN:
- Race/Ethnicity
- Gender
- Citizenship
- Non-U.S. Citizenship
- Biometric data
 - Fingerprints
 - Voiceprints
 - Retina scans/prints
 - Photographs
 - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/Age:
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information
- Home address
- Home address history
- Home telephone number(s)
- Personal cell phone number(s):
- Personal fax number(s)
- Personal e-mail address(es):
- Emergency contact data:
- Credit card number(s)
- Driver's license number(s)
- Bank account(s)
- Personal e-mail address(es)
- Non-FCC personal employment records
- Military records
- Financial history
- Foreign countries visited
- Law enforcement data
- Background investigation history
- National security data
- Communications protected by legal privileges
- Digital signature
- Other information: The information system includes data on individuals who are or have been the subjects of investigations conducted by the Office of Inspector General (OIG), which relate to allegations raised pertaining to fraud, waste, and abuse of the FCC's programs and operations.

Information about Business Customers and others (usually not considered “personal information”):

- Not applicable
- Name of business contact/firm representative, customer, and/or others
- Race/Ethnicity
- Gender
- Full or partial SSN:
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional affiliations
- Business/office address
- Intra-business office address (office or workstation)
- Business telephone number(s)
- Business cell phone number(s)
- Business fax number(s)
- Business pager number(s)
- Business e-mail address(es)
- Bill payee name
- Bank routing number(s)
- Income/Assets
- Web navigation habits
- Commercially obtained credit history data
- Commercially obtained buying habits
- Credit card number(s)
- Bank account(s)
- Other information: The information system includes data on individuals who are or have been the subjects of investigations conducted by the Office of Inspector General (OIG), which relate to allegations raised pertaining to fraud, waste, and abuse of the FCC's programs and operations.

1.9 What are the sources for the information that you are collecting:

- Personal information from FCC employees: PII concerning current and former FCC employees who are or have been subjects of OIG criminal investigations.
- Personal information from FCC contractors: PII concerning individuals who are or have been subjects of OIG criminal investigations..
- Personal information from non-FCC individuals and/or households: Individuals who are or have been subjects of OIG criminal investigations.
- Non-personal information from businesses and other for-profit entities: PII concerning individuals who are or have been subjects of OIG criminal investigations.
- Non-personal information from institutions and other non-profit entities: PII concerning individuals who are or have been subjects of OIG criminal investigations.
- Non-personal information from farms:
- Non-personal information from Federal Government agencies: PII concerning individuals who are or have been subjects of OIG criminal investigations.
- Non-personal information from state, local, or tribal governments: PII concerning individuals who are or have been subjects of OIG criminal investigations.
- Other sources: PII concerning individuals working for international companies or who are themselves not U.S. citizens, who are or have been subjects of OIG criminal investigations.

1.10 Will the information system obtain, use, store, analyze, *etc.* information about individuals *e.g.*, personally identifiable information (PII), from other information systems, including both FCC and non-FCC information systems?

- Yes
- No

Please explain your response:

As noted in Question 1.6, the Criminal Investigative Files information system is a "stand alone" information system except that information is collected, used, and stored from other FCC information systems, *i.e.*, payroll and time and attendance data, *etc.*, but there is no "electronic transfer" of information between this information system and other FCC or non-FCC information systems, *e.g.*, it has no electronic links to any other FCC or non-FCC information systems.

The OIG is adding secured servers that will contain information, including PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, which is used in the conduct of audits and investigations. These servers are owned and used exclusively by OIG, although the Information Technology Center (ITC) staff will maintain and manage the operation of these servers.

If the information system does not use any PII from other information systems, including both FCC and non-FCC information systems, please skip to Question 1.15.

1.11 If the information system uses information about individuals from other information systems, what information will be used?

- FCC information system and information system name(s): Payroll and Time and Attendance.
- Non-FCC information system and information system name(s): Various external law enforcement databases.
- FCC employee's name:
- (non-FCC employee) individual's name
- Other names used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- Other Federal Government employee ID information, *i.e.*, badge number, *etc.*
- SSN:
- Race/Ethnicity
- Gender
- U.S. Citizenship
- Non-U.S. Citizenship
- Biometric data
 - Fingerprints
 - Voiceprints
 - Retina scan/prints
 - Photographs
 - Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*
- Birth date/Age
- Place of birth
- Medical data
- Marital status
- Spousal information
- Miscellaneous family information:
 - Home address
 - Home address history

- Home telephone number(s)
- Personal cell phone number(s)
- Personal fax number(s)
- Personal e-mail address(es)
- Emergency contact data
- Credit card number(s)
- Driver's license
- Bank account(s)
- Non-FCC personal employment records
- Non-FCC government badge number (employee ID)
- Law enforcement data
- Military records
- National security data
- Communications protected by legal privileges
- Financial history
- Foreign countries visited
- Background investigation history
- Digital signature
- Other information:

Information about Business Customers and others (usually not considered “personal information”):

- Not applicable
- Name of business contact/firm representative, customer, and/or others
- Race/Ethnicity
- Gender
- Full or partial SSN:
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional affiliations
- Intra-business office address (office or workstation)
- Business telephone number(s)
- Business cell phone number(s)
- Business fax number(s)
- Business e-mail address(es)
- Bill payee name
- Bank routing number(s)
- Income/Assets
- Web navigation habits
- Commercially obtained credit history data
- Commercially obtained buying habits
- Personal clubs and affiliations
- Credit card number(s)
- Bank account(s)
- Other information:

- 1.12 Will this information system derive new information, records, or data, or create previously unavailable information, records, or data, through aggregation or consolidation from the information that will now be collected via this link to the other system, including information, records, or data, that is being shared or transferred from the other information system(s)?

Yes
 No

Please explain your response:

This information system does not create or derive new information, and the information within OIG's Criminal Investigative Files information system will not be electronically obtained from nor linked to other FCC or non-FCC information systems.

- 1.13 Can the information, whether it is: (a) in the information system, (b) in a linked information system, and/or (c) transferred from another system, be retrieved by a name or a "unique identifier" linked to an individual, *e.g.*, SSN, name, home telephone number, fingerprint, voice print, *etc.*?

Yes
 No

Please explain your response:

As noted in Question 1.12, the information in the Criminal Investigative Files information system can be obtained by various identifiers, but there are no electronic links to other information systems.

- 1.14 Will the new information include personal information about individuals, *e.g.*, personally identifiable information (PII), be included in the individual's records, or be used to make a determination about an individual?

Yes
 No

Please explain your response:

The information system includes data on individuals who are or have been the subjects of criminal investigations conducted by the OIG, which relate to the allegations raised pertaining to fraud, waste, and abuse of the FCC's programs and operations.

- 1.15 Under the *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, Federal agencies are required to have a System of Records Notice (SORN) for an information system like this one, which contains information about individuals, *e.g.*, "personally identifiable information" (PII).

A System of Records Notice (SORN) is a description of how the information system will collect, maintain, store, and use the personally identifiable information (PII).

Is there a SORN that already covers this PII in this information system?

Yes
 No

If yes, what is this System of Records Notice (SORN): This system of records notice, FCC/OIG-5, "Integrated Library System (ILS) Records," was published in the *Federal Register* on April 5, 2006.

Please provide the citation that was published in the *Federal Register* for the SORN: 71 FR 17234, 17245.

If a SORN already covers this PII, please skip to **Section 2.0 System of Records Notice (SORN) Update** to address any changes to this SORN.

If a system of records notice (SORN) does not presently cover the information about individuals in this system, then it is necessary to determine whether a new FCC system of records notice must be created for the information.

- 1.16 If this information system is not covered by a system of records notice (SORN), does the information system exist by itself, or does it now, or did it previously exist as a component or subset of another SORN?

Yes
 No

If yes, please explain what has occurred:

What is the System of Records Notice (SORN) of which it is currently or previously a component or subset:

Please also provide the citation that was published in the *Federal Register* for the SORN:

- 1.17 What are the purposes or functions that make it necessary to create a new a system of records notice (SORN) for this information system, *e.g.*, why is the information being collected?

- 1.18 Where is this information for the system of records notice (SORN) located?

- 1.19 Is the use of the information both relevant and necessary to the purposes for which the information system is designed, *e.g.*, is the SORN only collecting and using information for the specific purposes for which the SORN was designed so that there is no “extraneous” information included in the database(s) or paper files?

Yes
 No

Please explain your response:

If the use of this information is both relevant and necessary to the processes for this information system is designed, please skip to Question 1.21.

- 1.20 If not, why or for what reasons is the information being collected?

1.21 Is the information covered under a Security Classification as determined by the FCC Security Officer?

- Yes
- No

Please explain your response:

1.22 What is the legal authority that authorizes the development of the information system and the information/data collection?

1.23 In what instances would the information system's administrator/manager/developer permit disclosure to those groups outside the FCC for whom the information was not initially intended.

Such disclosures, which are referred to as "Routine Uses," are those instances that permit the FCC to disclose information from a SORN to specific "third parties." These disclosures may be for the following reasons:

(check all that are applicable)

- Adjudication and litigation:
- Committee communications and reporting:
- Compliance with welfare reform requirements:
- Congressional inquiries:
- Emergency response by medical personnel and law enforcement officials:
- Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:

- Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*:
- FCC enforcement actions:
- Financial obligations under the Debt Collection Information Act:
- Financial obligations required by the National Finance Center:
- First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc.*:
- Government-wide oversight by NARA, DOJ, and/or OMB:
- Labor relations (NTEU):
- Law enforcement and investigations:
- Program partners, *e.g.*, WMATA, *etc.*:
- Breach of Federal data:
- Others "third party" disclosures:

1.24 Will the information be disclosed to consumer reporting agencies?

- Yes
- No

Please explain your response:

1.25 What are the policies for the maintenance and secure storage of the information?

- 1.26 How is information in this system retrieved?
- 1.27 What policies and/or guidelines are in place on how long the bureau/office will retain the information?
- 1.28 Once the information is obsolete or out-of-date, what policies and procedures have the system's managers/owners established for the destruction/purging of the data?
- 1.29 Have the records retention and disposition schedule(s) been issued or approved by the National Archives and Records Administration (NARA)?

- Yes
 No

Please explain your response:

If a NARA records retention and disposition schedule has been approved for this System of Records Notice (SORN), please skip to **Section 2.0 System of Records Notice (SORN) Update:**

- 1.30 If there is no NARA approved records retention and disposal schedule, has there been any coordination with the Performance Evaluation and Records Management Branch (PERM) or the Records Officer?

- Yes
 No

Please explain your response:

If this is a new System of Records Notice (SORN), please skip to **Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:**

Section 2.0 System of Records Notice (SORN) Update:

If a System of Records Notice (SORN) currently covers the information, please provide information to update and/or revise the SORN:

- 2.1 Have there been any changes to the Security Classification for the information covered by the system of records notice (SORN) from what was originally determined by the FCC Security Officer?

- Yes
 No

Please explain your response:

The FCC's Security Operations Center (SOC) has not assigned a security classification to the Criminal Investigative Files information system, and to the personally identifiable information

(PII) that it collects, uses, and maintains that is covered by FCC/OIG-1, “Criminal Investigative Files” SORN.

2.2 Have there been any changes to the location of the information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

The information, including the PII covered by FCC/OIG-1, “Criminal Investigative Files” SORN, is located in the Office of Inspector General (OIG), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

2.3 Have there been any changes to the categories of individuals covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

The categories of individuals that are covered by FCC/OIG-1, “Criminal Investigative Files” SORN, include current and former Federal Communications Commission (FCC) employees, contractors, and other individuals who are or have been the subjects of criminal investigations conducted by the Office of Inspector General (OIG), which relate to allegations that pertain to fraud, waste, and abuse of the FCC's programs and operations..

2.4 Have there been any changes to the categories of records, *e.g.*, types of information (or records) that the system of records notice (SORN) collects, maintains, and uses?

- Yes
- No

Please explain your response:

The categories of records, including the PII covered by FCC/OIG-1, “Criminal Investigative Files” SORN, include:

- (1) Case files developed during investigations of known or alleged fraud, waste, and abuse, or other irregularities or violations of criminal laws and regulations;
- (2) Case files related to programs and operations administered or financed by the FCC, including contractors and others doing business with the FCC;
- (3) Investigative files relating to FCC employees' hotline complaints and other miscellaneous complaint files; and
- (4) Investigative reports and related documents, such as correspondence, notes, attachments, and working papers.

2.5 Have there been any changes to the legal authority under which the FCC collects and maintains the information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

The legal authority for maintenance of the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN is the Inspector General Act of 1978, as amended by Public Law 100 - 504, October 18, 1988.

- 2.6 Have there been any changes to the purposes for collecting, maintaining, and using the information covered by the system of records notice (SORN)?

- Yes
 No

Please explain your response:

The purposes for collecting maintaining, and using the information in the FCC/OIG-1, "Criminal Investigative Files" SORN are to:

- (1) Document investigations designed to prevent or detect fraud, waste, or abuse;
- (2) Conduct and supervise audits and investigations relating to programs and operations in the Commission; and
- (3) Inform the Chairman of the FCC about problems and deficiencies in the FCC's programs and operations; and/or
- (4) Suggest corrective action that will address the irregularities, problems, or deficiencies, which the FCC's Inspector General has identified in its case files and investigations.

- 2.7 Have there been any changes to the Routine Uses under which disclosures are permitted to "third parties" as noted in the system of records notice (SORN)?

- Yes
 No

Please check all Routine Uses that apply and provide any explanation as required:

- Adjudication and litigation:
- Committee communications and reporting:
- Compliance with welfare reform requirements:
- Congressional inquiries:
- Emergency response by medical personnel and law enforcement officials:
- Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:
- Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*:
- FCC enforcement actions:
- Financial obligations under the Debt Collection Act:
- Financial obligations required by the National Finance Center:
- First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc.*:
- Government-wide oversight by NARA, DOJ, and/or OMB:
- Labor relations:
- Law enforcement and investigations:
- Program partners, *e.g.*, WMATA:
- Public Access:
- Breach of Federal data: OMB Memorandum M-07-16 (May 22, 2007).
- Others Routine Use disclosures not listed above:

2.8 Have there been any changes as to whether the FCC will permit the information covered by the system of records notice (SORN) can be disclosed to consumer reporting agencies?

- Yes
 No

Please explain your response:

Information in the Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is not disclosed to any consumer reporting agencies.

2.9 Have there been any changes to the policies and/or guidelines for the storage and maintenance of the information covered by this system of records notice (SORN)?

- Yes
 No

Please explain your response:

The information in the Criminal Investigative Files information system, including the PII that is covered by FCC/OIG-1, "Criminal Investigative Files" SORN, consists of:

- (1) Electronic data and records that are stored in the FCC's computer network databases and computer CDs and diskettes; and
- (2) Paper documents, records, and files that are stored in file cabinets.

2.10 Have there been any changes to how the information covered by the system of records notice (SORN) is retrieved or otherwise accessed?

- Yes
 No

Please explain your response:

Information in the Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is retrieved by name of the subject of the investigation or by a unique file number assigned to each investigation.

2.11 Have there been any changes to the safeguards that the system manager has in place to protect unauthorized access to the information covered by the system of records notice (SORN)?

- Yes
 No

Please explain your response:

Access to information in the Criminal Investigative Files information system, including the PII that is covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is restricted to OIG supervisors and employees and to ITC employees and contractors who manage the FCC's computer network databases. Other FCC employees and/or contractors may be granted access on a "need to know" as dictated by their job duties and responsibilities.

The electronic data, files, and records that are maintained in servers on the FCC's computer network. These servers are used exclusively by OIG. The servers are protected by with passwords and other security features. Data resident on the computer network are backed-up routinely onto magnetic media. Back-up tapes are stored securely on-site and at an off-site storage location.

Paper document, records, and files are kept in secured (locked) file cabinets in "non public areas." These file cabinets are further secured at the end of the business day. Access to these documents, records, and files, *etc.*, is limited to authorized OIG employees and to other FCC employees as dictated by their job duties and responsibilities. Thus, unauthorized examination of these files during business hours would be easily detected.

Please note that you must also provide an update of the current protections, safeguard, and other security measures that are in place in this SORN in **Section 5.0 Safety and Security Requirements:**

2.12 Have there been any changes to the records retention and disposition schedule for the information covered by the system of records notice (SORN)? If so, has the system manager worked with the Performance Evaluation and Records Management (PERM) staff to insure that this revised schedule been approved by the National Archives and Records Administration (NARA)?

- Yes
 No

Please explain your response:

Records and files (including investigative reports and related documents, which may include such information as correspondence, notes, attachments, and working paper) in the following categories are cutoff and closed at the end of each fiscal year. These records and files are retired to the Federal Records Center (FRC) five years after the cut off; they are then transferred to the National Archives 25 years after the cutoff date:

- (1) Investigative files, including case files developed during investigations of known or alleged fraud, waste, and abuse or their irregularities or violations of law and regulations;
- (2) Case files related to programs and operations administered or financed by the FCC, including contractors and others doing business with the FCC;
- (3) Investigative files related to FCC hotline complaints, and other miscellaneous complaint files;
- (4) Information on individuals, including present and former FCC employees, who are or have been the subject of criminal investigations conducted by the OIG relating to allegations raised pertaining to fraud, waste, and abuse with respect to programs and operations of the Commission; and
- (5) Case files of significant value because the case attracts substantial national media attention, results in a Congressional investigation, or results in substantive changes in agency policies and procedures.

Records and files in the following category are cut off and closed at the end of each fiscal year. They are then transferred to the FRC five years after the cutoff date and destroyed 10 years after cut off:

All other investigative case files not deemed to be of significant value.

Records and files in the following categories are cutoff and closed at the end of each fiscal year. They are then retired to the FRC five years after the cut off date and destroyed seven years after cut off:

Records and files containing information or allegations, which are of an investigative nature but do not related 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 records and files providing general information that may prove useful in OIG investigations.

Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:

3.1 Who will develop the information system(s) covered by this system of records notice (SORN)?

- Developed wholly by FCC staff employees:
- Developed wholly by FCC contractors:
- Developed jointly by FCC employees and contractors:
- Developed offsite primarily by non-FCC staff:
- COTS (commercial-off-the-shelf-software) package:
- Other development, management, and deployment/sharing information arrangements:

3.2 Where will the information system be hosted?

- FCC Headquarters
- Gettysburg
- San Diego
- Colorado
- New York
- Columbia Lab
- Chicago
- Other information:

3.3 Who will be the primary manager(s) of the information system who will be responsible for assuring access to, proper use of, and protecting the security and integrity of the information? (Check all that apply and provide a brief explanation)

- FCC staff in this bureau/office exclusively: OIG supervisors and staff have responsibility for access and proper use of the information in the Criminal Investigative Files information system.
- FCC staff in other bureaus/offices:
- Information system administrator/Information system developers:
- Contractors:
- Other information system developers, *etc*:

3.4 What are the FCC's policies and procedures that the information system administrators and managers use to determine who gets access to the information in the system's files and/or database(s)?

Access to the information is restricted to the OIG's supervisors and staff and the ITC staff. Other FCC employees, and law enforcement officials, and contractors working at the FCC may be granted access on a "need to know" basis as dictated by their job duties and responsibilities.

3.5 How much access will users have to data in the information system(s)?

- Access to all data:
- Restricted access to data, as determined by the information system manager, administrator, and/or developer: The Assistant Inspector General (AIG) or his/her designee determines which OIG employees, law enforcement officials, and contractors working at the FCC may be granted access on a "need-to-know" basis as part of their job duties and responsibilities.
- Other access policy:

- 3.6 Based on the Commission policies and procedures, which user group(s) may have access to the information at the FCC:
(Check all that apply and provide a brief explanation)
- Information system managers: OIG supervisory staff.
 - Information system administrators: ITC employees and contractors who manage the IT systems that hold and process the PII data in the OIG's servers that are part of the FCC's computer network.
 - Information system developers:
 - FCC staff in this bureau/office: OIG employees are granted access on a "need to know" basis.
 - FCC staff in other bureaus/offices: FCC employees in other bureaus/offices are granted access on a "need to know" basis.
 - FCC staff in other bureaus/offices in FCC field offices: FCC employees in field offices are granted access on a "need to know" basis.
 - Contractors:
 - Other Federal agencies: Law enforcement personnel working at the FCC are granted access on a "need to know" basis.
 - State and/or local agencies: State and/or local agency officials working at the FCC are granted access on a "need to know" basis.
 - Businesses, institutions, and other groups:
 - International agencies:
 - Individuals/general public:
 - Other groups:

3.7 If contractors are part of the staff in the FCC who collect, maintain, and access the information, does the IT supervisory staff ensure that contractors adhere fully to the Privacy Act provisions, as required under subsection (m) of the Privacy Act, as amended, 5 U.S.C. 552a(m)? We are not sure why the answer to 3.7 would not be "no."

- Yes
- No

Please explain your response:

The ITC supervisory staff provides periodic privacy training to the IT contractors who handle the PII contained in the Criminal Investigative Files that are located in the OIG's servers in the FCC's computer network.

3.8 Do any Section M contract(s) associated with the information system covered by this system of records notice (SORN) include the required FAR clauses (FAR 52.224-1 and 52.224-2)?

- Yes
- No

Please explain your response:

The OIG does not use contractors.

As noted in Question 3.7, the ITC supervisory staff manages the contractors who manage the OIG's servers that house the OIG's audit and investigative information. These servers are housed in the FCC's computer network. The contracts covering these contractors include the FAR clauses.

3.9 Does the information system covered by this system of records notice (SORN) transmit/share personal information, *e.g.*, personally identifiable information (PII), between the FCC information technology (ITC) network(s) and a public or other non-FCC IT network(s), which are not covered by this Privacy Impact Assessment?

- Yes
- No

Please explain your response:

As noted in Question 1.6, the Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is a "stand alone" information system, except that information is collected, used, and stored from other FCC information systems, *i.e.*, payroll and time and attendance data, *etc.*, but there is no "electronic transfer" of information between this information system and other FCC or non-FCC information systems.

The OIG is adding secured servers that will contain information, including PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, which is used in the conduct of audits and investigations. These servers are owned and used exclusively by OIG, although the Information Technology Center (ITC) staff will maintain and manage the operation of these servers.

If there is no information sharing or transmission, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.10 If the information system covered by this system of records noticed (SORN) transmits/shares personal information between the FCC network and a public or other non-FCC network, which is not covered by this Privacy Impact Assessment, what information is shared/transmitted/disclosed and for what purposes?

3.11 If there is such transmission/sharing of personal information, how is the information secured for transmission—what security measures are used to prevent unauthorized access during transmission, *i.e.*, encryption, *etc.*?

3.12 If there is sharing or transmission to other information systems, with what other non-FCC organizations, groups, and individuals will the information be shared?
(Check all that apply and provide a brief explanation)

- Other Federal agencies:
- State, local, or other government agencies:
- Businesses:
- Institutions:
- Individuals:
- Other groups:

If there is no "matching agreement," *e.g.*, *Memorandum of Understand (MOU)*, *etc.*, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.13 What kind of “matching agreement,” *e.g.*, *Memorandum of Understanding (MOU)*, *etc.*, as defined by 5 U.S.C. 552a(u) of the Privacy Act, as amended, is there to cover the information sharing and/or transferal with the external organizations?

3.14 Is this a new or a renewed matching agreement?

- New matching agreement
- Renewed matching agreement

Please explain your response:

3.15 Has the matching agreement been reviewed and approved (or renewed) by the FCC’s Data Integrity Board, which has administrative oversight for all FCC matching agreements?

- Yes
If yes, on what date was the agreement approved:
- No

Please explain your response:

3.17 How is the information that is covered by this system of records notice (SORN) transmitted or disclosed with the external organization(s) under the *MOU* or other “matching agreement?”

3.18 How is the shared information secured by the recipient under the *MOU*, or other “matching agreement?”

Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:

OMB regulations require Federal agencies to insure that the information/data that they collect and use meets the highest possible level of quality and integrity. It is important, therefore, that the information the Commission’s information systems use meets the “benchmark standards” established for the information.

4.1 How will the information that is collected from FCC sources, including FCC employees and contractors, be checked for accuracy and adherence to the Data Quality guidelines?

(Please check all that apply)

- Information is processed and maintained only for the purposes for which it is collected.
- Information is reliable for its intended use(s).
- Information is accurate.
- Information is complete.
- Information is current.
- Not applicable:

Please explain any exceptions or clarifications:

The Office of Inspector General (OIG) is exempt from the Data Quality guidelines requirements.

If the Data Quality Guidelines do not apply to the information in this information system, please skip to **Section 5.0 Safety and Security Requirements:**

4.2 Is any information collected from non-FCC sources; if so, how will the information sources be checked for accuracy and adherence to the Data Quality guidelines?

(Please check all that apply and provide an explanation)

- Yes, information is collected from non-FCC sources:
 - Information is processed and maintained only for the purposes for which it is collected:
 - Information is reliable for its intended use(s):
 - Information is accurate:
 - Information is complete:
 - Information is current:
 - No information comes from non-FCC sources:

Please explain any exceptions or clarifications:

If the information that is covered by this system of records notice (SORN) is not being aggregated or consolidated, please skip to Question 4.5.

4.3 If the information that is covered by this system of records notice (SORN) is being aggregated or consolidated, what controls are in place to insure that the information is relevant, accurate, and complete?

4.4. What policies and procedures do the information system's administrators and managers use to insure that the information adheres to the Data Quality guidelines both when the information is obtained from its sources and when the information is aggregated or consolidated for the use by the bureaus and offices?

4.5 How often are the policies and procedures checked routinely—what type of annual verification schedule has been established to insure that the information that is covered by this system of records notice adheres to the Data Quality guidelines?

Section 5.0 Safety and Security Requirements:

5.1 How are the records/information/data in the information system covered by this system of records notice (SORN) stored and maintained?

- IT database management system (DBMS)
- Storage media including CDs, CD-ROMs, *etc.*
- Electronic tape
- Paper files
- Other:

5.2 Is the information collected, stored, analyzed, or maintained by this information system available in another form or from another source (other than a “matching agreement” or *MOU*, as noted above)?

- Yes
 No

Please explain your response:

The information that the Criminal Investigative Files information system collects, uses, and maintains, including the PII that is covered by FCC/OIG-1, “Criminal Investigative Files” SORN, is obtained from information concerning including present and former FCC employees, and contractors and other individuals who do business with the FCC who are or have been the subjects of the OIG's criminal investigations.

5.3 Is the information system covered by this system of records notice (SORN) part of another FCC information system that collects personally identifiable information (PII)?

- Yes
 No

Please explain your response:

As noted in Question 1.6, the Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, “Criminal Investigative Files” SORN, is a "stand alone" information system with no links to either FCC or non-FCC information systems.

If this information system is not part of another FCC information system, please skip to Question 5.7.

5.4 If the information system (under review here) has personally identifiable information (PII) and is part of another FCC information system, is there a transfer of records/data/information between these two FCC information system(s)?

- Yes
 No

Please explain your response:

5.5 If the information system’s personally identifiable information (PII) is part of another FCC information system, does the information system have processes and/or applications that are part of those from the other FCC information systems?

- Yes
 No

Please explain your response:

5.6 If either or both such situations, as noted in Questions 5.4 and 5.5 exist, what security controls are there to protect the PII information and to prevent unauthorized access?

- Not applicable.

Please explain your response:

5.7 Would the unavailability of this information system prevent the timely performance of FCC operations?

- Yes
 No

Please explain your response:

The Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, “Criminal Investigative Files” SORN, performs a necessary a function for the Commission. This information system collects, stores, analyzes, maintains, and uses the data, *e.g.*, documents, records, files, and other data, *etc.*, related to information concerning present and former FCC employees, contractors and others who do business with the FCC, who are or have been the subjects of the OIG's criminal investigations. This information system is necessary for the FCC's use in these criminal investigations. Without this information system, it would not be possible for the FCC:

- (1) To carry out its responsibilities to prevent or detect fraud, waste, or abuse;
- (2) To conduct and supervise audits and investigations relating to the FCC's programs and operations; and
- (3) To inform the Chairman of the FCC about problems and deficiencies in the Commission's programs and operations; and
- (4) To suggest corrective action that will address the irregularities, problems, or deficiencies identified by the FCC's Inspector General.

5.8 Will the information system include an externally facing information system or portal such as an Internet accessible webpage application at www.fcc.gov or other URL that allows customers/users to access development, production, or internal FCC networks, and which may pose potential risks to the information's security?

- Yes
 No

Please explain your response:

The Criminal Investigative Files information system is an internal FCC information system.

If the information is collected by some method or mechanism other than the externally facing information system portal at www.fcc.gov or other URL, please skip to Question 5.11.

5.9 If the information is collected via www.fcc.gov or other URL from the individuals, how does the information system notify users about the Privacy Notice:

- Link to the FCC's privacy policies for all users:
 Privacy notice displayed on the webpage:
 Privacy notice printed at the end of the form or document:
 Web site uses another method to alert users to the Privacy Act Notice, as follows:
 If there is no link or notice, why not:

5.10 If a privacy notice is displayed, which of the following are included?

- Proximity and timing—the privacy notice is provided at the time and point of data collection.
 Purpose—describes the principal purpose(s) for which the information will be used.
 Authority—specifies the legal authority that allows the information to be collected.

- Conditions—specifies whether providing the information is voluntary, and the effects, if any, of not providing it.
- Disclosures—specify the routine use(s) that may be made of the information.
- Not applicable, as information will not be collected in this way.

Please explain your response:

5.11 Will the information system include another customer-facing website not on www.fcc.gov or other URL?

- Yes
- No

Please explain your response:

As noted in Question 5.8, the Criminal Investigative Files information system is an internal FCC information system.

If the information is collected by some method or mechanism in addition to or other than via the FCC Internet website at www.fcc.gov or the FCC Intranet for FCC employees and contractors working at the FCC, please skip to Question 5.14.

5.12 If the information system has a customer-facing website via the FCC Intranet for FCC employees and contractors working at the FCC, does this web site(s) have a Privacy Act Notice and how is it displayed?

- Yes
 - Notice is displayed prominently on this FCC Intranet web site:
 - Link is provided to a general FCC Privacy Notice for all users:
 - Privacy Notice is printed at the end of the form or document:
 - Website uses another method to alert users to the Privacy Act Notice:
- No:

If there is no Privacy Act Notice, please explain why not:

5.13 If a privacy notice is displayed, which of the following information is included?

- Proximity and timing—the privacy notice is provided at the time and point of data collection.
- Purpose—describes the principal purpose(s) for which the information will be used.
- Authority—specifies the legal authority that allows the information to be collected.
- Conditions—specifies if providing the information is voluntary, and the effects, if any, of not providing it.
- Disclosures—specify the routine use(s) that may be made of the information.
- Not applicable, as information will not be collected in this way.

Please explain your response:

If information is collected by some method or mechanism other than by fax, e-mail, FCC form(s), or regular mail, please skip to Question 5.16.

5.14 If information is collected from the individual by fax, e-mail, FCC form(s), regular mail, or some other means not listed above, how is the privacy notice provided?

- Privacy notice is on the document, *e.g.*, FCC form, *etc.*
- Privacy notice displayed on the webpage where the document is located:
- Statement on the document notifies the recipient that they may read the FCC Privacy Notice at www.fcc.gov.
- Website or FCC document uses other method(s) to alert users to the Privacy Act Notice: The OIG Home Page has a link to the FCC Privacy Policy at: <http://www.fcc.gov/fccprivacypolicy.html>.
- Privacy notice is provided via a recorded message or given verbally by the FCC staff handling telephone calls:
- No link or notice, please explain why not:
- Not applicable, as personally identifiable information (PII) will not be collected.

5.15 If a privacy notice is displayed, which of the following information is included?

- Proximity and timing—the privacy notice is provided at the time and point of data collection.
- Purpose—describes the principal purpose(s) for which the information will be used.
- Authority—specifies the legal authority that allows the information to be collected.
- Conditions—specifies if providing the information is voluntary, and the effects, if any, of not providing it.
- Disclosures—specify the routine use(s) that may be made of the information.
- Not applicable, as information will not be collected in any other way.

Please explain your response:

If there is no access to the information system from outside the FCC via www.FCC.gov or other URL, please skip to Question 5.17.

5.16 If consumers may access the information and/or the information system on-line via www.FCC.gov, does it identify ages or is it directed to people under 13 years old?

- Yes
- No

Please explain your response:

5.17 Will the FCC use the newly obtained information or revised information in this information covered by the existing system of records notice (SORN) to make a determination about the individual?

- Yes
- No

Please explain your response:

The FCC's Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is used to gather, store, analyze, and use information on present and former FCC employees and contractors and other individuals who do business with the Commission, who are or have been the subjects of the OIG's criminal

investigations conducted. This information system is necessary for the FCC's use in these criminal investigations. Without this information system, it would not be possible for the FCC:

- (1) To carry out its responsibilities to prevent or detect fraud, waste, or abuse;
- (2) To conduct and supervise audits and investigations relating to the FCC's programs and operations; and
- (3) To inform the Chairman of the FCC about problems and deficiencies in the Commission's programs and operations; and
- (4) To suggest corrective action to address the irregularities, problems, or deficiencies identified by the FCC's Inspector General.

5.18 Do individuals have the right to decline to provide personally identifiable information (PII)?

- Yes
 No

Please explain your response:

The FCC's Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is used to gather, store, analyze, and use information present and former FCC employees and contractors and other individuals who do business with the Commission, who are or have been the subjects of the OIG's criminal investigations. Since this information is essential to the OIG's efforts to prevent or to detect fraud, waste, or abuse, the OIG requires that individuals must cooperate fully with the OIG, including their obligation to provide their PII as necessary as part of the investigative process, as authorized by the Inspector General Act of 1978, as amended.

5.19 Do individuals have the right to consent to particular uses of their personal information?

- Yes
 No

Please explain your response:

The FCC's Criminal Investigative Files information system, which includes the PII that is covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is used to gather, store, analyze, and use information on present and former FCC employees and contractors and other individuals who do business with the Commission, who are or have been the subjects of the OIG's criminal investigations. Since this information is essential to the OIG's efforts to prevent or to detect fraud, waste, or abuse, the OIG requires that individuals must cooperate fully with the OIG, including their obligation to provide their PII as part of the investigative process, as authorized by the Inspector General Act of 1978, as amended.

If individuals do not have the right to consent to the use of their information, please skip to Question 5.22.

5.20 If individuals have the right to consent to the use of their personal information, how does the individual exercise this right?

5.21 What processes are used to notify and to obtain consent from the individuals whose personal information is being collected?

5.22 Is the information, *i.e.*, records, data, documents, *etc.*, that the information system collects, uses, maintains, *etc.*, being used to produce reports on the individuals whose PII is part of this information covered by the system of records notice (SORN)?

- Yes
- No

Please explain your response:

In compliance with Section 5 of the Inspector General Act, as amended, 5 U.S.C. App. § 5, OIG prepares a semi-annual report summarizing the activities and accomplishments of OIG that it submits to the Chairman of the FCC. Information taken from the Criminal Investigative Files information system, including PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, may be included in this semi-annual report.

5.23 What safeguards and security measures, including physical and technical access controls, are in place to secure the information and to minimize unauthorized access, use, or dissemination of the information that is stored and maintained in the information system?

(Check all that apply)

- Account name
- Passwords
 - Accounts are locked after a set period of inactivity
 - Passwords have security features to prevent unauthorized disclosure, *e.g.*, "hacking"
 - Accounts are locked after a set number of incorrect attempts
 - One time password token
 - Other security features:
- Firewall
- Virtual private network (VPN)
- Data encryption:
- Intrusion detection application (IDS)
- Common access cards (CAC)
- Smart cards:
- Biometrics
- Public key infrastructure (PKI)
- Locked file cabinets or fireproof safes
- Locked rooms, with restricted access when not in use
- Locked rooms, without restricted access
- Documents physically marked as "sensitive"
- Guards
 - Identification badges
 - Key cards
 - Cipher locks
 - Closed circuit TV (CCTV)
- Other:

5.24 Please explain what staff security training and other measures are in place to assure that the security and privacy safeguards are maintained adequately?

All FCC employees and contractors who work with the information that is collected, used, stored and maintained in the Criminal Investigative Files information system, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, are required to complete privacy training.

In addition, the OIG staff provides various notices and warnings to the employees and contractors who have access that the PII is not to be shared or disclosed without authorization.

5.25 How often are security controls reviewed?

- Six months or less:
- One year: The OIG staff reviews the security controls in the Criminal Investigative Files information system at least annually.
- Two years
- Three years
- Four years
- Five years
- Other:

5.26 How often are personnel (information system administrators, users, information system/information system developers, contractors, *etc.*) who use the information system trained and made aware of their responsibilities for protecting the information?

- There is no training
- One year: In September 2006, the FCC inaugurated a Commission-wide privacy training program, which has required all FCC employees and contractors to complete an initial privacy training course and to take a privacy refresher course annually thereafter, as required by the Office of Management and Budget (OMB).
- Two years
- Three years
- Four years
- Five years
- Other:

If privacy training is provided, please skip to Question 5.28.

5.27 What are the safeguards to insure that there are few opportunities for disclosure, unavailability, modification, and/or damage to the information system covered by this system of records notice (SORN), and/or prevention of timely performance of FCC operations if operational training is not provided?

5.28 How often must staff be “re-certified” that they understand the risks when working with personally identifiable information (PII)?

- Less than one year:
- One year: The OIG staff requires that the personnel who use the Criminal Investigative Files information system, including both FCC employees and contractors, must be trained at once a year about their responsibilities for protecting the PII contained in this information system.
- Two years
- Three or more years
- Other re-certification procedures:

5.29 Do the Commission's training and security requirements for this information system that is covered by this system of records notice (SORN) conform to the requirements of the Federal Information Security Management Act (FISMA)?

- Yes
 No

Please explain your response:

The Criminal Investigative Files information system is a non-major information system, and as such, it is exempt from the FISMA regulations.

If the Privacy Threshold Analysis was completed recently as part of the information system's evaluation, please skip to Question 5.34.

5.30 What is the potential impact on individuals on whom the information is maintained in the information system(s) if unauthorized disclosure or misuse of information occurs? (check one)

- Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual.
 Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual.
 Results in significant harm, embarrassment, inconvenient, or unfairness to the individual.

Please explain your response:

The Criminal Investigative Files information system includes PII on present and former FCC employees and contractors and other individuals who do business with the Commission, who are or have been the subjects of criminal investigations conducted by the Office of Inspector General (OIG). Since this PII by its very nature may be very sensitive, it is highly likely that any inadvertent disclosure would be detrimental to the effected individuals.

5.31 Is the impact level for the information system(s) covered by this system of records notice (SORN) consistent with the guidelines as determined by the FIPS 199 assessment?

- Yes
 No

Please explain your response:

The Criminal Investigative Files information system is a non-major information system, as and such, it is exempt from the FIPS 199 assessment guidelines.

5.32 Has a "Certification and Accreditation" (C&A) been completed for the information system(s) covered this system of records notice (SORN)?

- Yes
 No

If yes, please explain your response and give the C&A completion date:

The Criminal Investigative Files information system is a non-major information system, and as such, it is exempt for the Certification and Accreditation (C&A) requirements.

5.33 Has the Chief Information Officer (CIO) and/or the Chief Security Officer (CSO) designated this information system as requiring one or more of the following:

- Independent risk assessment:
 Independent security test and evaluation:

- Other risk assessment and/or security testing procedures, *etc.* :
- Not applicable: Criminal Investigative Files information system is a non-major information system, and as such, it is exempt from the independent risk assessment, independent security test and evaluation, and other risk assessment and/or security testing procedures.

5.34 Is the system using technology in ways that the Commission has not done so previously, *i.e.*, Smart Cards, Caller-ID, *etc*?

- Yes
- No

Please explain your response:

The Criminal Investigative Files information system does not use any technology in the process of collecting, storing, maintaining, and/or using the data, including documents and records, in this information system that impacts the privacy of individuals.

5.35 How does the use of the technology affect the privacy of the general public and FCC employees and contractors?

The Criminal Investigative Files information system does not use any technology in the process of collecting, storing, maintaining, and/or using the data, including documents and records, in this information system. The data in this information system consist of electronic data and records that are stored on the FCC's computer network databases and paper documents, records, and files. The OIG only uses the computer databases to collect and store the PII it collects.

5.36 Will the information system that is covered by this system of records notice (SORN) include a capability to identify, locate, and/or monitor individuals?

- Yes
- No

Please explain your response:

The OIG staff attorneys use the Criminal Investigative Files information system to collect and store documents and records, *e.g.*, case files covering criminal investigations, investigative files relating to internal FCC employees' complaints, and other investigative reports and documents, *i.e.*, correspondence, notes, attachments, and working papers, as part of the OIG's duties to prevent or to detect fraud, waste, or abuse. This information system has no other uses, nor does it have any capability to identify, locate, or monitor these individuals.

If the information system does not include any monitoring capabilities, please skip to **Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):**

5.37 If the information system includes these technical capabilities identified in Questions 5.34 through 5.36 above, what kinds of information will be collected as a function of the monitoring of individuals?

5.38 Does the information system covered by this system of records notice (SORN) contain any controls, policies, and procedures to prevent unauthorized monitoring?

- Yes
- No

Please explain your response:

Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):

6.1 Does this system of records notice (SORN) require non-FCC employees and contractors to perform any paperwork or recordkeeping activities?

Yes, individuals, who are not FCC employees or contractors, are required to complete paperwork or recordkeeping functions or activities, *i.e.*, fill out forms and/or licenses, participate in surveys, and or maintain records *etc.*

Please explain your response:

No, individuals, who are not FCC employees or contractors, are not required to perform any paperwork or recordkeeping functions or activities

Please explain your response:

The Criminal Investigative Files information system is used to gather, analyze, and use PII that relates to the OIG's investigation of known or alleged fraud, waste, and abuse, or other irregularities or violations of criminal laws and regulations inside the FCC. There are no PRA paperwork or recordkeeping requirements.

No, this system of records notice includes only FCC employees and/or contractors, which exempts it from the PRA. Please skip to **Section 7.0 Correction and Redress:**

6.2 If the website requests information, such as the information necessary to complete an FCC form, license, authorization, *etc.*, has the information collection covered by this system of records notice (SORN) been identified for possible inclusion under the FCC's Paperwork Reduction Act (PRA) requirements?

Yes
 No

Please explain your response:

If there are no PRA information collections associated with the information system or its applications, please skip to **Section 7.0 Correction and Redress:**

6.3 If there are one or more PRA information collections that are covered by this system of records notice (SORN) that are associated with the information system's databases and paper files, please list the OMB Control Number, Title of the collection, and Form number(s) as applicable for the information collection(s):

6.4 If there are any FCC forms associated with the information system(s) covered by this system of records notice (SORN), do the forms carry the Privacy Act notice?

Yes:
 No
 Not applicable—the information collection does not include any forms.

6.5 Have the system managers contacted the Performance Evaluation and Records Management (PERM) staff to coordinate PRA requirements and submission of the information collection to the Office of Management and Budget?

- Yes
- No

Please explain your response:

Section 7.0 Correction and Redress:

7.1 Are the procedures for individuals wishing to inquire whether this system of records notice (SORN) contains information about them consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements?

- Yes
- No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined that under 47 CFR § 0.561 of FCC rules, this system of records is exempt from disclosing to individuals the notification procedures under 47 CFR §§ 0.554 – 0.555 of FCC rules for FCC/OIG-1, “Criminal Investigative Files” SORN.

7.2 Are the procedures for individuals to gain access to their own records/information/data in this information system that is covered by this system of records notice (SORN) consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements?

- Yes
- No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined that under 47 CFR § 0.561 of FCC rules, this system of records is exempt from disclosing to individuals the record access procedures under 47 CFR §§ 0.554 – 0.555 of FCC rules for FCC/OIG-1, “Criminal Investigative Files” SORN.

7.3 Are the procedures for individuals seeking to correct or to amend records/information/data about them in the information system that is covered by this system of records notice (SORN) consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

- Yes
- No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined that under 47 CFR § 0.561 of FCC rules, this system of records is exempt from disclosing to individuals the procedures to correct or to amend information about themselves under 47 CFR §§ 0.556 – 0.558 of FCC rules for FCC/OIG-1, “Criminal Investigative Files” SORN.

- 7.4 Does the FCC provide any redress to amend or correct information about an individual covered by this system of records notice (SORN), and if so, what alternatives are available to the individual, and are these consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

Yes
 No

Please explain your response:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined that under 47 CFR § 0.561 of FCC rules, this system of records is exempt from disclosing to individuals the record redress procedures to amend or correct information themselves under 47 CFR §§ 0.556 – 0.558 of FCC rules for FCC/OIG-1, “Criminal Investigative Files” SORN.

If this is a new system of records notice (SORN), please skip to Question 7.6.

- 7.5 Have the sources for the categories of records in the information system(s) covered by this system of records notice (SORN) changed?

Yes
 No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined that under 47 CFR § 0.561 of FCC rules, this system of records is exempt from disclosing the sources for the categories of records in the FCC/OIG-1, “Criminal Investigative Files” SORN.

- 7.6 Does this system of records notice (SORN) claim any exemptions to the notification, access, and correction, and/or amendment procedures as they apply to individuals seeking information about them in this SORN, and if so, are these exemptions consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.561?

Yes
 No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

FCC/OIG-1, "Criminal Investigative Files," SORN is exempt from sections (c)(3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;
2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act; and
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

7.7 What processes are in place to monitor and to respond to privacy and/or security incidents? Please specify what is changing if this is an existing system of records notice (SORN) that is being updated or revised?

The OIG supervisory staff issues periodic reminders to its employees and contractors that the information in the Criminal Investigative Files information system's electronic records and paper files, including the PII covered by FCC/OIG-1, "Criminal Investigative Files" SORN, is "non public for internal use only." The OIG also notifies those who are granted access to the information that they are to keep the information confidential and to safeguard any printed materials.

7.8 How often is the information system audited to ensure compliance with FCC and OMB regulations and to determine new needs?

- Six months or less
- One year
- Two years
- Three years
- Four years
- Five years
- Other audit scheduling procedure(s): This information system is exempt from the auditing requirements under the Inspector General Act.

Section 8.0 Consumer Satisfaction:

8.1 Is there a customer satisfaction survey included as part of the public access to the information covered by this system of records notice (SORN)?

- Yes
- No
- Not applicable

Please explain your response:

The Criminal Investigative Files information system's purposes are to document investigations designed to prevent or detect fraud, waste, or abuse; to conduct and supervise audits and investigations, and to identify problems and deficiencies in the FCC's programs and operations and suggest corrective actions.

A customer satisfaction survey is not appropriate or applicable to these purposes.

If there are no Consumer Satisfaction requirements, please skip to **Section 9.0 Risk Assessment and Mitigation:**

8.2 Have any potential Paperwork Reduction Act (PRA) issues been addressed prior to implementation of the customer satisfaction survey?

- Yes
- No

Please explain your response:

If there are no PRA issues, please skip to **Section 9.0 Risk Assessment and Mitigation:**

8.3 If there are PRA issues, were these issues addressed in the PRA component of this PIA template?

- Yes
- No

Please explain your response:

Section 9.0 Risk Assessment and Mitigation:

9.1 What are the potential privacy risks for the information covered by this system of records notice (SORN), and what practices and procedures have you adopted to minimize them?

Risks:	Mitigating factors:
a. Some of the information in the Criminal Investigative Files information system's PII is contained in electronic records that are stored in the OIG's servers, which are part of the FCC's computer network databases.	a. PII that is contained in electronic records is protected in the OIG's servers that are used exclusively by OIG, although they are part of the FCC's computer network. No other bureau or office staff may have access to these servers. These servers use the FCC's security protocols that require users to provide log-ins, passwords, and other access rights to these records.
b. Some of the information in the Criminal Investigative Files information system's PII is contained in paper documents that are stored in file cabinets.	b. The file cabinets that store the paper document are located in non-public areas so that the presence of unauthorized individuals would be readily noticed. The file cabinets are locked at the close of business or when not in use.

9.3 What is the projected production/implementation date for the database(s):

Initial implementation: April 2006
 Secondary implementation: April 2009
 Tertiary implementation:
 Other implementation:

9.4 Are there any ancillary and/or auxiliary information system(s) applications linked to this information system that is covered by this system of records notice (SORN), which may also require a Privacy Impact Assessment (PIA)?

Yes

No

If so, please state the application(s), if a Privacy Impact Assessment (PIA) has been done, and the completion date for PIA:

At this time, the staff in the Office of Inspector General (OIG) does not anticipate that there will be any new ancillary or auxiliary information systems linked to the Criminal Investigative Files information system.