Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the Inter-Office and Remote Access Internet E-Mail Systems

July 7, 2009

FCC Bureau/Office: Office of Managing Director (OMD)
Division: Associate Managing Director, Information Technology Center (AMD-ITC)

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: March 2009

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

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

Please explain your response:

The Associate Managing Director, Information Technology Center (AMD-ITC) in the Office of Managing Director is making various minor revisions to the Inter-Office and Remote Access Internet E-mail information system that is covered by the system of records notice (SORN) FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN. ITC has upgraded various parts of this information system and added a 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:

This system of records notice pre-dates the OMB requirements contained in OMB Memorandum M-03-18 (September 22, 2003) that established the Privacy Impact Assessment requirements.

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 information system that is covered by this system of records notice, FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, was originally part of another FCC system of records notice, FCC/Central-8, "Inter-Office and Remote Access Internet E-mail" SORN. In 2006, the Commission renumbered the SORNs maintained by the Office of Managing Director. This SORN is now titled: FCC/OMD-18, "Inter-Office and Remote Access Internet E-mail." It was published in the Federal Register on April 5, 2006, *see* 71 FR 17234, 17265.

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 ITC staff has made only minor updates to the operating system, *etc*., for the Inter-Office and Remote Access Internet E-mail 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 Inter-Office and Remote Access Internet E-mail information system is connected to the Internet, but it functions as a conduit through which users can transmit and receive e-mail, *etc*. The FCC has various security protocols that are designed to ensure that the information that is transmitted and/or received is secured from malicious intrusions, *i.e*., hacking, spam, *etc*.

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

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

☐ Yes
☐ No

Please explain your response:

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

Information about FCC Employees:

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

- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☒ Other information: The information also includes the office e-mail address, passwords, and all inter-office and remote access Internet e-mail that originates from or is received via the computer network accounts of FCC employees, interns, and co-op students.

Information about FCC Contractors:

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

☒ Other information: The information also includes the office e-mail address, passwords, and all inter-office and remote access Internet e-mail that originates from or is received via the computer network accounts of FCC contractors.

Information about FCC 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: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.

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

- ☐ Not applicable
- ☒ Name of business contact/firm representative, customer, and/or others
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Full or partial SSN:
- ☐ Business/corporate purpose(s)
- ☐ Other business/employment/job description(s)
- ☐ Professional affiliations
- ☐ Business/office address
- ☐ Intra-business office address (office or workstation)
- ☐ Business telephone number(s)
- ☐ Business cell phone number(s)
- ☐ Business fax number(s)
- ☐ Business pager number(s)
- ☒ Business e-mail address(es)
- ☐ Bill payee name
- ☐ Bank routing number(s)
- ☐ Income/Assets
- ☐ Web navigation habits
- ☐ Commercially obtained credit history data
- ☐ Commercially obtained buying habits
- ☐ Credit card number(s)
- ☐ Bank account(s)
- ☒ Other information: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.

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

- ☒ Personal information from FCC employees: Computer network accounts of FCC employees, interns, and co-op students.
- ☒ Personal information from FCC contractors: Computer network accounts of contractors working at the FCC.
- ☒ Personal information from non-FCC individuals and/or households: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.
- ☒ Non-personal information from businesses and other for-profit entities: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.
- ☒ Non-personal information from institutions and other non-profit entities: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.
- ☒ Non-personal information from farms: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.
- ☐ Non-personal information from Federal Government agencies:
- ☐ Non-personal information from state, local, or tribal governments:
- ☒ Other sources: Individuals who send or receive e-mails from the FCC's computer users. This e-mail correspondence may include personally identifiable information.

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 Inter-Office and Remote Access Internet E-mail information system is connected to the Internet, but it functions as a conduit through which users can transit and receive e-mail, *etc*. Users may include, at their discretion, personally identifiable information (PII) in their e-mails.

The Inter-office and Remote Access Internet E-mail information system does not support any applications that transmit PII from this information system to any other FCC or non-FCC information systems.

The FCC has various security protocols that are designed to ensure that the information, *e.g.*, e-mail traffic, that is transmitted and/or received is secured from malicious intrusions, *i.e.*, hacking, spam, *etc*.

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

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

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

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

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

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

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

☐ Yes
☐ No

Please explain your response:

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:

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:

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/OMD-20, "Inter-Office and Remote Access Internet E-mail," 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, 17265.

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

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

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

☐ Yes
☐ No

If yes, please explain what has occurred:

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

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

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

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

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

☐ Yes
☐ No

Please explain your response:

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

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

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

☐ Yes
☐ No

Please explain your response:

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

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

Such disclosures, which are referred to as "Routine Uses," [2] are those instances that permit the FCC to disclose information from a SORN to specific "third parties." These disclosures may be for the following reasons:
(check all that are applicable)

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

1.24 Will the information be disclosed to consumer reporting agencies?

- ☐ Yes
- ☐ No

Please explain your response:

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

1.26 How is information in this system retrieved?

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

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

1.28 Once the information is obsolete or out-of-date, what policies and procedures have the system's managers/owners established for the destruction/purging of the data?

1.29 Have the records retention and disposition schedule(s) been issued or approved by the National Archives and Records Administration (NARA)?

☐ Yes
☐ No

Please explain your response:

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

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

☐ Yes
☐ No

Please explain your response:

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

Section 2.0 System of Records Notice (SORN) Update:

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

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

☐ Yes
☒ No

Please explain your response:

The FCC's Security Operations Center (SOC) has not assigned a security classification to the Inter-Office and Remote Access Internet E-mail information center and to the personally identifiable information (PII) that it collects, uses, and maintains, which are covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" 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 FCC/OMD-20, "Inter-office and Remote Access Internet E-mail" SORN, is located in the Information Technology Center (ITC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

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

☐ Yes
☒ No

Please explain your response:

The categories of individuals that are covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, include all other individuals who are assigned a FCC e-mail account, *i.e*, FCC employees, interns, co-op students, and contractors.

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/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, and include the names, e-mail addresses, passwords, and badge numbers of FCC employees and contractors.

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

☐ Yes
☒ No

Please explain your response:

The legal authority for maintenance of the personally identifiable information (PII) covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, is 47 U.S.C. 154(i).

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, including PII, and other records, which are covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, are to insure that all users of the FCC's Inter-office and Internet e-mail information systems abide by the FCC's Intranet and Internet regulations. The information, *i.e.*, electronic records and data, can also be used to identify possible abusers.

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

☒ Yes
☐ No

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 Inter-Office and Remote Access Internet E-mail information system, including the personally identifiable information (PII) covered by FCC/OMD-20, " Inter-Office and Remote Access Internet E-mail Systems" SORN, is not disclosed to any consumer reporting agencies.

[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.

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 this information system, including the personally identifiable information (PII) that is covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, includes electronic data stored in the FCC's computer network databases, DVDs, CD ROMs, electronic tape, and scanned documents, *etc*.

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 Inter-Office and Remote Access Internet E-mail information system's electronic databases is retrieved by searching by organizational unit (bureau/office), the name of the FCC employee (full or part-time), intern, co-op student, and/or contractor, and the employee or contactor's log-in name.

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 Inter-Office and Remote Access Internet E-mail, including the personally identifiable information that is covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, is restricted to FCC employees or contractors whose job duties and responsibilities require such access.

The information (electronic data) in the FCC's computer network databases is secured through controlled access and passwords restricted to administrative staff in the Information Technology Center, Chief Information Officer (CIO) in the Office of Managing Director (OMD). The information that is resident on network servers (electronic data) is backed-up daily to magnetic media. Back-up tapes are stored on-site and at an off-site storage location.

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:

Information Technology Center, Associate Managing Director (AMD-ITC) in the Office of Managing Director (OMD) maintains the information, including the electronic records and data that are covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, in accordance with the General Records Schedule 12 issued by the National Archives and Records Administration (NARA).[4] Records are retained until the FCC employee or contractor leaves the FCC. Electronic records and data disposal is by electronic erasure. Individuals may request a copy of the disposition schedule from the FCC Privacy Officer or directly access to Schedule 12 at: http://www.archives.gov/records-mgmt/ardor/grs12.html.

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

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

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

3.2 Where will the information system be hosted?

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

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

- ☒ FCC staff in this bureau/office exclusively: The ITC staff has responsibility for access and proper use of the information in the Inter-Office and Remote Access Internet E-mail information system.
- ☐ FCC staff in other bureaus/offices:
- ☐ Information system administrator/Information system developers:
- ☐ Contractors:
- ☐ Other information system developers, *etc*:

[4] The FCC is currently under Congressional mandate to retain all e-mails, files, and documents.

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

Access to the data that is stored in the FCC's computer network databases, is restricted to the staff in the Information Technology Center, Chief Information Officer (CIO) in the Office of Managing Director and to FCC employees and contractors working at the FCC 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: FCC employees and contractors in ITC may be granted access on a "need-to-know" basis as dictated by their job duties and responsibilities. In addition, bureaus/offices may determine which employees have access to their data.
☐ 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: ITC supervisors.
☒ Information system administrators: ITC staff, including both FCC employees and contractors, who manage the IT systems that hold and process the PII data.
☐ Information system developers:
☒ FCC staff in this bureau/office: ITC employees are granted access on a "need to know" basis.
☒ FCC staff in other bureaus/offices: Employees in the bureau/offices are granted access on a "need to know" basis.
☒ FCC staff in other bureaus/offices in FCC field offices: Employees in the FCC field offices granted access on a "need to know" basis.
☒ Contractors: Contractors working at the FCC are granted access on a "need to know" basis.
☐ Other Federal agencies:
☐ State and/or local agencies:
☐ Businesses, institutions, and other groups:
☐ International agencies:
☐ Individuals/general public:
☐ Other groups:

3.7 If contractors are part of the staff in the FCC who collect, maintain, and access the information, does the IT supervisory staff ensure that contractors adhere fully to the Privacy Act provisions, as required under subsection (m) of the Privacy Act, as amended, 5 U.S.C. 552a(m)?

☒ Yes
☐ No

Please explain your response:

The supervisory staff in the Information Technology Center, Associate Managing Director (AMD-ITC) provides periodic privacy training to the IT contractors.

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

☒ Yes
☐ No

Please explain your response:

All contracts covering the ITC contractors who work with the Inter-Office and Remote Access Internet E-mail information system include the FAR clauses.

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

☐ Yes
☒ No

Please explain your response:

The Inter-Office and Remote Access Internet E-mail information system, including the personally identifiable information (PII) covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, is a "stand alone" information system. It has no links to any other FCC or non-FCC information systems.

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

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

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

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

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

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

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

3.14 Is this a new or a renewed matching agreement?

☐ New matching agreement
☐ Renewed matching agreement

Please explain your response:

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

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

Please explain your response:

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

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

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

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

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

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

Please explain any exceptions or clarifications:

The information contained in the Inter-Office and Remote Access Internet E-mail information system, including the personally identifiable information (PII) covered by FCC/OMD-20, "Inter-

Office and Remote Access Internet E-mail Systems" SORN, is collected via the FCC's Intranet and Internet networks whenever an individual sends or receives e-mail messages or uses the Internet. The FCC's e-mail system functions as a basic conduit to transfer information from point to point. Thus, there are no data quality issues because all users of the FCC's Intranet and Internet must abide by FCC's Intranet and Internet regulations by signing FCC Forms A-201, "Power User Account Certification Form," FCC Form A-203, "Computer System Separation Clearance Form," and FCC Form A-204, "Modem Use Certification Form," before they are granted access.

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: FCC computer users, *e.g.*, FCC employees, interns, co-op students, and contractors, *etc*., send and receive e-mails from individuals, businesses, *etc*., from outside the FCC.
- ☐ 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:

FCC computer users, *e.g.*, FCC employees, interns, co-op students, and contractors, *etc*., send and receive e-mails from individuals, businesses, *etc*., from outside the FCC through the e-mail system with functions as a "conduit" to transfer information from point to point, and the information that is transferred is not checked specifically for accuracy and adherence to 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?

The ITC staff does continual observation, review, and notification for users of the FCC's computer protocols to insure that the Commission's networks function properly. The Data Quality guidelines do not pertain to this administrative oversight.

Section 5.0 Safety and Security Requirements:

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

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

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

☐ Yes
☒ No

Please explain your response:

All information that the Inter-Office and Remote Access Internet E-mail information system collects, uses, and maintains is obtained from the e-mail data that are derived from the FCC's network Intranet and Internet e-mail traffic that is generated by FCC employees and contractors using the 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:

The Inter-Office and Remote Access Internet E-mail information system, including the personally identifiable information (PII) covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, functions as a "service" or "conduit" information system. a "stand alone" information system--it has no direct electronic links to either other FCC or non-FCC information systems.

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

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

☐ Yes
☐ No

Please explain your response:

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

☐ Yes
☐ No

Please explain your response:

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

☐ Not applicable.

Please explain your response:

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

☒ Yes
☐ No

Please explain your response:

The Inter-Office and Remote Access Internet E-mail information system necessary for the continued and efficient operation of the FCC in order to perform its functions. This information system collects the e-mail data in the FCC's Internet and Intranet network traffic, which is generated by FCC employees and contractors. The ITC staff collects this information to insure that the FCC's Intranet and Internet are being used appropriately, as required in FCC regulations. This recordkeeping function is necessary for the FCC to meet its statutory and regulatory duties to insure that government property is used only for allowed purposes.

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

☒ Yes
☐ No

Please explain your response:

The electronic records that comprise the FCC's Intranet and Internet e-mail traffic are generated via the personal computers that FCC employees and contactors use. The FCC does not maintain confidential, other than business confidential, material on this system. .

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

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

☒ Link to the FCC's privacy policies for all users: This warning: " ***Non Public, For Internal Use Only*** is included in all e-mails sent by FCC computer 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:

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

5.12 If the information system has a customer-facing web site via the FCC Intranet for FCC employees and contractors working at the FCC, does this web site(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*. All FCC computer users must sign and comply with the requirements stated therein: FCC Form A-200, "FCC Computer System Application Access Assignment Form," FCC Form A-201, "FCC Computer System User Rules of Behavior," FCC Form A-201, "Power User Account Certification Form," FCC Form A-203, “Computer System Separation Clearance Form,” and FCC Form A-204, "Modem Use Certification Form." These forms include a "privacy statement."
☐ 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:

☐ Privacy notice is provided via a recorded message or given verbally by the FCC staff handling telephone calls:
☐ No link or notice, please explain why not:
☐ Not applicable, as personally identifiable information (PII) will not be collected.

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

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

Please explain your response:

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

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

☐ Yes
☐ No

Please explain your response:

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

☐ Yes
☒ No

Please explain your response:

The FCC's Inter-Office and Remote Access Internet E-mail information system, which includes the PII that is covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, is used solely to keep track of the FCC's Intranet and Internet e-mail traffic that is generated by FCC employees and contractors using the personal computers assigned to them.

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

☐ Yes
☒ No

Please explain your response:

FCC employees, interns, co-op students, and visitors, *etc*., and contractors working at the FCC who use the FCC's Intranet and Internet networks must sign forms stating that they will abide by FCC regulations when they log-on to the FCC network and when they send and receive e-mail. The requested information is the minimal necessary for the proper functioning of this information system. These requirements are necessary to insure that users do not abuse the FCC's Intranet and Internet networks.

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

☐ Yes
☒ No

Please explain your response:

Individuals do not have the right to consent to particular uses of their personally identifiable information (PII) because the FCC requires this information to insure that FCC employees and contractors abide by the regulations governing use of the FCC's Intranet and Internet networks. The purpose of the information that is collected, stores, and used in the Inter-Office and Remote Access Internet E-mail information system is to insure that these networks function properly. This information system is authorized under the FCC's statuory and regulatory authority to protect the use of the FCC's computer network and cellular) and to regulate the uses and charges related to the use of FCC telephones (wireline and cellular). The FCC can only comply with these responsibilities if this information system has the requisite PII of those who are using FCC telephones, receiving telephone charges, etc. for wireline and cellular telephones.

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

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

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

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

☐ Yes
☒ No

Please explain your response:

This information system does not does not produce reports.

This information system is used to insure that all users of the FCC's Inter-office and Internet e-mail information systems abide by the FCC's Intranet and Internet regulations. The information, *i.e.*, electronic records and data, can also be used to identify possible abusers.

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 Inter-Office and Remote Access Internet E-mail information system are required to complete privacy training. In addition, the ITC staff provides various notices and warnings as part of the "e-protocols" 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: The ITC staff reviews the "e-protocol" security controls in the Inter-Office and Remote Access Internet E-mail information system at least annually.
☐ One year:
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☐ Other:

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

☐ There is no training
☐ One year:
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☒ Other: In September 2006, the FCC has inaugerated a Commission-wide privacy training program that has required all FCC employees and contractors to complete a privacy training course when they are first hired. FCC employees and contractors must take an annual refresher course thereafter.

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 ITC staff requires that the personnel who use the information system, including FCC employees and contractors working at the FCC, must be trained at least

annually on their responsibilities for protecting the PII contained in the Inter-Office and Remote Access Internet E-mail 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 Inter-office and Remote Access Internet E-mail 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 Inter-Office and Remote Access Internet E-mail information system collects only minimal personally identifiable information (PII), *e.g.*, the individual's name, from FCC employees and contractors when they sign FCC Form A-201, "Power User Account Certification Form," and FCC Form A-203, "FCC Computer System Separation Clearance Form," and FCC Form A-204, Modem Use Certification Form, which gives the individual permissions to use the FCC Intranet to send and receive e-mails and to access the Internet. Inadvertent disclosure of this information would pose only a minimal harm to an individual.

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 Inter-office and Remote Access Internet E-mail information system is a non-major information system, and as such, it is exempt from the requirements of the FIPS 199 assessment.

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 Inter-office and Remote Access Internet E-mail information system is a non-major information system, and as such, it is exempt from the Certification and Accreditation (C&A) requirement. However, the FCC does the C&A because it is a "best practice" metric.

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.*: The ITC staff conducts an "in house" risk assessment because this is a "best practice" metric.
☐ Not applicable:

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

☐ Yes
☒ No

Please explain your response:

The ITC staff is making only minor, non-substantive changes to FCC/OMD-20, “Inter-Office and Remote Access Internet E-mail Systems” SORN, which covers the PII that is collected, used, and maintained by the Inter-Office and Remote Access Internet E-mail information system. These changes do not include any new technologies or modifications to existing information technology that the Commission has not used previously.

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

FCC employees, interns and co-op students and contractors working at the FCC are required to provide certain minimal personally identifiable information (PII), *i.e.*, user's name, *etc.*, that allows the Commission to regulate the use of the FCC's computer network, including the transmission and receipt of e-mail and access to Internet sites. FCC needs this information to monitor usage to insure that users, *e.g.*, FCC employees and contractors, abide by the regulations governing use of the FCC's Intranet and Internet networks, and that the Inter-Office and Remote Access Internet E-mail information system functions properly. .

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 Inter-Office and Remote Access Internet E-mail information system is used to insure that all users of the FCC's Inter-office and Internet e-mail information systems abide by the FCC's Intranet and Internet regulations. The information, *i.e.*, electronic records and data, can also be used to identify possible abusers. This information system includes the capability to identify individuals who are using the e-mail and Internet what computer terminal by tracking the transmission, receipt, and termination of e-mail.

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:

☐ 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:

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

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

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

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

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

☐ Yes
☐ No

Please explain your response:

Section 7.0 Correction and Redress:

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

☒ Yes
☐ No

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

Individuals wishing to inquire whether the Inter-Office and Remote Access Internet E-mail information system, which is covered by the FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, contains information about them may address their inquiries to the Chief Information Officer (CIO). This is consistent with FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act, as noted in this SORN.

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

☒ Yes
☐ No

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

Individuals who seek access to the information about them that is contained in the Inter-Office and Remote Access Internet E-mail information system, and which is covered by FCC/OMD-20,

"Inter-Office and Remote Access Internet E-mail Systems" SORN, may address their inquiries to the Chief Information Officer (CIO). This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, as noted in the SORN.

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

☒ Yes
☐ No

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

Individuals seeking to correct or to amend information about them in the Inter-Office and Remote Access Internet E-mail information system, which is covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, may address their inquiries to the Chief Information Officer (CIO). 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 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:

Individuals seeking any redress to amend or correct information about them in the Inter-Office and Remote Access Internet E-mail information system, which is covered by FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, may address their inquiries to the Chief Information Officer (CIO). This is consistent with FCC policies and rules under 47 CFR §§ 0.556 – 0.558, as noted in the SORN.

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

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

☐ Yes
☒ No

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

The sources for the categories of records in the FCC/OMD-20, "Inter-Office and Remote Access Internet E-mail Systems" SORN, which covers the PII that is collected, used, and maintained by the Inter-Office and Remote Access Internet E-mail information system remain unchanged. These record sources include access by FCC employees and contractors to the FCC's Inter-office and Internet E-mail systems.

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

☐ Yes
☒ No

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

FCC/OMD-20, “Inter-Office and Remote Access Internet E-mail Systems” 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.

7.7 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 ITC supervisors issue periodic warnings to their employees and contractors that the information in the Inter-Office and Remote Access Internet E-mail information system's electronic records and data, including the PII that is covered by FCC/OMD-20, “Inter-Office and Remote Access Internet E-mail Systems” SORN, is "non public for internal use only." The ITC supervisors also notify those granted access to the information that they are to keep the information confidential and to avoid unauthorized disclosures.

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 ITC staff does continual observation, review, and notification for users of the FCC's computer protocols to insure that the Commission's Inter-office and remote access internet networks function properly.

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. The information system's personally identifiable information (PII) includes 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 require users to provide login's and access rights to these records. In addition, users can only access their own information.

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

Initial implementation: April 2006
Secondary implementation: March 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 staff in the Information Technology Center of the Associate Managing Director (AMD-ITC) does not anticipate that there will be any new ancillary or auxiliary information systems linked to the Inter-Office and Remote Access Internet E-mail information system.