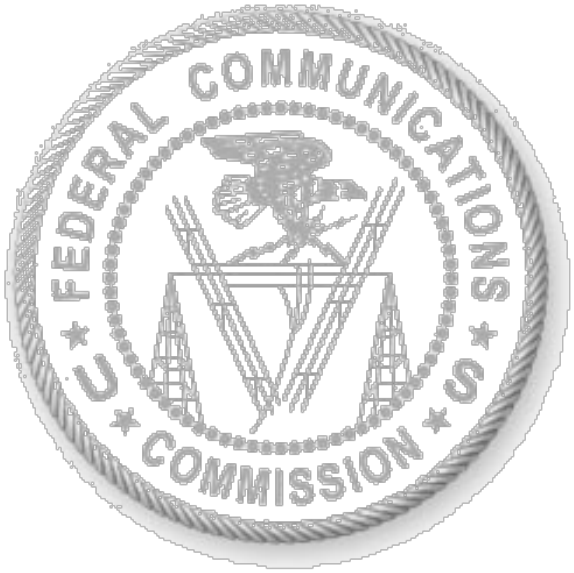
Federal Communications Commission

Office of the Managing Director



Privacy Impact Assessment[1] (PIA) for the FCC/OMD-30, "FCC Visitors Database"

December 31, 2012

FCC Bureau/Office: Office of Managing Director (OMD)
Division: Security Office 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.

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[2]:

☒ New information system—Implementation date: June 2012
☐ Revised or upgraded information system—Revision or upgrade date:

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

☐ Placed in existing information system—Implementation Date: June 2011
☐ Placed in new auxiliary/ancillary information system—Date:
☐ Other use(s)—Implementation Date:

Please explain your response:

The FCC's Security Operations Center (SOC) has created a FCC Visitors Database for people who visit the FCC. The personally identifiable information (PII) in this database is covered by a FCC system of records, FCC/OMD-30, "FCC Visitors Database."

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

☐ Yes
Date:

☒ No

If a PTA has not been done, please explain why not:

The FCC did not create a PTA because it was initially determined that this database would contain PII, and a system of records was created first.

If the Privacy Threshold Assessment (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

Please explain your response:

The FCC Visitors Database is a new information system.

1.4 Has this information system undergone a "substantive change" in the system's format or operating system?

[2] "Information system" is a general term that refers to electronic databases, licensing, and records systems and formats and also to paper based records and filing systems.

☐ Yes
☒ No

If yes, please explain your response:

As noted in Question 1.3, this is a new information system.

1.5 Has the medium in which the information system stores the records or data in the system changed:

☐ Paper files to electronic medium (computer database);
☐ From one IT (electronic) information system to IT system, *i.e.*, from one database, operating system, or software program, *etc*.

Please explain your response:

1.6 What information is the system collecting, analyzing, managing, using, and/or storing, *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:

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:

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: Foreign visitor's passport data, passport issuer data, and visa data.

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: Foreign visitor's passport data, passport issuer data, and visa data.

1.7 What are the sources for the PII and other information that this information system (or database) is collecting:

- ☐ Personal information from FCC employees:
- ☐ Personal information from FCC contractors:
- ☒ Personal information from non-FCC individuals and/or households: Foreign individuals who wish to visit the FCC.
- ☒ Non-personal information from businesses and other for-profit entities: Individuals in business/industry who wish to visit the FCC.
- ☒ Non-personal information from institutions and other non-profit entities: Individuals connected to institutions who wish to visit the FCC.
- ☐ Non-personal information from farms:
- ☐ Non-personal information from Federal Government agencies:
- ☒ Non-personal information from state, local, or tribal governments: State, local, and/or tribal government officials who wish to visit the FCC.
- ☒ Other sources: Individuals, e.g., family members of FCC employees and contractors, etc., who wish to visit the FCC.

1.8 Does this information system have any links to other information systems or databases?

An information system (or database) may be considered as linked to other information systems (or databases) if it has one or more of the following characteristics:

- ☐ The information system is a subsystem or other component of another information system or database that is operated by another FCC bureau/office or non-FCC entity (like the FBI, DOJ, National Finance Center, etc.);
- ☐ The information system transfers or receives information, including PII, between itself and another FCC or non-FCC information system or database;

☒ The information system has other types of links or ties to other FCC or non-FCC information systems or databases;
☐ The information system has other characteristics that make it linked or connected to another FCC or non-FCC information system or database;
☒ The information system has no links to another information system (or database), *i.e.*, it does not share, transfer, and/or obtain data from another system.

If this system has any of these criteria or characteristics, please explain; otherwise please skip to Question 1.11:

The FCC Visitor's Database is a "stand alone" system with no links to other FCC system, although this system does resides on the FCC's network computer databases.

1.9 What PII does the information system obtain, share, and/or use from other information systems?

☐ FCC information system and information system name(s):
☐ Non-FCC information system and information system name(s):
☐ 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)
☐ Personal e-mail address(es)
☐ 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:

1.10 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).

Does a SORN cover the PII in this information system?

☒ Yes
☐ No

If yes, what is this SORN: FCC/OMD-30, "FCC Visitors Database."

Please provide the citation that was published in the *Federal Register* for the SORN: 77 FR 31851 (May 30, 2012).

Section 2.0 System of Records Notice (SORN):

2.1 What is the Security Classification for the information in this SORN, as determined by the FCC Security Officer?

The FCC's Security Operations Center (SOC) has not assigned a security classification to this system of records.

2.2 What is the location of the information covered by this SORN?

This system of records is located in the Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

2.3 What are the categories of individuals in the system of records covered by this SORN?

The records in this system include all visitors to the FCC. These individuals include, but are not limited to U.S. citizens, permanent residents (*i.e.*, green card holders), and foreign nationals.

2.4 What are the categories of records[3] covered by this SORN?

The categories of records in the FCC Visitors Database include, but are not limited to the individual's first and last name, photographic identification (including but not limited to a driver's license, passport, or other types of photo identification), the authority issuing the photo identification, U.S. visa number, FCC point of contact, visitor signature, professional title, organizational affiliation, contact information for the visitor, including but not limited to wireline and wireless (cell) phone numbers, correspondence related to information required to obtain visitor entry to the FCC, and purpose(s) for visiting the FCC.

2.5 Under what legal authority(s) does the FCC collect and maintain the information covered by this SORN?

5 U.S.C. 301; 6 U.S.C. 202; 8 U.S.C. 1103, 1158, 1201, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, 1732; Federal Information Security Act (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 203); and Federal Property and Administrative Act of 1949, as amended.

2.6 What are the purposes for collecting, maintaining, and using the information covered by this SORN?

The purpose of the system is to cover the personally identifiable information (PII) that all visitors to the FCC, including but not limited to U.S. citizens, permanent residents (*i.e.*, green card holders), and foreign nationals, must provide to the FCC's Security Operations Center (SOC) to gain admittance to the FCC headquarters buildings and other FCC facilities.

2.7 What are the Routine Uses under which disclosures are permitted to "third parties," as noted in this SORN?

☒ Adjudication and litigation: Department of Justice (DOJ).
☒ Court or Adjudicative Body:
☐ Committee communications:
☐ Compliance with welfare reform requirements:

[3] This refers to the types of information that this information system or database collects, uses, stores, and disposes of when no longer needed.

☒ Congressional inquiries:
☒ Contract services, grants, or cooperative agreements:
☐ 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:
☒ National security and intelligence matters:
☒ Department of State, Department of Homeland Security, and other Federal agencies:
☒ Program partners, *e.g.*, WMATA:
☒ Breach of Federal data: OMB Memorandum M-07-16 (May 22, 2007).
☒ Others Routine Use disclosures not listed above: Foreign governments.

2.8 What is the FCC's policy concerning whether information covered by this SORN is disclosed to consumer reporting agencies?

Information in the FCC Visitor Database is not disclosed to consumer reporting agencies.

2.9 What are the policies and/or guidelines for the storage and maintenance of the information covered by this SORN?

The information in the FCC Visitors Database includes paper documents, files, and records, which are stored in file cabinets in file cabinets in the Security Operations Center (SOC), and electronic records, files, and data that are stored in the FCC's computer network databases.

2.10 How is the information covered by this SORN retrieved or otherwise accessed?

The information in the FCC Visitors Database may be retrieved by the name of the individual, driver's license number, U.S. passport number, foreign passport number, U.S. visa number, date of birth (DOB), and/or photo ID number.

2.11 What are the safeguards that the system manager has in place to protect unauthorized access to the information covered by this SORN?

The paper documents, records, and files are maintained in file cabinets in the SOC office suite. The file cabinets where these paper documents, files, and records are stored are controlled by on-site personnel when unlocked and locked when not in use. Access to the SOC office suite is through a card-coded main door. Access to the file cabinets is restricted to authorized SOC supervisors, staff, and contractors, whose duties and responsibilities require use of the information.

The electronic records, files, and data are stored in the FCC computer network databases that are secured by limited access card readers. The computer servers themselves are password-protected. Access to the electronic files is restricted to authorized SOC supervisors, staff, and contractors, and to the Information Technology Center (ITC) staff and contractors, who maintain the FCC's computer network. Other FCC employees and contactors may be granted access on a "need-to-

know" basis. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. A *PRIVACY WARNING NOTICE* appears on the monitor screen when records containing information on individuals are first displayed. Information resident on the SOC database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

2.12 What is the records retention and disposition schedule for the information covered by this SORN?

Records in the FCC Visitors Database are retained in accordance with General Records Schedule (GRS) 18, Item 17 approved by the National Archives and Records Administration (NARA). The records disposal is done in accordance with the Commission's disposal policies. Unless retained for specific, on-going security investigations, records of facility access are maintained for one year and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with GRS 18, item 22a, approved by NARA. The records are disposed of in accordance with SOC disposal policies, as follows:

1. All returned day contractor cards will be reused on a daily basis.
2. Transaction data for all FCC Visitors Database cards will be stored using a secure medium and retained for one year in the SOC, which is locked and secured with an alarm system.

In accordance with Homeland Security Presidential Directive (HSPD-12), Personal Identity Verification (PIV) Cards are deactivated within eighteen (18) hours of notification of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with GRS 11, Item 4. PIV Cards are destroyed by burning in an approved Federal burn-facility.

2.13 What are the sources for the information in the categories of records covered by this SORN?

The sources for information in this system are the visitors themselves and/or their agency or organizational sponsor(s) who have been invited to visit or have requested admittance to the FCC headquarters buildings and other FCC facilities as visitors.

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 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 housed?

☒ 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, *i.e.*, 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: The SOC staff and contractors have responsibility for access and proper use of the information in this system's database.
☐ 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's administrators and managers use to determine who gets access to the information in the system's files and/or database(s)?

As noted in Question 2.11, access to the paper documents, files, and records, and the electronic records, files, and data in the FCC Visitors Database, which is stored on the FCC's computer network databases, is restricted to SOC supervisors and staff and the ITC supervisor, staff, and contractors. Other FCC employees and contractors may be granted access only 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: SOC staff and contractors may be granted access only 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 supervisors and staff and ITC supervisors, staff, and contractors.
☒ Information system administrators: ITC supervisors, staff, and contractors.
☐ Information system developers:
☒ FCC staff in this bureau/office: SOC employees and contractors are granted access on a "need to know" basis.
☒ FCC staff in other bureaus/offices: Other FCC employees and contractors are granted access on a "need-to-know" basis.
☒ FCC staff in other bureaus/offices in FCC field offices: FCC employees and contractors are granted access based on a "need to know" basis.
☒ Contractors: Contractors working under SOC and ITC authority.
☒ Other Federal agencies: if the FCC approves a request under the Routine Use (Federal agencies).
☐ State and/or local agencies:
☐ Businesses, institutions, and other groups:
☐ International agencies:
☐ Individuals/general public:

☒ Other groups: if the FCC approves a request under a Routine Use (Foreign governments).

If contractors do not have access to the PII in this system, please skip to Question 3.9.

3.7 What steps have been taken to ensure that the contractors who have access to and/or work with the PII in the system are made aware of their duties and responsibilities to comply with the requirements under subsection (m) "Contractors" of the Privacy Act, as amended, 5 U.S.C. 552a(m)?

The ITC supervisors provide periodic privacy training to the IT contractors who handle the PII that is contained in the FCC Visitors Database.

3.8 What steps have been taken to insure that any Section M contract(s) associated with the information system covered by this SORN include the required FAR clauses (FAR 52.224-1 and 52.224-2)?

The OGC staff has reviewed and signed-off on the Section M contacts for the ITC contractors who manage the FCC Visitors Database, including the PII covered by FCC/OMD-30, "FCC Visitors Database," SORN, as required by Sections 52.224-1 and 52.224-2 of the Federal Acquisition Regulation (FAR).

If there are no information linkages, sharing, and/or transmissions, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.9 If the information system has links to other information systems (or databases), *i.e.*, it shares, transmits, or has other linkages, 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:

Please explain your response:

3.10 If this information system transmits or shares information, including PII, between any other FCC systems or databases, is the other system (or database) covered by a PIA?

☐ Yes
☐ No

Please explain your response:

3.11 Since this information system transmits/shares PII between the FCC computer network and another non-FCC network, what security measures or controls are used to protect the PII that is being transmitted/shared and to prevent unauthorized access during transmission?

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:**

3.12 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?

3.13 Is this a new or a renewed matching agreement?

☐ New matching agreement
☐ Renewed matching agreement

Please explain your response:

3.14 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:

3.15 How is the information that is covered by this SORN transmitted or disclosed with the external organization(s) under the *MOU* or other "matching agreement?"

3.16 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 ensure 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: Information in the FCC Visitors Database is obtained from individuals who are not FCC employees or contractors.

Please explain any exceptions or clarifications:

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

4.2 If any information collected from non-FCC sources, 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 in the FCC Visitors Database is obtained from individuals who U.S. citizens, U.S. residents (*i.e.*, green card holders), and non-U.S. citizens. As noted in Question 4.1, none of these individuals are FCC employees or contractors.

☒ 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 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 ensure that the information is relevant, accurate, and complete?

4.4. What policies and procedures do the information system's administrators and managers use to ensure 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 ensure that the information that is covered by this SORN adheres to the Data Quality guidelines?

Due to the potential security violations that might occur without proper surveilance, the FCC's SOC takes its security responsibilities seriously:

(1) The SOC staff performs regular, routine records verification on the information (including the PII covered by FCC/OMD-30, "FCC Visitors Database" SORN), which is contained in the FCC Visitor Database to ensure that this information is accurate, current, and meets the Data Quality guidelines.

(2) In addition, and as noted in Question 2.12, the FCC's SOC maintains the information in the FCC Visitors Database in accordance with NARA General Records Schedule (GRS) 18, Item 18, *i.e.*, the information is kept for one year and is then destroyed, unless the information must be retained for specific, on-going security investigations.
(3) Furthermore, the SOC deactivates the Personal Identify Verification (PIV) Card (visitor's ID badge), which is issused to each visitor, within 18 hours of the visitor's separation (*i.e.*, no longer a FCC visitor), loss of card, or expiration. This deactivation protocol is done in accordance with the Homeland Security Presidential Directive (HSPD-12).

Section 5.0 Safety and Security Requirements:

5.1 How are the records/information/data in the information system or database covered by this 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 or database 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 in the FCC Visitor's Database is unique. It is used exclusively to compile limited background and security data on all visitors to determine their suitability to visit the FCC's headquarters and faciliites.

5.3 What would be the consequences to the timely performance of the FCC's operations if this information system became dysfunctional?

As noted in Questions 5.2 and 5.3, the information in the FCC Visitor's Database, including the PII covered by FCC/OMD-30 SORN, is unique and is used specifically for background analysis to determine a visitor's suitability to visit the FCC's headquarters and facilities. However, this database is not considered an essential FCC system whose unavailability would prevent the timely performance of FCC operations.

5.4 What will this information system do with the information it collects:

☐ The system will create new or previously unavailable information through data aggregation, consolidation, and/or analysis, which may included information obtained through link(s), sharing, and/or transferals to/from other information systems or databases;
☒ The system collects PII, but it will not perform any analyses of the PII data.

Please explain your response:

As noted in Question 1.8, the FCC Visitor's Database collects data from individuals who wish to visit the FCC. The SOC makes a determination of the individual's suitability to visit the FCC based on the information that the SOC staff gathers, i.e., whether the individual would pose a security or other risk to the FCC's staff and facilities.

5.5 Will the FCC use the PII that the information system (or database) collects to produce reports on these individuals?

☐ Yes
☒ No

Please explain your response:

As noted in Question 4.5, the FCC Visitors Database is used to collect and store information on a short-term basis, *i.e.*, while the individual's data is being reviewed for clearance to be allowed to visit the FCC's buildings and facilities. The information is only used for this clearance process, thus any reports on an individual. which are related to assessing the individual's suitability as a visitor (and could include the individual's PII) are destroyed after the individual's visit is concluded.

5.6 What will the system's impact(s) be on individuals from whom it collects and uses their PII:

☐ The information will be included in the individual's records;
☒ The information will be used to make a determination about an individual;
☐ The information will be used for other purposes that have few or no impacts on the individuals.

Please explain your response (including the magnitude of any impact(s)):

As noted in Question 5.5, the information in the FCC Visitor's Database, including the PII that is covered by FCC/OMD-30, "FCC Visitors Database," is collected to provide the necessary information that the SOC needs to ensure that visitors to the FCC's headquarters and facilities are eligible to visit, *i.e.*, that these individuals do not pose any security or other risks..

5.7 Do individuals have the right to the following?
(check all that apply)

☒ They may decline to provide their PII?
☒ They may consent to particular uses of their PII?

Please explain your response (including the potential consequences for refusing to provide PII):

Permission to visit the FCC is done on voluntary basis. Therefore, an individual's refusal to provide PII may result in the SOC's refusal to grant this person a visitor's pass to visit the FCC.

If individuals do not have the right to consent to the use of their information, please skip to Question 5.10.

5.8 If individuals have the right to consent to the use of their PII, how does the individual exercise this right?

5.9 What processes are used to notify and to obtain consent from the individuals whose PII is being collected?

As noted in Question 5.5, the information in the FCC Visitor's Database, including the PII that is covered by FCC/OMD-30, "FCC Visitors Database," is collected to provide the necessary information that the SOC needs to ensure that visitors to the FCC's headquarters and facilities are eligible to visit, *i.e.*, that these individuals do not pose any security or other risks.

5.10 How will the information be collected and/or input into this information system (or database):

(choose all the apply)

- ☐ The information system has a link to the FCC's Internet address at www.fcc.gov or other customer-facing URL;
- ☐ The information system has a customer-facing web site via the FCC Intranet for FCC employees and contractors working at the FCC;
- ☒ The information is collected from the individual by fax;
- ☒ The information is collected from the individual by e-mail;
- ☒ The information is collected from the individual by completing a FCC form, license, and/or other document;
- ☒ The information is collected from the individual by regular mail; and/or
- ☐ The information is collected from the individual by other method.

Please explain your response:

Information in the FCC Visitors Database is collected from documentation that potential visitors to the FCC provide to the SOC staff. This information may be cross-checked with data from other Federal and state databases to ensure it is accurate and correct. There is no externally facing portal or web application nor are there any links that would allow access to other FCC internal networks, etc.

5.11 How does this system advise individuals of their privacy rights when they submit their PII?

- ☐ The system contains a link to the FCC's privacy policies for all users at the FCC's website www.fcc.gov:
- ☐ A Privacy Notice is displayed on the webpage:
- ☒ A Privacy Notice is printed at the end of the FCC form(s), license(s), and/or other Commission document(s): The SOC collects information directly from those individuals who wish to visit the FCC's buildings and facilities. The SOC provides a privacy notice to each individual when the individual completes the interview as part of the information collection process to determine his/her suitability as a visitor.
- ☐ The FCC Intranet site displays a Privacy Notice:
- ☐ The collection or input mechanism uses another method to provide individuals with the Privacy Notice: As noted in Question 5.8, information in the FCC Visitors Database is collected directly from individuals who wish to visit the FCC.
- ☐ No Privacy Notice is provided:

5.12 If a Privacy Notice is provided, 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:

5.13 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:

5.14 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:

5.15 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 FCC Visitors Database, including the PII that is covered by FCC/OMD-30, "FCC Visitors Database" SORN, are required to complete the FCC's bureau-wide privacy training. In addition the SOC staff holds an annual privacy awareness review session and provides various notices and warnings to the employees and contractors who have access to the PII that it is not to be shared or disclosed without authorization.

5.16 How often are the security controls reviewed?

- ☐ Six months or less:
- ☒ One year: In addition, the SOC conducts an annual security review for its paper document files. The SOC reviews its computer database records and files in cooperation with ITC.
- ☐ Two years

☒ Three years:
☐ Four years
☐ Five years
☐ Other:

5.17 How often are ITC personnel (*e.g.*, information system administrators, information system/information system developers, contractors, and other ITC staff, *etc*.) who oversee the FCC network operations trained and made aware of their responsibilities for protecting the information?

☐ There is no training
☒ One year: As noted in Question 5.24, the FCC has a Commission-wide privacy training program, which requires all FCC employees and contractors to complete a privacy training course annually, beginning in September 2006.
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☐ Other:

If privacy training is provided, please skip to Question 5.19.

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

5.19 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: ITC does a review at least every three years.
☒ Other re-certification procedures: The SOC management does periodic evaluations of the SOC staff security clearance authorizations.

5.20 How do the Commission's training and security requirements for this information system conform to the requirements of the Federal Information Security Management Act (FISMA)?

As noted in Question 5.28, the SOC management does periodic evaluations of the SOC staff security clearance authorizations.

If the Privacy Threshold Assessment was completed recently as part of the information system's evaluation, please skip Questions 5.30 through 5.33, and proceed to Question 5.34.

5.21 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 FCC Visitors Database does contain PII that may be sensitive. Unauthorized disclosure could create a moderate risk for any privacy issues for those who are affected.

5.22 What is the impact level for the information system(s) covered by this SORN and is it consistent with the guidelines as determined by the FIPS 199 assessment?

As a "non major" information system, the FCC Visitors Database is exempt from the FIPS 199 requirements.

5.23 When was the “Certification and Accreditation” (C&A) completed for the information system(s) covered this SORN—please provide the C&A completion date?

As a "non major" information system, the FCC Visitors Database is exempt from the C&A requirements.

5.24 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: As a "non major" information system, the FCC Visitors Database is exempt from the independent risk assessment, security testing, related requirements..

5.25 Does this information system use technology in ways that the Commission has not done so previously, *i.e.*, Smart Cards, Caller-ID, *etc*?

The FCC Visitors Database is an information system that is hosted on the FCC's computer network--it does not use any new technologies. The only technologies involved are the FCC's computer network databases where this information is collected, stored , and used and the temporary ID badge that each individual, who is approved for (temporary) entry, must wear while visiting the FCC's buildings and facilities.

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

The FCC Visitors Database only affects individuals who are not FCC employees or contractors. Anyone who wishes to visit the FCC's buildings and facilities must submit to a background check, as required by Federal law, and as noted in Question 5.34, each visitor must wear a FCC temporary visitors ID badge.

5.27 Does this information system (covered by this SORN) include a capability to identify, locate, and/or monitor individuals?

The FCC Visitors Database is used solely to collect information that is used to do basic background checks about individuals (who are not FCC employees or contractors) who wish to visit the FCC's buildings and facilities. These visitors are issued temporary FCC ID badges that do include the capability to identify and locate each individual within the FCC buildings and facilities. These badges have the same capabilities and functions as the ID badges that are issued to FCC employees and contractors, and all individuals, including FCC employees, contractors, and temporary visitors must wear the FCC ID badge as required by Federal law.

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):**

5.28 If the information system includes the technical ability to monitor an individual's movements identified in Questions 5.34 through 5.36 above, what kinds of information will be collected as a function of the monitoring of individuals?

The FCC temporary ID badges, which are issued to those who are allowed permission to visit the FCC's buildings and facilities on a short-term or temporary basis, are used to monitor the movement of individuals, including all FCC employees and contractors and visitors. This is part of the security requirements for all Federal agencies as required by Federal law.

5.29 What controls, policies, and procedures, if any, does this information system (covered by this SORN) contain any controls, policies, and procedures to prevent unauthorized monitoring?

As noted in Question 5.37, all people who are admitted to FCC buildings and facilities, including FCC employees, contractors, and visitors are required by Federal law to wear a FCC ID badge. The badge does include a monitoring capability, as also required by Federal law.

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

6.1 Does the information system or database covered by this SORN solicit information via paperwork and/or recordkeeping requirements, which may include any of the following (including both voluntary and required compliance):

☒ FCC forms, licenses, or other documentation that an individual must complete;
☒ Participation in marketing, consumer, or customer satisfaction surveys or questionnaires;
☒ Recordkeeping or related activities.

☒ If so, then this information system is subject to the requirements of the PRA because it solicits information via paperwork and/or recordkeeping requirements.

Which of these groups are affected?

☒ Individuals (public-at-large), who are not FCC employees or contractors.
☐ FCC employees and/or contractors.

☐ No, the information system does not include any paperwork and/or recordkeeping requirements.

If there are no paperwork or recordkeeping requirements, or if only FCC employees and contractors are the effected groups, this information system is exempt from the requirements of the PRA. Please skip to **Section 7.0 Correction and Redress:**

6.2 Is there a website that requests information, such as the information necessary to complete an FCC form, license, authorization, *etc*.?

☐ Yes
☒ No or Not applicable

Please explain your response:

The FCC Visitors Databse requires that anyone who wishes to visit the FCC's buildings on a temporary basis must submit their PII for a routine background check, as required by Federal law.

This requirement is exempt from the PRA under 5 CFR Section 1320.3(h)(1) of the PRA since the burden on an individual to provide their PII is no more than that "necessary to identify the individual."

6.3 If there are one or more PRA information collections that are covered by this 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 Are there are any FCC forms associated with the information system(s) covered by this SORN, and if so, do the forms carry the Privacy Act notice?

☐ Yes:
☐ No
☒ Not applicable—the information collection does not include any forms. As noted in Question 6.2, this information collection is exempt from the PRA regulations.

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:

As noted in Question 6.2, the Office of General Counsel staff were contacted to determine that this collection of information is exempt from the PRA requirements.

Section 7.0 Correction and Redress:

7.1 What are the procedures for individuals wishing to inquire whether this 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?

Individuals wishing to inquire whether FCC/OMD-30, "FCC Visitors Database" SORN, contains information about them may address their inquiries to the SOC system manager in OMD. This is consistent with FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act, as noted in this SORN.

7.2 What are the procedures for individuals to gain access to their own records/information/data in this information system that is covered by this 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?

Individuals who seek access to the information about them that is contained in FCC/OMD-30, "FCC Visitors Database" SORN, may address their inquiries to the SOC system manager in OMD. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, as noted in the SORN.

7.3 What 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 SORN consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

Individuals seeking to correct or to amend information about in FCC/OMD-30, "FCC Visitors Database" SORN, may address their inquiries to the SOC system manager in OMD. This is consistent with FCC policies and rules under 47 CFR §§ 0.556 – 0.558, as noted in the SORN.

7.4 Does the FCC provide any redress to amend or correct information about an individual covered by this 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?

Individuals seeking any redress to amend or correct information about them in FCC/OMD-30, "FCC Visitors Database" SORN, may address their inquiries to the SOC system manager in OMD. This is consistent with FCC policies and rules under 47 CFR §§ 0.556 – 0.558, as noted in the SORN.

7.5 Does this 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?

FCC/OMD-30, "FCC Visitors Database" SORN does not claim any exemption to the notification, access, and correction and/or amendment procedures, as they apply to individuals seeking information about themselves in this SORN.

7.6 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 SORN that is being updated or revised?)

The SOC staff issue periodic reminders to the staff who work with the information in the FCC Visitors Database, including the PII that is covered by FCC/OMD-30 SORN, that it is "non public for internal use only," and that they should keep the information confidential and safeguard any printed materials. A "*PRIVACY WARNING NOTICE*" also appears on the pc monitor screen when records containing information on individuals in the FCC Visitors Database files are first displayed.

7.7 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): The information in the FCC Visitors Database is maintained in accordance with NARA GRS 18, item 22a, *i.e.*, the SOC only maintains the information (including the PII) in the FCC Visitor's Database during the time that an individual is permitted to visit the FCC's buildings and facilities, unless the information is retained for specific, on-going security investigations; such records of facility access are maintained for one year and then destroyed. Once the visitation period has expired, the PII is deleted from the FCC Visitors Database files. The SOC conducts periodic audits of the data [provide audit schedule info].

Section 8.0 Risk Assessment and Mitigation:

8.1 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. Potential foreign visitors, *i.e.*, individuals who are not US citizens or permanent residents (green card holders), could provide false information to obtain entry to FCC buildings and facilities.	a. The SOC conducts a fairly extensive background check, including comparison with information from the Department of Homeland Security and other Federal agencies tasked with law enforcement and national security duties to ensure that those who visit the FCC are thoroughly investigated prior to their visits.
b.	b.

8.2 What is the projected production/implementation date for the information system(s) or database(s):

Initial implementation: June 2012
Secondary implementation:
Tertiary implementation:
Other implementation:

8.3 Are there any ancillary and/or auxiliary information system(s) or database(s) linked to this information system that are covered by this 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:

As noted in Question 1.6 and elsewhere, the FCC Visitors Database resides in the FCC's computer network databases, but it is a stand alone information system with no links to other FCC or non-FCC systems.