Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the
Personal Security Files
October 30, 2009

Information System: Personal Security Files
FCC Bureau/Office: Office of the Managing Director, Administrative Operations (OMD-AO)
Division: Security Operations Center (SOC)

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—Development date:
☒ Revised or upgraded information system—Revision or upgrade date: September 2006

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

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

Please explain your response:

The Personal Security Files information system was revised to conform to the requirements of Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors, " (August 27, 2004) and associated guidance provided in OMB Memorandum M-06-06 (February 17, 2006). HSPD-12 required the FCC and other Federal agencies to have these requirements in effect on October 26, 2006.

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 Personal Security Files information system, including the personnally identifiable information (PII) covered by the system of records notice (SORN), FCC/OMD-16, "Personal Security Files" pre-dates the implementation of the Privacy Impact Assessment requirement. The SORN was published in the *Federal Register* on September 25, 2006 (71 FR 55787, 55790).

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:

As noted in Question 1.1, this information system was revised to conform to the HSPD-12 requirements in 2006. As part of this process, the FCC changed the name of the SORN from FCC/Central-6, "Personnel Investigative Records" to FCC/OMD-16, "Personal Security Files" when the SORN was published in the *Federal Register* on September 25, 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 Security Operations Center (SOC) staff has made only minor changes to the Personal Security 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 Personal Security Files information system is a "stand alone" information system. It has no electronic links to other FCC or non-FCC information systems.

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: Relatives' names, birth date(s), home address, and citizenship; relatives who work for the Federal government.
- ☒ 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: Inquiries with law enforcement agencies, employers, and reports of action after the Office of Personnel Management or FBI Section 8(d) Full Field Investigation; Notice of Security Investigation and other information developed from such Certificates of Clearance, e.g., security clearance date(s), requests for appeals, witness statements, investigator's notes, security violations, violation circumstances, and agency actions taken, *etc*.
- ☒ Background investigation history: Investigating agency, investigation dates, security clearance(s), and grant date(s), and position sensitivity level(s); and miscellaneous

investigation comments; reports about individual's qualifications for a position, e.g., employee/applicant's employment/work history, summary report of investigation, results of suitability decisions, employment references and contact information; and educational/training institutions attended, degrees and certifications earned, and educational and training references.

- ☒ National security data: Security classification, types and dates of investigations.
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☒ Other information: FCC organizational unit, *e.g.*, bureau/office, division, etc., and position title; information taken to investigate allegations of FCC employee's misconduct; information taken to investigate miscellaneous complaints not covered by FCC formal or informal grievance procedure; information need to conduct inquiries under the "President's Program to Eliminate Waste and Fraud in Government; and information needed to investigate violence, threats, harassment, intimidation, or other inappropriate behavior causing an FCC employee, contractor, or visitor(s) to fear for his/her personal safety in FCC workplace; case number, victim's name, office telephone number, room number, organizational unit, duty station, position, supervisor, supervisor's telephone number, location of incident, activity at time of incident, circumstance surrounding incident, perpetrator, name(s) and telephone number(s) of witness(es), injured party(s), medical treatment(s), medical report, property damages, report(s) to policy and/or Federal Protective Services, and related miscellaneous information; and information obtained from SF-85, SF-85P, SF-86, and SF-87 forms; summary reports from OPM or another Federal agency conducting background investigations; and results of adjudications and security violations.

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
☐ FCC Contractor badge number (Contractor ID)
☐ Law enforcement data
☐ Background investigation history
☐ National security data
☐ Communications protected by legal privileges
☐ Digital signature
☐ Other information:

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)

☐ 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:

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:

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

☒ Personal information from FCC employees: PII sufficient to satisfy the background investigation criteria requirements.
☒ Personal information from FCC contractors: PII sufficient to satisfy the background investigation criteria requirements.
☒ Personal information from non-FCC individuals and/or households: PII sufficient to satisfy the background investigation criteria requirements.
☐ Non-personal information from businesses and other for-profit entities:
☐ Non-personal information from institutions and other non-profit entities:
☐ Non-personal information from farms:
☐ Non-personal information from Federal Government agencies:
☐ Non-personal information from state, local, or tribal governments:

☐ Other sources:

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:

The PII covered by FCC/OMD-16, "Personal Security Files," SORN may included all relevant data, from both FCC and non-FCC sources, *etc.*, including Federal, state, local and tribal law enforcement agencies, educational institutions, medical institutions, etc., that are deemed adequate and necessary to meet the standards and requirements of the FCC's security office staff and Federal regulations to conduct a full personal background investigation of all FCC employees, contractors working at the FCC, and the suitability of students, interns, or volunteers to the extent that their duties require access to FCC and other Federal facilities, information, systems, or applications, and to document such determinations, *etc*.

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):
☐ Non-FCC information system and information system name(s):
☒ FCC employee name(s)
☐ (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 are being shared or transferred from the other information system(s)?

☒ Yes
☐ No

Please explain your response:

The information covered by FCC/OMD-16, "Personal Security Files," SORN is intended to create a personal background file on each FCC employee as required by Federal employment and security regulations.

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, *i.e.*, SSN, name, home telephone number, fingerprint, voice print, *etc*.?

☒ Yes
☐ No

Please explain your response:

As noted in Question 1.8, the Personal Security Files information system includes such PII as the individual's name, SSN, birth date, home address and home telephone number, *etc*, all of which can be to identify the individual.

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

☒ Yes
☐ No

Please explain your response:

As noted in Question 1.12, the information in the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN is intended to create a personal background file on each FCC employee as required by Federal employment and security regulations.

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 SORN is titled FCC/OMD-16, "Personal Security Files."

Please provide the citation that was published in the *Federal Register* for the SORN: This SORN was published on September 25, 2006 (71 FR 55787, 55790).

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,"[2] 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 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

[2] Information about individuals in a system of records may routinely be disclosed for the following conditions, *e.g.*, "routine uses"; however, in each of these routine uses that are checked, the FCC will determine whether disclosure of the information, *i.e.*, records, files, documents, and data, *etc*., is compatible with the purpose(s) for which the information has been collected

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 <u>new</u> 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:

Most personally identifiable information (PII) in this information system that is covered by FCC/OMD-16, "Personal Security Files," SORN is not classified; however, in some cases, records of certain individuals, or portions of some records may have national defense/foreign policy classifications.

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 PII covered by FCC/OMD-16, "Personal Security Files," SORN is maintained in the Security Operations Center (SOC) of the Administrative Operations Division in the Office of the Managing Director (OMD-AO).

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:

FCC/OMD-16, "Personal Security Files," SORN includes the PII on the following:

(1) Current and former FCC employees, including Commission retirees and those who resigned from the Commission, other Federal employees, applicants for employment in the Federal service or contracts, contractors working at the FCC, experts, instructors, consultants to the FCC and other Federal programs, visitors, and all others who may require regular, on-going access to FCC and other Federal facilities, information technology systems, or information classified in the interest of national security, and individuals formerly in any of these positions;

(2) Individuals who are authorized to perform or to use services provide in FCC facilities, *e.g.*, FCC credit union and employee assistance program staff (EAP); and

(3) Individuals who are neither applicants nor employees of the Federal Government, but who are or were involved in Federal programs under a co-operative agreement, e.g., students and interns.

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 in this information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN are consistent with the requirements of Homeland Security Presidential Directive (HSPD) 12 and OMB guidance in Memorandum M-06-06. The categories include:

(1) Data needed to identify an individual, including: individual's last, first, middle names (filed alphabetically by last name), and former name(s) (as applicable); Social Security Number; date of birth; birthplace; home address; home telephone number(s); residential history; organizational unit; position title;

(2) Individual's citizenship; security classification; types and dates of investigations; and agency conducting investigation, investigation dates, security clearance(s) and grant date(s), and position sensitivity level(s); and miscellaneous investigation comments;

(3) Names of relatives; birth date(s), home address, and citizenship; relatives who work for the Federal government;

(4) Reports about the individual's qualifications for a position, e.g., employee/applicant's employment/work history, summary report of investigation, results of suitability decisions, employment references and contact information; and educational/training institutions attended, degrees and certifications earned, and educational and training references;

(5) Information needed to investigate an individual's character, conduct, and behavior in the community where he or she lives or lived; criminal history, e.g., arrests and convictions for violations against the law; mental health history; drug use; financial information, e.g., income tax return information and credit reports; reports of interviews with present and former supervisors, co-workers, associates, educators, and other related personal references and contact information;

(6) Reports of inquiries with law enforcement agencies, employers, and reports of action after the Office of Personnel Management or FBI Section 8(d) Full Field Investigation; Notices of Security Investigation and other information developed from the above described Certificates of Clearance, e.g., date of security clearances, requests for appeals, witness statements, investigator's notes, security violations, circumstances of violations, and agency action(s) taken;

(7) Information needed to investigate allegations of FCC employee's misconduct;

(8) Information needed to investigate miscellaneous complaints not covered by the FCC's formal or informal grievance procedure;

(9) Information needed to conduct inquiries under the "President's Program to Eliminate Waste and Fraud in Government;" and

(10) Information needed to investigate violence, threats, harassment, intimidation, or other inappropriate behavior causing an FCC employee, contractor, or visitor(s) to fear for his/her personal safety in the FCC workplace: case number, victim's name, office telephone number, room number, organizational unit, duty station, position, supervisor, supervisor's telephone number, location of incident, activity at time of incident, circumstances surrounding the incident, perpetrator, name(s) and telephone number(s) of witness(es), injured party(s), medical treatment(s), medical report, property damages, report(s) to police and/or Federal Protective Services, and related miscellaneous information.

(11) Information obtained from SF-85, SF-85P, SF-86, and SF-87 forms; summary reports from OPM or another Federal agency conducting background investigations; and results of

adjudications and security violations. (Note: This system of records does not duplicate or supersede the Office of Personnel Management (OPM) Central-9 system of records, which covers the investigations OPM and its contractors conduct on behalf of other agencies.)

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:

Depending upon the purpose(s) for the investigation under which the U.S. government is authorized to ask for this information, the legal authorities for the information system(s) covered by FCC/OMD-16, "Personal Security Files," SORN collects, maintains, and uses the personally identifiable information (PII) include 5 U.S.C. 1303, 1304, 3301, 7902, 9101; 42 U.S.C. 2165 and 2201; 50 U.S.C. 781 to 887; 5 CFR Parts 5, 732, and 736; Executive Orders 9397, 10450, 10865, 12196, 12333, 12356, and 12674; and Homeland Security Presidential Directive (HSPD) 12, “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004.

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:

To comply with the requirements of HSPD-12, FCC/OMD-16, "Personal Security Files," SORN that allows the FCC Security Officer and the Personnel Security Specialist to use this information to document and support decisions:

(1) To determine compliance with Federal regulations and/or to make a determination about an individual's suitability, eligibility, and fitness for Federal employment, access to classified information or restricted areas, position sensitivity, security clearances, evaluations of qualifications, and loyalty to the United States, and to document such determinations;

(2) To evaluate an applicant’s qualifications and suitability to perform contractual services for the U.S. Government and to document such determinations;

(3) To evaluate the eligibility and suitability of students, interns, or volunteers to the extent that their duties require access to FCC and other Federal facilities, information, systems, or applications, and to document such determinations;

(4) To respond to a written inquiry conducted under the “President's Program to Eliminate Waste and Fraud in the Government;”

(5) To take action on, or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees, and to counsel employees; and

(6) To document security violations and supervisory actions taken.

2.7 Have there been any changes to the "Routine Uses"[3] under which disclosures are permitted to "third parties" as noted in the system of records notice (SORN)?

☒ Yes
☐ No

If the Routine Uses have changed, what changes were made:

(check all that apply and explain the changes)

☒ Adjudication and litigation: Court or adjudicative body.
☐ 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 program management and oversight by NARA, DOJ, and/or OMB:
☒ Labor relations:
☒ Law enforcement and investigations:
☒ National security and intelligence matters:
☐ Program partners, *e.g.*, WMATA:
☒ Breach of Federal data: Required by OMB Memorandum M-07-16 (May 22, 2007).
☒ Others Routine Use disclosures not listed above: Litigation by the Department of Justice (DOJ)

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:

The FCC does not permit information in FCC/OMD-16, "Personal Security Files," SORN to be disclosed to 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

[3] Information about individuals in a system of records may routinely be disclosed for the following conditions, *e.g.*, "routine uses"; however, in each of these routine uses that are checked, the FCC will determine whether disclosure of the information, *i.e.*, records, files, documents, and data, *etc*., is compatible with the purpose(s) for which the information has been collected

Please explain your response:

Information in FCC/OMD-16, "Personal Security Files," SORN is maintained as follows:

(1) Paper files, records, and documents are stored in file folders in locked file cabinets and/or security containers in the SOC office suite, which is alarmed and monitored by the Federal Protective Service (FPS); and

(2) Electronic records, data, and files are stored on the FCC's network computer database. The Information Technology Center (ITC) staff does a monthly security back-up of the information, which is stored on an external hard-drive and a "thumb drive."

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, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN is accessed by the individual's name or his/her Social Security Number (SSN).

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:

Information, in the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN includes paper documents, records, and files and electronic records, data, and files. The safeguards that the system manager has in place to protect unauthorized access to the information covered by the system of records notice (SORN) comply with the requirements of HSPD-12, as follows:

(1) Comprehensive paper records are maintained in file folders and stored in approved security containers, which are locked and located within a secure, access-controlled area. Access is limited to approved security office and administrative personnel who have a need for them in the performance of their official duties, *e.g.*, who have responsibility for suitability determinations. Paper records limited (in number and scope) are kept in the FCC's regional offices and laboratory facilities in locked metal file cabinets in locked rooms.

(2) Comprehensive electronic records are maintained in networked computer database(s). The computer database is secured through controlled access and passwords restricted to Federal employee and contractor security and administrative personnel on a "need to know" basis, *e.g.*, who have a need for them in the performance of their official duties, *e.g.*, who have responsibility for suitability determinations. Access to the records is restricted to those with a specific role in the Personal Identification Verification (PIV) process that requires access to background investigation forms to perform their duties, and who have been given a password to access that part of the system including background investigation records. The FCC Security Office staff maintains an audit trail. Individuals given roles in the PIV process must complete training specific to their roles to ensure that they are knowledgeable about how to protect individually identifiable information. The databases are backed-up on a daily basis to an external hard-drive and also backed up on a "thumb drive." The back-up mechanisms are then stored in a secured area.

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:

The SOC staff maintains and disposes of the information in the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN, in accordance with General Records Schedule 18, item 22a, as approved by the National Archives and Records Administration (NARA), as follows:

(1) Both paper and electronic records are retained during employment or while an individual is actively involved in Federal programs. As appropriate, records are returned to investigating agencies after employment terminates; otherwise, the records are destroyed upon notification of death or not later than five years after the employee's retirement or separation from the FCC, or the employee's transfer to another Federal agency or department, whichever is applicable.

(2) In accordance with NARA guidelines, the FCC destroys paper records are by shredding; and electronic records are destroyed by electronic erasure. Individuals interested in further information about retention and disposal may request a copy of the disposition instructions from the FCC Privacy Act Officer.

The NARA Schedule 18 may be viewed at: http://www.archives.gov/records-mgmt/ardor/grs18.html.

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: SOC staff has responsibility for access and proper use of the information in the Personal Security 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 in the Personal Security Files information system, including the electronic records and data stored in the FCC's computer network databases and the paper documents, files, and records, is restricted to the SOC supervisory staff. Other FCC employees and contractors working at the FCC may be granted access on a "need to know" basis as dictated by their 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: FCC employees and contractors in SOC may be granted access on a "need-to-know" basis as dictated by 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: SOC and ITC supervisory staff.
- ☒ Information system administrators: ITC staff, including both FCC employees and contractors who manage the IT systems that hold and process the PII.
- ☐ Information system developers:
- ☒ FCC staff in this bureau/office: FCC employees in the SOC are granted access based on a "need to know" basis.
- ☐ FCC staff in other bureaus/offices:
- ☒ FCC staff in other bureaus/offices in FCC field offices: FCC employees are granted access based on a "need to know" basis.
- ☒ Contractors: Contractors working at the FCC are granted access based on a "need to know" basis.
- ☐ Other Federal agencies:
- ☐ State and/or local agencies:
- ☐ 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)?

☒ Yes
☐ No

Please explain your response:

The ITC supervisory staff provides periodic privacy training to the IT contractors.

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 contacts that cover the IT contractors who are associated with the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files" SORN, include the required FAR clauses.

3.9 Does the information system covered by this system of records noticed (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:

The Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN, is a "stand alone" information system. Although it has links to other FCC computer networks, no data are transmitted outside the FCC's computer network system, nor are the paper files shared or otherwise made available for use outside the FCC, except as stated in the Routine Uses.

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
☐ Revised 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:

3.16 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?"

3.17 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 information contained in the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN, encompasses the personal (background) information that the FCC is required to gather and maintain as required by Homeland Presidential Directive (HSPD) 12 and OMB Memorandum M-06-06 (February 17, 2006). HSPD-12 also includes regulations to insure that the information that the FCC and other Federal agencies gather and maintain is accurate and adheres to the Data Quality guidelines. The PII covers the following individuals:

(1) Current and former FCC employees, including Commission retirees and those who resigned from the Commission, other Federal employees, applicants for employment in the Federal service or contracts, contractors working at the FCC, experts, instructors, consultants to the FCC and other Federal programs, visitors, and all others who may require regular, on-going access to FCC and other Federal facilities, information technology systems, or information classified in the interest of national security, and individuals formerly in any of these positions;

(2). Individuals who are authorized to perform or to use services provide in FCC facilities, *e.g.*, FCC credit union and employee assistance program staff (EAP); and

(3) Individuals who are neither applicants nor employees of the Federal Government, but who are or were involved in Federal programs under a co-operative agreement, *e.g.*, students and interns.

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:

The information contained in the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files," SORN, encompasses the personal (background) information (PII) that the FCC is required to gather and maintain as required by Homeland Presidential Directive (HSPD) 12. HSPD-12 also includes regulations to insure that the information that the FCC and other Federal agencies gather and maintain is accurate and adhere to the Data Quality guidelines. These regulations apply equally to information that is gathered from non-FCC sources.

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?

Homeland Presidential Directive (HSPD) 12 regulations require the FCC and other Federal agencies to insure that the PII that they gather and maintain on individuals is relevant, accurate, and complete and that adheres to the Data Quality guidelines in those instances and circumstances when it is aggregated or consolidated by the FCC.

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?

The SOC staff follows the HSPD-12 regulations when the staff obtains PII from its sources and when the information is aggregated or consolidated for use by the FCC's bureaus and offices. Such scrupulous compliance insures that the Data Quality guidelines are always met with regards to this PII.

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?

As noted in Question 4.4, the SOC staff follows HSPD-12 regulations concerning PII safety and security. There is no annual verification schedule because the SOC staff do routine checks and verifications on continuous basis background data (BD).

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, and CD-ROMs, *etc.*
☒ Electronic tape
☒ Paper files
☒ Other: External hard drive and "thumb drive" for security back-up.

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 Personal Security Files information system is the information system that the FCC's Security Officer and the Personnel Security Specialist use to collect, store, maintain, and use PII that is necessary to document and support decisions on background investigations, *etc.*, on FCC employees and contractors working at the FCC, as required of HSPD-12.

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 Personal Security Files information system is a "stand alone" information system. It has no electronic links to other FCC or non-FCC information systems.

If this information system is <u>not</u> 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 information covered by FCC/OMD-16, "Personal Security Files," SORN is required under HSPD-12 and other Federal regulations governing personnel hiring, contracting, *etc*. Without the ability to gather, to analyze, and to maintain this PII, the FCC could not conduct satisfactory hiring, employment, contracting programs that will insure that those who are hired as Federal employees, contractors who work at the FCC, and others who are authorized to perform or to use services provided in FCC facilities, those who require regular on-going access to FCC and other Federal facilities, information technology, *etc*., those who are temporary or short-term employees, *i.e*., instructors, consultants, and visitor, and those who are or were involved in Federal programs such as students and interns, *etc*., are granted the necessary security clearances for access to FCC buildings, facilities, and services.

5.8 Will the information system include an externally facing information system or portal such as an Internet accessible web 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 FCC's employment application process includes an externally facing information portal at www.fcc.gov through which applicants may submit their Federal employment application form(s) and accompanying documentation.

If the information is collected by some method or mechanism other than the externally facing information system portal at www.fcc.gov or other ULR, 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 form or document:
☐ Website 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—specifies 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:

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

☐ Yes
☒ No

Please explain your response:

If the information is collected by some method or mechanism 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 web site via the FCC Intranet for FCC employees and contractors working at the FCC, does this web site have a Privacy Act Notice and how is it displayed?

☐ Yes
  ☐ Notice is displayed prominently on this FCC Intranet website:
  ☐ 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—specifies 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 information is 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), or regular mail, how is the privacy notice provided?

☒ Privacy notice is on the document, *e.g.*, FCC form, *etc*.: OMB Form 50.
☐ 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 http://www.fcc.gov/fccprivacypolicy.html.

☐ Website or FCC document uses other method(s) to alert users to the Privacy Act Notice:

☐ Privacy notice is provided via a recorded message or given verbally by the FCC staff handling telephone calls: [Do you ever interview or obtain information orally—if so we probably need an oral privacy notice.]
☒ No link or notice, please explain why not: The FCC gathers the personal contact information from the participating organizations, *i.e.*, Federal agencies, as required under HSPD-12.
☐ 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—specifies 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:

Individuals applying for employment at the FCC via www.FCC.gov would be older than 13 years of age.

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

☒ Yes
☐ No

Please explain your response:

The HSPD-12 regulations require the FCC's Security Operations Center to use the PII in this information system, including data obtained from paper files, records, and documents, and electronic records, files, and data, for the following reasons:

1. To determine compliance with Federal regulations and/or to make a determination about an individual's suitability, eligibility, and fitness for Federal employment, access to classified information or restricted areas, position sensitivity, security clearances, evaluations of qualifications, and loyalty to the United States, and to document such determinations;
2. To evaluate an applicant’s qualifications and suitability to perform contractual services for the U.S. Government and to document such determinations;

3. To evaluate the eligibility and suitability of students, interns, or volunteers to the extent that their duties require access to FCC and other Federal facilities, information, systems, or applications, and to document such determinations;
4. To respond to a written inquiry conducted under the "President's Program to Eliminate Waste and Fraud in the Government;"
5. To take action on, or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees, and to counsel employees; and
6. To document security violations and supervisory actions taken.

All the uses of the information, as enumerated above, that are collected from both FCC and non-FCC sources and are maintained by this information system are covered by FCC/OMD-16, "Personal Security Files," SORN.

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

☒ Yes
☐ No

Please explain your response:

Individuals may decline to provide their PII, which the FCC will collect as part of its responsibilities under HSPD-12 and other Federal employment regulations. However, such an action will likely to terminate any job application process or prevent the individual from gaining access to the FCC's buildings, facilities, and services.

5.19 Do individuals have the right to consent to particular uses of their personal information that pertain to the uses for which the FCC created this system of records?

☐ Yes
☒ No

Please explain your response:

Individuals do not have the right to consent to particular uses of their PII, which the FCC will collects as part of its responsibilities under HSPD-12 and other Federal employment regulations. By signing the employment or background review document, the individual gives his/her consent. Failure to consent is likely to terminate any job application process or prevent the individual from gaining access to the FCC's buildings, facilities, and services.

If individuals do <u>not</u> 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:

The Personal Security Files information system does not produce any reports using the PII that pertains to the background investigations on FCC employees and contractors working at the Commission.

The purposes for collecting maintaining, and using the information, including PII covered by FCC/OMD-16, "Personal Security Files" SORN, are to comply with the requirements of HSPD-12, so that the information that is collected will allow the FCC Security Officer and the Personnel Security Specialist to use this information to document and support decisions:

(1) To determine compliance with Federal regulations and/or to make a determination about an individual's suitability, eligibility, and fitness for Federal employment, access to classified information or restricted areas, position sensitivity, security clearances, evaluations of qualifications, and loyalty to the United States, and to document such determinations;

(2) To evaluate an applicant's qualifications and suitability to perform contractual services for the U.S. Government and to document such determinations;

(3) To evaluate the eligibility and suitability of students, interns, or volunteers to the extent that their duties require access to FCC and other Federal facilities, information, systems, or applications, and to document such determinations;

(4) To respond to a written inquiry conducted under the "President's Program to Eliminate Waste and Fraud in the Government;"

(5) To take action on, or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees, and to counsel employees; and

(6) To document security violations and supervisory actions taken.

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 system covered under FCC/OMD-16, "Personal Security Files," SORN are required to complete privacy training. In addition the SOC staff emphasizes to those with access that this informationthat it is not to be shared or disclosed.

5.25 How often are security controls reviewed?

- ☐ Six months or less
- ☒ One year: The Security Control Center staff requires the security controls to be reviewed at least annually for the Personal Security Files information system.
- ☐ 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:
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other: 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 refresher course each year thereafter, as required by the Office of Management and Budget (OMD).

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
- ☐ Two years
- ☐ Three or more years
- ☒ Other re-certification procedures: The SOC staff must have their security clearance authorizations reviewed every five years.

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 Personal Security Files information system is a "non-major" information system, and as such,it is exempt from the FISMA requirements.

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 HSPD-12 regulations require, at a minimum, that the FCC's Security Operations Center staff must conduct a background investigation and evaluation on all individuals who are allowed access to the FCC's buildings, facilities, and information technology systems. Individuals who are granted higher level of access or are required to pass security clearance must undergo more extensive background investigations. Consequently, the PII data that this information system collects, maintains, and uses, and which is covered by FCC/OMD-16, "Personal Security Files," SORN is quite extensive, *e.g.*, includes a comprehensive collection of PII on the individual. Unauthorized disclosure or misuse of the PII could subject individuals to identity theft and other significant harm, embarrassment, inconvenience, or unfairness.

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 Personal Security Files information system is a "non-major" information system, and as 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 Personal Security Files information system is a "non-major" information system, and as such, it is exempt from the Certification and Accreditation 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: Required by HSPD-12 regulations.
☒ Independent security test and evaluation: Required by HSPD-12 regulations.
☐ Other risk assessment and/or security testing procedures, *etc.*:
☐ Not applicable:

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 Personal Security Files information system is used solely to comply with the requirements of HSPD-12, which include the requirements to determine an individual's suitability and eligibility for Federal service; an individual's suitability to perform contractual services for the U.S. Government; to evaluate an individual's eligibility and suitability for internships and volunteer programs; to respond to situations involving threats, harassment, and violence, *etc.*, and to respond to inquiries concerning waste, fraud, and abuse. This information system does not use technology in ways that the Commission has not done so previously.

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

The FCC is required by OPM regulations and the HSPD-12 requirements to collect the background data and other personally identifiable information (PII) that is included in the paper files and electronic records in the Personal Security Files information system, including the PII covered by FCC/OMD-16, "Personal Security Files" SORN. There are no specific technological impacts.

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 Personal Security Files information system is used to collect PII on individuals, as required by OPM regulations and HSPD-12 requirements, which is elated to the applicable eligibility, suitability, and/or security requirements for current and former FCC and other Federal employees, contractors, consultants, temporary employees, visitors, students, interns, and all others who are granted access to FCC and other Federal buildings, facilities, and technology systems, but there is no capability to identify, locate, and/or monitor 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 contractions, are required to complete paperwork or recordkeeping functions or activities, *i.e.*, fill out forms and/or licensees, participate in surveys, and or maintain records *etc*.

Please explain your response:

The personally identifiable information (PII) contained in the paper files and electronic records that are included in this information system, which are covered by FCC/OMD-16, "Personal Security Files," SORN, also includes information about FCC employees and contractors working at the FCC. FCC employees were required to complete their Federal employment applications prior to hiring. What OPM, FCC, and/or SF Forms are used to gather information?

☐ 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:

☐ 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: What OPM, FCC, and/or SF Forms are used to gather information?

The employment applications and background applications fall under the PRA requirements. All applications, forms, etc., covered by this information system have been approved by OMB under the PRA.

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 this information system's database(s) and paper file(s), please list the OMB Control Number, Title of the collection, 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

FCC Form Number(s) and Title(s):

☐ 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 that the information system covered by FCC/OMD-16, "Personal Security Files," SORN is exempt from disclosing its notification procedure for this system of records, as noted in the 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 that the information system covered by FCC/OMD-16, "Personal Security Files," SORN is exempt from disclosing its record access procedure for this system of records, as noted in the 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 that the information system covered by FCC/OMD-16, "Personal Security Files," SORN is exempt from disclosing its correction or amendment procedures for this system of records, as noted in the 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 that the information system covered by FCC/OMD-16, "Personal Security Files," SORN is exempt from disclosing its contesting record procedure for this system of records, as noted in the 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/OMD-16, "Personal Security 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:

This system of records 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. (Information will be withheld to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the background investigation.)

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 SOC staff issues periodic reminders to its employees and contractors that the information in the Personal Security Files information system's electronic records, data, and files, and the paper documents, files, and records, including the PII covered by FCC/OMD-16, "Personal Telephone Call Detail" SORN, are "non public for internal use only." The SOC staff also notify those granted access to the information that they are to keep the information confidential and to safeguard it from unauthorized disclosure.

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): Although this information system does not have an audit requirement, the SOC staff does have procedures, identified elsewhere in this PIA, noting the administrative protections, privacy training, and access controls that are in place to safeguard the PII contained in this information system covered by FCC/OMD-16, "Personal Security Files," SORN.

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:

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. PII in these paper files and in the electronic records may be inadvertently disclosed.	a. The FCC's Security Operations Center staff who administers FCC/OMD-16 "Personal Security Files," SORN have numerous safeguards in place to minimize the inadvertent disclosure of this PII and the staff is reviewed to undergo a review of their credentials at least every five years.
b. Some of the information system's PII include paper documents that are stored in file cabinets.	b. PII that is contained in paper documents is stored in locked file cabinets, which are located in rooms that are locked when not in use. These rooms have security alarms and are monitored by FPS staff.
c. Some of the PII includes electronic records that are stored in the FCC's computer network databases.	c. PII that is contained in electronic records is protected in the FCC's computer network databases, which require users to provide login's and access rights to these records.

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

Initial implementation: April 2006
Secondary implementation: January 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 Security Control Center does not anticipate that there will be any new ancillary or auxiliary information systems linked to the Personal Security Files information system.