Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the Violators Files

July 15, 2009

FCC Bureau/Office: Enforcement Bureau
Division(s): Violators Files Division and FCC field facilities

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

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

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

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

(a) What changes are being made to the information that the system presently collects and maintains; and/or

(b) What new information will be collected and maintained to determine the continuing impact(s) on the privacy of the individuals.

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

Section 1.0 Information System's Contents:

1.1 Status of the Information System:

☐ New information system—Implementation date:
☒ Revised or upgraded information system—Revision or upgrade date: January 2009

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

☒ Placed in existing information system—Implementation Date: January 2009
☐ Placed in new auxiliary/ancillary information system—Date:
☐ Other use(s)—Implementation Date:

Please explain your response:

The Enforcement Bureau (EB) has made several updates to the Violators Files information system that is covered by the system of records notice (SORN) FCC/EB-1, "Violators Files" SORN. The updates are:

(1) Field Actions Case Tracking System (FACTS) for monitoring EB's violator files cases (see Question 2.11);

(2) Powerpoint for consolidated EB actions; and

(3) New routine use, "breach notification," as required by OMB Memorandum M-07-16 (May 22, 2007).

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

☐ Yes
Date:
☒ No

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

The Violators Files information system has a system of records, FCC/EB-1, "Violators Files," that pre-dates the implementation of the Privacy Impact Assessment requirement.

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:

The FCC developed the Violators Files information system when the Enforcement Bureau was created to centralize the FCC's Violators Files policies, activities, and programs in one bureau at the Commission. This information system has never existed under another name, nor has the name been changed since the SORN was published in the *Federal Register* on April 5, 2006.

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

☐ Yes
☒ No

If yes, please explain your response:

The staff in the Enforcement Bureau (EB) has made only minor updates to the operating system, *etc*., for the Violators 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 Violators Files information system is linked to the information system covered by the System of Records known as FCC/CIB-1 "Informal Complaints and Inquiries" in that the Violators Files contain complaints and inquiries referred from the Consumer and Governmental Affairs Bureau to the Enforcement Bureau for handling.

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:

The Violators File information system was created for the Enforcement Bureau.

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

Information about FCC Employees:

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

☐ Digital signature
☐ Other information:

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: FCC license callsign

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: FCC license call sign

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

☒ Personal information from FCC employees: Names and badge numbers
☒ Personal information from FCC contractors: Names and badge numbers
☒ Personal information from non-FCC individuals and/or households: Individuals who are subjects of FCC field enforcement actions.
☒ Non-personal information from businesses and other for-profit entities: Individuals who are subjects of FCC field enforcement actions, whose PII is included as part of the enforcement actions.
☒ Non-personal information from institutions and other non-profit entities: Individuals who are subjects of FCC field enforcement actions, whose PII is included as part of the enforcement actions.
☒ Non-personal information from farms: Individuals who are subjects of FCC field enforcement actions, whose PII is included as part of the enforcement actions.
☒ Non-personal information from Federal Government agencies: Individuals who are subjects of FCC field enforcement actions whose PII is included as part of the enforcement actions.
☒ Non-personal information from state, local, or tribal governments: Individuals who are subjects of FCC field enforcement actions, whose PII is included as part of the enforcement actions.
☐ 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 Violators Files information system, including the personally identifiable information (PII) covered by FCC/EB-1, "Violators Files" SORN, is linked to the Consumer and Government Affairs Bureau's (CGB) Informal Complaints and Inquiries information system in that the Violators Files information system contains complaints and inquiries referred from CGB to the

Enforcement Bureau for handling. The PII in the Informal Complaints and Inquiries information system is covered by FCC/CGB-1 "Informal Complaints and Inquiries" SORN.[2]

There is no electronic link or electronic transmission between the two information systems--only paper copies of documents are transferred between the two information systems. The Informal Complaints and Inquiries

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): FCC/CGB-1 Informal Complaints and Inquiries
- ☐ 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

[2] FCC/CGB-1, "Informal Complaints and Inquiries" SORN was formerly titled as FCC/CIB-1, "Informal Complaints and Inquiries," SORN. The title of this SORN was changed when the Consumer and Information Bureau (CIB) was renamed the Consumer and Governmental Affairs Bureau (CGB).

☐ 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: FCC license callsign

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: FCC license callsign.

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

☒ Yes
☐ No

Please explain your response:

The Violators File data are collected and used in the aggregate to track enforcement cases and sanctions. Information from this sytem will also be used as the basis of published and unpublished sanctons and letters of inquiry.

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

☒ Yes
☒ No

Please explain your response:

Information in the Violators File information system is retrieved by the violator's name or FCC license callsign.

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

☒ Yes
☐ No

Please explain your response:

The published sanctions will include the subject names and, in some cases, home or business address.

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

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

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

☒ Yes
☐ No

If yes, what is this System of Records Notice (SORN): This system of records notice, FCC/EB-1, "Violators File," was published in the *Federal Register* on April 5, 2006.

Please provide the citation that was published in the *Federal Register* for the SORN: 71 FR 17234, 17237.

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 location of the information covered by the system of records notice (SORN)?

☐ Yes
☐ No

Please explain your response:

1.23 What are the categories of individuals covered by the system of records notice (SORN)?

☐ Yes
☐ No

Please explain your response:

1.24 What are 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:

1.25 What is 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:

1.26 What are the purposes for collecting, maintaining, and using the information covered by the system of records notice (SORN)?

☐ Yes
☐ No

Please explain your response:

1.27 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,"[3] 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:

[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.

☐ Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:

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

1.28 Will the information be disclosed to consumer reporting agencies?
☐ Yes
☐ No

Please explain your response:

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

1.30 How is information in this system retrieved?

1.31 hat policies and/or guidelines are in place on how long the bureau/office will retain the information?

1.32 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?

1.33 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**:

1.34 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:

Coordination is now taking place with PERM to finalize a NARA records retention and disposition schedule for this SORN.

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

Section 2.0 System of Records Notice (SORN) Update:

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

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

☐ Yes
☒ No

Please explain your response:

The FCC's Security Operations Center (SOC) has not assigned a security classification to the Violators File information system and to the personally identifiable information (PII) that it collects, uses, and maintains, which is covered by FCC/EB-1, "Violators File" SORN.

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

☐ Yes
☒ No

Please explain your response:

The information, including the personally identifiable information (PII) that is covered by this SORN, is located in:

Primary: Enforcement Bureau (EB), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554; and

Secondary: various field facilities.

Information about FCC Field Offices may also be found in 47 CFR Sections 0.121 and 0.401.

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

☐ Yes
☒ No

Please explain your response:

The categories of individuals that are covered by FCC/EB-1, "Violators Files" SORN, include:

(1) Individuals who have been subjects of Federal Communications Commission (FCC) field enforcement actions, *i.e.*, monitoring, inspection, and/or investigation, *etc*., for violations of radio law, FCC rules and regulations, or international treaties; and

(2) Licensees, applicants, and unlicensed individuals about whom there are questions of compliance with FCC rules under 47 CFR Parts 80, 87, 90, 94, 95, and 97 and/or the Communications Act of 1934, as amended.

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

☐ Yes
☒ No

Please explain your response:

The categories of records, including the personally identifiable information (PII) that is covered by FCC/EB-1, "Violators Files" SORN, include inspection reports, complaints, monitoring reports, investigative cases, referral memos, correspondence, discrepancy notifications, warning notices, and forfeiture actions.

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

☐ Yes
☒ No

Please explain your response:

The legal authorities for maintenance of the personally identifiable information (PII) covered by FCC/EB-1, "Violators Files" SORN, are 47 U.S.C. 101, 102, 104, 301, 303, 309(e), 312, 315, 318, 362, 364, 386, 501, 502, 503, 507, and 510.

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

☐ Yes
☒ No

Please explain your response:

The purposes for collecting maintaining, and using the information in the Violators Files information system, including the personally identifiable information (PII) that is covered by FCC/EB-1, "Violators Files" SORN, include:

(1) Records that are used in connection with the Commission's field enforcement programs:

(a) to determine levels of compliance among radio users;

(b) to issue marine certificates of compliance;

(c) to document Commission monitoring inspections and investigations for enforcement purposes; and

(d) to provide a basis for various administrative, civil, or criminal sanction actions taken against violators by the Enforcement Bureau (EB) or other appropriate Commission bureaus or offices; and

(2) Records that are used for cross-reference purposes:

(a) to prevent the duplication of the FCC's enforcement actions; and

(b) to track the progress of enforcement cases.

2.7 Have there been any changes to the Routine Uses[4] under which disclosures are permitted to "third parties" as noted in the system of records notice (SORN)?

☒ Yes
☐ No

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

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

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

☐ Yes
☒ No

Please explain your response:

Information in the Violators Files information system, including the personally identifiable information covered by FCC/EB-1, "Violators Files" SORN, is not disclosed to any consumer reporting agencies.

[4] 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.

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

☐ Yes
☒ No

Please explain your response:

The information in the Violators Files information system, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, includes both paper documents and electronic data.

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

☐ Yes
☒ No

Please explain your response:

Information in the Violators Files information system, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, is retrieved as follows:

(1) Information in the electronic records that are stored and maintained in the FCC computer network are retrieved by the complainant's name; and

(2) Information in the central files, *e.g.*, paper documents, is retrieved by a unique case number assigned to each case

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

☐ Yes
☒ No

Please explain your response:

Access to information in the paper files covered by the Violators Files information system, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, is restricted to supervisors and employees in the Enforcement Bureau (EB) and to other FCC employees and contractors whose job duties and responsibilities require such access. The new records are aggregate numbers created for tracking and cross-referencing reporting.

The electronic records and data are maintained in the FCC computer network database, which is secured through controlled access and passwords restricted to administrative staff in the Associate Managing Director, Information Technology Center (AMD-ITC). The computer terminals are located in non-public rooms. The rooms are locked outside of business hours. Information that is resident on the network servers is backed-up daily to magnetic media. Back-up tapes are stored on-site and in an off-site storage location.

The Violators File also includes the field offices' database known as the Field Activity Case Tracking System (FACTS):

(1) The FACTS "database" is actually 25 standalone databases, each residing in one of the field's district or resident agent offices.

(2) The databases are on-line or "live" only for employees in the respective field office. Employees in an individual office have read, write, update, and delete access permissions only on the database in their office.

(3) An individual office's database is not accessible by anyone outside the office.

(4) Data from each of the 25 office databases is sent nightly to a single computer on the FCC network.

(5) This combined database provides read-only access for reporting purposes available to any FCC employee behind the FCC firewall connected to the agency computer network.

(6) Actions are currently being taken to restrict access to the FACTS database to only Enforcement Bureau employees working in the field offices or using field data for other enforcement actions, by using log-ins and passwords.

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 Performance Evaluation and Records Management Division of Office of Managing Director (OMD-PERM) has not determined a records retentions schedule for the Violators Files information system data (both the electronic records and the paper documents), including the PII that is covered by FCC/EB-1, "Violators Files" SORN. No records (electronic and/or paper) will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA).

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 locations: All field office locations

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: The EB supervisory staff has responsibility for access and proper use of the information in the Violators 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 paper files is restricted to EB employees working on the cases involved.

The Violators File also includes the field offices' database known as the Field Activity Case Tracking System (FACTS):

(1) The FACTS "database" is actually 25 standalone databases, each residing in one of the field's district or resident agent offices.

(2) The databases are on-line or "live" only for employees in the respective field office. Employees in an individual office have read, write, update, and delete access permissions only on the database in their office.

(3) An individual office's database is not accessible by anyone outside the office.

(4) Data from each of the 25 office databases is sent nightly to a single computer on the FCC network.

(5) This combined database provides read-only access for reporting purposes available to any FCC employee behind the FCC firewall connected to the agency computer network.

(6) Actions are currently being taken to restrict access to the FACTS database to only Enforcement Bureau employees working in the field offices or using field data for other enforcement actions, by using log-ins and passwords.

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 the Enforcement Bureau may be granted access on a "need-to-know" basis as dictated by their job duties and responsibilities for the paper files. For the FACTS database, see answer to Question 3.4 above.
☐ 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: EB supervisory staff.
☒ Information system administrators: FCC employees and contractors who manage the IT systems that hold and process the PII electronic data.
☐ Information system developers:
☒ FCC staff in this bureau/office: See answer to Question 3.4 above.
☒ FCC staff in other bureaus/offices: See answer to Question 3.4 above.
☒ FCC staff in other bureaus/offices in FCC field offices: See answer to Question 3.4 above.
☒ Contractors: See answer to Question 3.4 above.
☐ 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 who handle the PII contained in the Violators Files information system.

3.8 Has the Office of the General Counsel (OGC) signed off on any Section M contract(s) for any contractors who work with the information system covered by this system of records notice (SORN)?

☒ Yes
☐ No

Please explain your response:

The OGC staff has reviewed and signed-off on the Section M contracts for the Violators Files information system, which includes the PII covered by FCC/EB-1, "Violators Files" SORN, as required by Sections 52.224-1 and 52.224-2 of the Federal Acquisition Regulations (FAR).

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

☐ Yes
☒ No

Please explain your response:

As noted in Question 1.10, the Violators Files information system is linked to the information system covered by the Informal Complaints and Inquiries information system, including the PII that is covered by the system of records notice, FCC/CGB-1 "Informal Complaints and

Inquiries," in that the Violators Files contain complaints and inquiries referred from the Consumer and Governmental Affairs Bureau to the Enforcement Bureau for handling.

There is no electronic link or electronic transmission between the two information systems--only paper copies of documents are transferred between the two information systems. The Informal Complaints and Inquiries information system is also covered by a PIA.

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

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

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

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

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

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

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

3.14 Is this a new or a renewed matching agreement?

☐ New matching agreement
☐ Renewed matching agreement

Please explain your response:

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

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

Please explain your response:

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

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

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

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

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

☐ Information is processed and maintained only for the purposes for which it is collected.
☐ Information is reliable for its intended use(s).
☐ Information is accurate.
☐ Information is complete.
☐ Information is current.
☒ Not applicable: The information comes from non-FCC sources.

Please explain any exceptions or clarifications:

The information contained in the Violators Files information system, including the PII covered by FCC/EB-1, "Violators Files" SORN, includes inspection reports, complaints, monitoring reports, investigative cases, *etc*., concerning individuals who are the subjects of FCC enforcement actions.

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: Individuals who are the subjects of FCC field enforcement actions or about whom there are questions of compliance with FCC rules and the Communications Act of 1934.

☒ 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 EB staff reviews inspections reports, complaints, monitoring reports, investigative cases, referral memos, correspondence, discrepancy notifications, warning notices and forfeiture actions. The information contained in these various documents must meet the criteria established by the Data Quality guidelines.

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

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

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

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

As noted above, the EB staff reviews all information contained in these various documents that identify individuals who are the subjects of enforcement actions and/or about whom there are questions of compliance with FCC rules, Communications Act regulations, *etc*.

The information contained in the Violators Files information system does not require an annual verification since it must meet the various legal criteria that govern the actions of the Enforcement Bureau as they pertain to the review and enforcement of violations of the Communications Act and FCC rules and regulations.

Furthermore, the EB webpage provides a link at: http://www.fcc.gov/omd/dataquality to the FCC's Information Quality Guidelines in which the FCC explains that its guidelines substantially follow the OMB Data Quality Guidelines.

Section 5.0 Safety and Security Requirements:

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

☒ IT database management system (DBMS)

☒ Storage media including diskettes, CDs, CD-ROMs, *etc*.
☒ Electronic tape [back up of the FCC computer network is on electronic tape]
☒ Paper files
☐ Other:

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

☐ Yes
☒ No

Please explain your response:

The information that the Violators Files information system collects, uses, and maintains, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, is obtained from the information contained in inspection reports, complaints, monitoring reports, investigative cases, referral memos, correspondence, discrepancy notifications, warning notices and forfeiture actions, etc., which serve as the basis for the Enforcement Bureau's actions. The information is not available from other sources, with the exception that, as noted in Question 3.9, the EB receives information, *e.g*., complaints and inquiries (paper documents), from CGB's Informal Complaints and Inquiries information system.

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 above, the Violators Files information system is linked to the information system covered by the Informal Complaints and Inquiries information system, including the PII that is covered by the system of records notice, FCC/CIB-1 "Informal Complaints and Inquiries," in that the Violators Files contain complaints and inquiries referred from the Consumer and Governmental Affairs Bureau to the Enforcement Bureau for handling.

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:

Complaints and inquiries are received by the Consumer and Governmental Affairs Bureau which forwards the complaints and inquiries to the relevant field office. These complaints and inquiries often contain PII.

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:

See answers to Questions 3.4 and 5.3, above.

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:

See answer to Question 3.4, above.

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

☒ Yes
☐ No

Please explain your response:

The Violators Files information system performs a necessary a function for the Commission. This information system collects, stores, and uses the data that are derived from inspection reports, complaints, monitoring reports, investigative cases, referral memos, correspondence, discrepancy notifications, warning notices, and forfeiture actions, etc. that concern individuals who are subjects of FCC enforcement actions or about whom there are questions of compliance with FCC rules and Communications Act regulations.

Without this information system, it would not be possible for the FCC to determine the levels of compliance among radio users; to issue marine certifications of compliance; to document FCC monitoring of inspections and investigations for enforcement purposes; to provide a basis for various administrative, civil, or criminal sanction actions taken against violators by the FCC's Enforcement Bureau; and to track the status of enforcement cases to prevent duplication, all such actions and activities are part of the Commission's regulatory responsibility under the Communications Act of 1934, as amended, *etc.*.

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:

All information contained in the FACTS database exists behind the FCC intranet firewall. The only records publicly accessible via www.fcc.gov or available at the Commission's Reference Information Center are the published sanctions issued.

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

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

- ☐ Link to the FCC's privacy policies for all users:
- ☐ Privacy notice displayed on the webpage:
- ☐ Privacy notice printed at the end of the form or document:
- ☐ 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—specify the routine use(s) that may be made of the information.
- ☐ Not applicable, as information will not be collected in this way.

Please explain your response:

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

- ☐ Yes
- ☒ No

Please explain your response:

See answer to Question 5.8, above.

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

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

- ☐ Yes
  - ☐ Notice is displayed prominently on this FCC Intranet 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—specify the routine use(s) that may be made of the information.
☐ Not applicable, as information will not be collected in this way.

Please explain your response:

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

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

☒ Privacy notice is on the document, *e.g.*, FCC form, *etc*. FCC Forms 475, 475-B, and 2000.
☐ Privacy notice displayed on the webpage where the document is located:
☐ Statement on the document notifies the recipient that they may read the FCC Privacy Notice at www.fcc.gov.
☒ Website or FCC document uses other method(s) to alert users to the Privacy Act Notice: Letters of Inquiries and sanctions issued that are used to collect data all notify the recipient of the Privacy Act and the recipient's rights thereunder.
☐ Privacy notice is provided via a recorded message or given verbally by the FCC staff handling telephone calls:
☐ No link or notice, please explain why not: I
☐ 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. [shouldn't "conditions" be checked?]
☒ Disclosures—specify the routine use(s) that may be made of the information.
☐ Not applicable, as information will not be collected in any other way.

Please explain your response:

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

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

☐ Yes
☒ No

Please explain your response:

The FCC Website policy states that although the Commission's Website contains some pages that offer educational content to children. It is FCC policy, in compliance with the requirements of the Children's Online Privacy Protection Act (COPPA), not to collect information online about or from children age 13 and under, except when it is needed to identify a submission or to answer a question. Under no circumstances will any of this information be used for another purpose or shared with third parties, nor will personally identifying information be published on the FCC website.

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

☒ Yes
☐ No

Please explain your response:

The Violators Files information system, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, is used solely to enable the Enforcement Bureau to carry out its regulatory responsibilities to monitor compliance with FCC field enforcement actions, *i.e.*, monitoring, inspection, and/or investigations, *etc.*, for violations of radio laws, FCC rules and regulations, and/or international treaties.

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

☐ Yes
☒ No

Please explain your response:

Individuals who have been the subjects of FCC field enforcement actions, *i.e.*, monitoring, inspection, and/or investigation, etc., for violations of radio law, FCC rules and regulations, and/or international treaties; and individuals about whom there are questions of compliance with FCC rules or the Communications Act of 1934, as amended, as it applies to licensees, applicants, and unlicensed persons under parts 80, 87, 90, 94, 95, and 97 of FCC rules must comply with these regulations that may include a requirement that they provide personally identifiable information as part of the Enforcement Bureau's actions stemming for an enforcement action.

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

☐ Yes
☒ No

Please explain your response:

As noted above, individuals who have been the subjects of FCC field enforcement actions are required to comply with FCC rules, which may include the provision of their personally identifiable information as part of the Enforcement Bureau's actions.

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 [I realized in other PIAs, that this question was unclear and revised it]
☒ No

Please explain your response:

The Violators Files information system does not produce any reports on any PII pertaining to the individuals whose PII is part of the information covered by FCC/EB-1, "Violators Files" SORN; rather, this PII is used as follows:

(1) In connection with the Commission's field enforcement programs:

(a) to determine levels of compliance among radio users;

(b) to issue marine certificates of compliance;

(c) to document Commission monitoring inspections and investigations for enforcement purposes; and

(d) to provide a basis for various administrative, civil, or criminal sanction actions taken against violators by the Enforcement Bureau (EB) or other appropriate Commission bureaus or offices; and

(2) For cross-reference purposes:

(a) to prevent the duplication of the FCC's enforcement actions; and

(b) to track the progress of enforcement cases, applicants, licensees, or filers.

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

☒ Account name
☒ Passwords
  ☒ Accounts are locked after a set period of inactivity
  ☒ Passwords have security features to prevent unauthorized disclosure, *e.g.*, “hacking”
  ☒ Accounts are locked after a set number of incorrect attempts
  ☐ One time password token
  ☐ Other security features:
☒ Firewall
☐ Virtual private network (VPN)
☒ Data encryption:
☒ Intrusion detection application (IDS)
☐ Common access cards (CAC)
☐ Smart cards:
☐ Biometrics
☐ Public key infrastructure (PKI)

☒ Locked file cabinets or fireproof safes
☒ Locked rooms, with restricted access when not in use
☐ Locked rooms, without restricted access
☐ Documents physically marked as "sensitive"
☒ Guards
  ☒ Identification badges
  ☒ Key cards
  ☒ Cipher locks
  ☒ Closed circuit TV (CCTV)
☐ Other:

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

All FCC employees and contractors who work with the information that is collected, used, stored and maintained in the Violators Files information system, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, are required to complete privacy training. In addition the EB staff provides various notices and warnings to the employees and contractors who have access that the PII is not to be shared or disclosed without authorization.

5.25 How often are security controls reviewed?

☐ Six months or less:
☒ One year: The EB staff reviews the security controls in the Violators Files information system at least annually.
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☐ Other:

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

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

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

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

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

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

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

☒ Yes
☐ No

Please explain your response:

The Violators 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 Violators Files information system may include PII about individuals who have been subjects of FCC field enforcement actions for violations of radio law, FCC rules and regulations, and/or international treaties; and/or individuals who are subject to FCC questioning concerning their compliance with FCC regulations and Communications Act statutes as they apply to licensees, applicants, and unlicensed individuals. Inadvertent disclosure of this PII could cause various issues for such individuals.

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

☒ Yes
☐ No

Please explain your response:

The Violators 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 Violators Files information system is a non-major information system, and as such, it is exempt from the C&A requirement.

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

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

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

☐ Yes
☒ No

Please explain your response:

The Violators Files information system uses existing FCC computer network databases to track the levels of compliance among radio users, to issue marine compliance certificates, to document FCC monitoring inspections and investigations for enforcement, and to provide the basis for administrative, civil, and/or criminal sanctions that are taken against violators. There are no other uses for information technology.

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

The Violators Files information system includes PII only on those individuals who have been subject to FCC enforcement actions resulting from an FCC investigation of their compliance with FCC rules, federal statutes, and/or international treaties. There is no effect on the privacy of the public-at-large or FCC employees and contractors.

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 Violators Files information system purpose is to track the status of the enforcement case proceedings. As such, the FCC's field enforcement actions include monitoring, inspection, and/or investigation of individuals who may have violated radio law, FCC rules and regulations, and/or international treaties, *etc.*

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 Violators Files information system, including the PII that is covered by FCC/EB-1, "Violators Files" SORN, uses FCC Forms 475, 475-B, and 2000.

☐ 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:

FCC Forms 475, 475B, and 2000 have been approved by the Office of Management and Budget (OMB) as part of the FCC's information collection budget as required by the Paperwork Reduction Act.

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

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

3060-0874, Consumer Complaint Forms, FCC Form 475, FCC Form 475-B, and FCC Form 2000 series.

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 Forms 475 Form 475-B, and Form 2000 series all carry the Privacy Act notice.
☐ 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:

The staffs in the Enforcement Bureaus and the Consumer and Governmental Affairs Bureau have coordinated the PRA requirements for these FCC forms with the PERM staff.

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 under 47 CFR Section 0.561 of FCC rules that this system of records, FCC/EB-1, "Violators Files," is exempt from disclosing its notification procedures for this system of records.

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 under 47 CFR Section 0.561 of FCC rules that this system of records, FCC/EB-1, "Violators Files," is exempt from disclosing its records access procedures for this system of records.

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 under 47 CFR Section 0.561 of FCC rules that this system of records, FCC/EB-1, "Violators Files," is exempt from disclosing its contesting records procedures for this system of records.

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 under 47 CFR Section 0.561 of FCC rules that this system of records, FCC/EB-1, "Violators Files," is exempt from disclosing its records sources for this system of records.

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:

The sources for the categories of records in the FCC/EB-1, “Violators Files” SORN, which covers the PII that is collected, used, and maintained by the Violators Files information system remain unchanged. However, as noted above, under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined under 47 CFR Section 0.561 of FCC rules that this system of records, FCC/EB-1, "Violators Files," is exempt from disclosing its records sources for this system of records.

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, FCC/EB-1, "Violators Files," 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 Sections 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 materials 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 materials compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

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

The EB supervisory staff issues periodic reminders that the information in the Violators Files information system's electronic records and paper files, including the personally identifiable information that is covered by FCC/EB-1, "Violators Files" SORN, is "non public for internal use only" and that they are to keep the information confidential and to safeguard any printed materials.

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

☐ Six months or less
☐ One year
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☒ Other audit scheduling procedure(s): As noted in Question 4.5, the EB staff does frequent reviews of the information contained in the Violators Files information system in accordance with the various legal criteria that govern the actions of the Enforcement Bureau as they pertain to the review and enforcement of violations of the Communications Act and FCC

rules and regulations. The EB believes that such reviews insure that the information in this information system is accurate and up-to-date.

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. Some of the information in the Violators Files information system's PII is contained in electronic records that are stored in the FCC's computer network databases.	a. PII that is contained in electronic records is protected in the FCC's computer network databases, which will require users to provide log-ins, passwords, and other access rights to these records.
b. Some of the information in the Violators Files information system's PII is contained in paper document files that are stored in file cabinets.	b. The file cabinets that store the paper document files are located in non-public areas. The file cabinets are locked at the close of business.

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

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

9.3 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 Enforcement Bureau staff does not anticipate that there will be any new ancillary or auxiliary information systems linked to the Violators Files information system.