Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the Core Financial System Replacement (CFSR)

August 21, 2008

FCC Bureau/Office: Office of the Managing Director
Division: Financial Operations (OMD-FO)

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 Assessment** 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—Implemention date: October 2010
☐ Revised or upgraded information system—Revision or upgrade date:

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

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

Please explain your response:

1.2 Has a Privacy Threshold Assessment been done?

☒ Yes
Date: August 2008
☐ No

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

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

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

☐ Yes
☐ No

If yes, please explain your response:

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:

If there have been no such changes, please skip to Question 1.7.

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:

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
  - ☐ Finger prints
  - ☐ Voice prints
  - ☐ 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
  - ☐ Finger prints
  - ☐ Voice prints
  - ☐ 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)
- ☐ Personal e-mail address(es)
- ☐ Non-FCC personal employment records
- ☐ Military records
- ☐ Financial history
- ☐ Foreign countries visited
- ☐ Law enforcement data
- ☐ Background investigation history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☐ Other information:

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

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

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

- ☐ Personal information from FCC employees:
- ☐ Personal information from FCC contractors:
- ☐ Personal information from non-FCC individuals and/or households:
- ☐ Non-personal information from businesses and other for-profit entities:
- ☐ Non-personal information from institutions and other non-profit entities:
- ☐ Non-personal information from farms:
- ☐ Non-personal information from Federal Government agencies:
- ☐ Non-personal information from state, local, or tribal governments:
- ☐ Other sources:

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

- ☐ Yes
- ☐ No

Please explain your response:

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
  - ☐ Finger prints
  - ☐ Voice prints
  - ☐ Retina scan/prints
  - ☐ Photographs
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
- ☐ Birth date/Age
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information:

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

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

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

1.12 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):

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

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:

The CFSR will be a new information system.

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?

A new SORN needs to be created based on developing a new financial system and new business processes for payment activities.

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

The location of the CFSR information system that will be covered by this SORN will be determined when the award of the contract takes place, and who will host the CFSR information system. OMD-FO is also responsible for the uses of this PII in the information system's development, processes, and activities.

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:

The new SORN will cover personally identifiable information (PII) that is used to process payments, reimbursement, debts owed, and other, miscellaneous debts, *etc*., owed or payable to the FCC.

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:

This information system is still in the development stage and has not been assigned a security classification by the FCC Security Officer. Once the information system is functional and ready to be used, *e.g.*, "goes live," the information system will be assigned a security classification.

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

31 U.S.C. 3302(e); 44 U.S.C. 3101, 3102, and 3309; Debt Collection Act as amended by the Debt Collection Improvement Act of 1996; Federal Financial Management Improvement Act of 1996; Chief Financial Officers Act of 1990; and Federal Managers Financial Integrity Act of 1982

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

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

☐ Adjudication and litigation:
☐ Committee communications:
☐ 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 Routine Use disclosures not listed above: Financial Systems Operations Group (FSOG) in OMD-FO has not yet determined what other "routine uses" will be appropriate for this new CFSR information system.

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?

At this point, because the CFSR is still in the planning stages, the FSOG staff in OMD-FO has not yet determined what this information systems's maintenance and security storage requirements will be, although such policies will be in accordance with contractual and vendor policy and contract agreement(s).

1.26 How is information in this system retrieved?

At this point, because the CFSR is still in the planning stages, the FSOG staff in OMD-FO has not yet determined exactly how the CFSR's information retrieval mechanisms will operate, although the personally identifiable information in this new information system can be retrieved via on-line access but will with sufficient various security and privacy measures to protect the PII.

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

The FCC's Office of the Managing Director-Performance Evaluation and Records Management (OMD-PERM) has not yet assigned a records retention schedule for the new CFSR information system that is covered by FCC/OMD-29, "Core Financial System Replacement (CFSR)" SORN. Upon development, the Records Officer in OMD-PERM will assign a records retention schedule for the SORN that covers the personally identifiable information. This records retention schedule will be consistent with the guidelines established by the National Archives and Records Administration (NARA).

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?

Once the Records Officer in OMD-PERM has assigned a records retention and disposal schedule, consistent with NARA guidelines, for the PII that is stored and maintained by this new SORN, the FSOG staff in OMD-FO will follow this schedule in determining the correct policies and procedures for disposing of obsolete or out-of-date information contained in this information system.

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:

As noted above, once the new CFSR information system has been fully developed and is operational, the Records Management Officer in OMD-PERM will review the information system and assign an appropriate records retention and disposal schedule consistent with NARA guidelines.

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:

OMD-FO is coordinating the records retention and disposal schedule with OMD-PERM's Records Management Officer.

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:

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:

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:

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:

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:

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:

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

☐ Yes
☐ No

If the Routine Uses have changed, what changes were made:
(check all that apply and explain the changes)

☐ Not applicable—there have been no changes to the Routine Uses
☐ Adjudication and litigation:
☐ Breach of Federal data:
☐ Committee communications:
☐ 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:
☐ 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:

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:

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:

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:

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:

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: At this point, because the CFRS information system is still in the planning and development stages, FSOG staff in OMD-FO has not yet determined where CFSR will be hosted..

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 FSOG staff in OMD-FO will have responsibility for access and proper use of the information in the CFSR 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)?

The CFSR information system is still in the planning and development stages. The FCC's Financial Systems Operations Group (FSOG) in OMD-FO has not finalized the specific FCC policies and procedures for who will be granted access to the information, other than a general policy that only staff who have a "need to know" as part of their job duties and responsibilities will have access.

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 Financial Systems Operations Group (FSOG) of the Office of the Managing Director (OMD-FO) may be granted access on a "need-to-know" basis as part of their job duties and responsibilities.
- ☐ Other access policy:

3.6 Based on the Commission policies and procedures, which user group(s) may have access to the information at the FCC:
(Check all that apply and provide a brief explanation)

- ☒ Information system managers: FCC employees in the FCC's Information Technology Divisions of the Office of the Managing Director (OMD-IT).
- ☒ Information system administrators: FSOG staff in the Finanical Operations Division of the Office of the Managing Director (OMD-FO), including both FCC employees and contractors, who manage the finanical and IT systems that hold and process the PII data.
- ☐ Information system developers:
- ☒ FCC staff in this bureau/office: FCC employees in the Financial Systems Operations Group (FSOG) of OMD-FO are granted access based on a "need to know" basis.
- ☐ FCC staff in other bureaus/offices:
- ☒ FCC staff in other bureaus/offices in FCC field offices: FCC employees are granted access based on a "need to know" basis.
- ☒ Contractors: Contractors working at the FCC are granted access based on a "need to know" basis.
- ☐ Other Federal agencies:
- ☐ State and/or local agencies:
- ☐ Businesses, institutions, and other groups:
- ☐ International agencies:
- ☐ Individuals/general public:
- ☐ Other groups:

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

- ☒ Yes
- ☐ No

Please explain your response:

The FCC's Information Technology (IT) supervisory staff provide periodic privacy training to the IT contractors.

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:

At this time in the development of the CFSR information system, OMD-FO has not yet selected any specific contracting firm(s) to work on this information system's administrative operations.

3.9 Does the information system covered by this system of records noticed (SORN) transmit/share personal information, *e.g.*, personally identifiable information (PII), between the FCC information technology (IT) 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 Financial Systems Operations Group (FSOG) staff in OMD-FO has determined that when fully developed and operational the CFSR information system may transmit PII data to other Federal agencies, *i.e.*, U.S. Department of the Treasury, and U.S. Department of Agriculture's National Finance Center (NFC), *etc*., as directed by Congressional actions, statutory requirements, and interagency agreements.

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?

Financial data are shared with the U.S. Treasury and U.S. Department of Agriculture as part of various Federal financial agreements and interagency agreements, *i.e.*, Congressionally mandated requirements and statutes.

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.*?

U.S. Department of Treasury, U.S. Department of Agriculture, NFC, Inter-Agency Security Agreement (ISA) will all have security measures in place to insure that the information, including PII) data remain secure during all data transmissions.

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: U.S. Treasury Department, *e.g.*, Internal Revenue Service, and U.S. Department of Agriculture's National Finance Center (NFC).
☐ State, local, or other government agencies:
☒ Businesses:
☒ Institutions: Banks with which the FCC has cooperative agreements.
☐ 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 Financial Services Operations Group staff in OMD-FO are designing the CFSR information system to ensure that the personally identifiable information (PII) on individuals (and all other entities such as businesses and institutions who make debt payments and conduct other financial transactions with the FCC) is reliable, accurate, complete, and current. Inaccurate and/or out-of-date information would be detrimental to the design, operations, and purposes for which the FCC is designing the CFSR financial system.

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: [we need to discuss this—you've said in several questions that business, etc. will use CFSR for financial transactions with 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:

At this time, because the CFSR information system is still in the planning and development stages, the FSOG staff in OMD-FO has not determined the specific policies and procedures that OMD-FO will use to insure that the information that is submitted in CFSR adheres 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?

Based on initial policy planning and development, OMD-FO intends to design the CFSR information system's functions to include data aggregation and will have agreements in place that permit this.

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?

As noted above, although the CFSR information system is still in the planning and development, OMD-FO will have various policies and procedures in place, consistent with FCC regulations to insure that the information that the CFSR collects, uses, maintains, and stores, *etc.*, adhere to the Data Quality guidelines.

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?

Athough the CFSR information system is still in its initial development, it is the intention of the FSOG staff in OMD-FO to conduct periodic reviews of the information that CFSR collects, uses, maintains, and stores, *etc.*, to ensure that the personally identifiable information (PII) on individuals, as well as the sensitive and/or confidential (non-PII) financial data from individuals

and other entities, including businesses and institutions, *etc*., who are assessed fees and other financial payments are reliable, accurate, complete, and current.

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
☒ 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:

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:

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 FCC's FSOG staff in OMD-FO will use the information in the new CFSR information system to track the fee assessments and other payments, *e.g.*, charges for FCC authorization certification, and licensing, *etc.*, that the FCC levies on individuals (and other entities, *e.g.*, businesses and institutions) to cover the costs of the FCC's regulatory activities and other administrative functions, which are mandated by Congress.

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:

If the information is collected by some method or mechanism other than is 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 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: The CFSR information system will have a link to the Carlson Wagonlit's E2 Solutions and Fee Filer systems, but neither of these two systems are directly linked to the CFSR information system..

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:

The CFSR information system will have a link to the Carlson Wagonlit's E2 Solutions and Fee Filer systems, but neither of these two systems are directly linked to the CFSR information system..

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:

The CFSR information system will have a link to the Carlson Wagonlit's E2 Solutions and Fee Filer systems, however, neither of these two systems are directly linked to the CFSR information system..

If the information is collected by some method or mechanism other than via 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: Carlson Wagonlit's E2 Solutions.
  ☒ Privacy Notice is printed at the end of the form or document: FCC Form A-220.
  ☐ Website uses another method to alert users to the Privacy Act Notice:
☒ No

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

we need to discuss this information procesing set up again.

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 mechansim other than via a customer-facing portal on the FCC Internet at www.fcc.gov or the FCC Intranet for FCC employees and contractors, please skip to Question 5.16.

5.14 If information is collected from the individual by fax, e-mail, FCC form(s), or regular mail, how is the privacy notice provided?

☒ Privacy notice is on the document, *e.g.*, FCC form, *etc*. FCC Form A-220.
☐ 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:

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 FCC's CORES registration process issues a FCC Registration Number (FRN) that contains and determines newly or revised information for each registrant, including individuals and all other entities, *i.e.*, businesses, institutions, *etc.*, which the registrant is then required to use in all subsequent dealings with the FCC.

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

☐ Yes
☒ No

Please explain your response:

Individuals may not decline to provide personally identifiable information (PII), which the FCC collects from them for use in the CFSR information system, including information in both paper files and the electronic data formats. Individuals who are assessed fees and other payments for authorizations, certifications, and licensing to use or operate in the radio telecommunications spectrum must adhere to FCC requirements that they provide their personally identifiable information in order to obtain these rights and privileges. These requirements are mandated by Congress and the telecommunications statutes.

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 solicitation of personal information, *e.g.*, PII including a Social Security Number (SSN) or Taxpayer Identification Number (TIN), that is requested as part of the FCC's CORES registeration process, and which is a component of the FCC's financial transaction systems, including CFSR, is authorized by the Communications Act, Sections 8 and 9 and the Debt Collection Act Improvement Act of 1996, P.L. 104-134.

If individuals do <u>not</u> have the right to consent to the use of their information, please skip to Question 5.23.

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 What kinds of report(s) can the information system and/or the information be used to produce on the individuals whose PII data are in the information system covered by the system of records notice (SORN)?

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 will work with the information that is stored and managed by this new information system will be required to complete privacy training. In addition the Financial Services Operations Group staff in OMD-FO will emphasize to those FCC employees and contractors who will have access that the PII in this new financial system that the information is not to be shared or disclosed.

5.25 How often are security controls reviewed?

- ☒ Six months or less: At this stage in its development, the FSOG staff in OMD-FO plans to require the security controls to be reviewed at least every six months for CFSR information system.
- ☐ 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: At this stage in its development, the FSOG staff in OMD-FO plans to require the that those personnel who use the information system to be trained once a year on their responsibilities for protecting the PII contained in the CFSR information system.
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other: The FCC has also inaugerated a Commission-wide privacy training program, and all employees and contractors were required to complete the privacy training course in September 2006.

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: At this stage in its development, the FSOG staff in OMD-FO plans to require the that those personnel who use the information system to be trained at least twice a year on their responsibilities for protecting the PII contained in CFSR.
- ☐ One year:
- ☐ 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:

At this stage in its development, the OMD-FO staff plans to require that the CFSR's development conform to the FISMA requirements that govern the FCC's training and security requirements.

If the Privacy Threshold Assessment 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:

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:

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:

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:

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:

As presently envisioned, the OMD-FO does not intend for the new CFSR information system to use technologies in ways that the Commission has not done so previously.

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

Individuals are required to provide their personally identifiable information (PII) when they register in the FCC's CORES registration system as part of the filing and payment processes. This PII is contained in the CORES electronic database's records, and a unique identification number, the FCC Registration Number or FRN, is assigned to each individual or vendor, *e.g.*, business, contractor, institution, *etc*.. The FCC believes that this technology has created a process that minimizes the disclosure of PII, *i.e.*, SSNs, TINs, etc., and reduces the potential for inadvertent disclosure of such PII.

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 CFSR information system will be used exclusively as part of the FCC's financial systems. The personally identifiable information (PII) that is covered by FCC/OMD-29, "Core Financial System Replace (CFSR)," SORN will be limited to the PII that individuals are required to provide to the FCC as part of the CORES registration process that is used to pay application and regulatory fees and to conduct other financial transactions.

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:

At this time, the FSOG staff in OMD-FO has not determined whether or not the new CFSR information system will include any FCC forms.

☐ 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 yes, what PRA information collections covered by this system of records notice (SORN) are associated with this database please list the OMB Control Number, Title of the collection, Form number(s) as applicable, and Expiration date:

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

☐ Yes

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

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

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

☐ Yes
☒ No

Please explain your response:

Section 7.0 Correction and Redress:

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

☒ Yes
☐ No

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

Upon development and implementation of the new CFSR information system, individuals, including those who submit their personally identifiable information (PII) to the FCC when they register in CFSR to pay their regulatory fees and other financial payments, and who wish to inquire whether this SORN contains their PII may address their inquiries to the system manager or the Deputy Division Chief of the Financial Systems Operations Group (FSOG) in OMD-FO for FCC/OMD-29, "Core Financial System Replacement (CFSR)," SORN. 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:

Upon development and implementation of the new CFSR information system, participation in the CFSR information system's activities and processes will be voluntary, and individuals who provide PII that is covered by the FCC/OMD-29, "Core Financial System Replacement (CFSR)," SORN may seek access to the information about them by contacting the system manager or the Deputy Division Chief of the Financial Systems Operations Group (FSOG) in OMD-FO. 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:

Upon development and implementation of the new CFSR information system, individuals who seek to correct or to amend information about them in the FCC/OMD-29, "Core Financial System Replacement (CFSR)," SORN may contact the system manager or the Deputy Division Chief of the Financial Systems Operations Group (FSOG) in OMD-FO. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, 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:

Upon development and implementation of the new CFSR information system, individuals seeking any redress to amend or correct information about them in the FCC/OMD-29, "Core Financial System Replacement (CFSR)," SORN may contact the system manager or the Deputy Division Chief in the Financial Systems Operations Group (FSOG) in OMD-FO. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, 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:

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:

At this time, the Financial Systems Operations Group (FSOG) in OMD-FO, which is responsible for the development and implementation of the new CFSR information system and the new FCC/OMD-29, “Core Financial System Replacement (CFSR),” SORN that will cover the personally identifiable information that individuals provide when the register in CFSR, does not plan to seek any exemptions to the notification, access, and correction and/or amendment procedures as they apply to individuals seeking information about them 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?

Once the new CFSR information system has been fully developed and implemented, the Financial Systems Operations Group (FSOG) staff in OMD-FO will post notices that the information in information systems's electronic records and paper files that are covered by FCC/OMD-29, “Core Financial System Replacement (CFSR),” SORN are "non public for internal use only." The FSOG staff will also issue reminders periodically to those granted access to the information that they are to keep the information confidential and to safeguard any printed materials.

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

- ☐ Six months or less
- ☐ One year
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other audit scheduling procedure(s): The new CFSR information system does not have an audit requirement at this time since it is still in the planning and development stages. Nonetheless, the FSOG staff in OMD-FO will determine upon completion of the development and implemention of CFSR ("go live") what practices and procedures OMD-FO should adopt to ensure compliance with FCC and OMB audit regulations and other new needs as necessary to safeguard the personally identifiable information (PII) contained in this information system covered by FCC/OMD-29, “Core Financial System Replacement (CFSR),” SORN.

Section 8.0 Consumer Satisfaction:

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

- ☐ Yes
- ☐ No
- ☒ Not applicable

Please explain your response:

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

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

☐ Yes
☐ No

Please explain your response:

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 system's personally identifiable information (PII) includes paper documents that are stored in file cabinets.	a. PII that is contained in paper documents is stored in locked file cabinets, which are located in rooms that are locked when not in use.
b. Some of the information system's personally identifiable information (PII) includes electronic records that are stored in the FCC's computer network databases.	b. 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.
c. Since CFSR is a new information system, there may be potential processes and procedures that could lead to PII security breaches that have not been discovered and remedied.	c. The FSOG staff in OMD-FO is working with the CFSR information system developers to review all the CFSR's processes and procedures with reference to the issue of PII protection and security to avoid any such breaches once the CFSR information system is fully developed and operational.

9.2 What deficiencies did the bureau/office find in its procedures for evaluating the information system(s) covered by this system of records notice (SORN) and what remedies did the bureau/office enact following this Privacy Impact Assessment (PIA)?

Deficiencies:	**Remedies:**
a. When completed and operational, the CSFR will process information that is submitted from non-FCC sources, including individuals, businesses, vendors, institutions, contractors, etc. The FCC mayl need some way to verify that the information meets Data Quality guidelines.	a. OMD-FO will have security and other measures in place to safeguard the CFSR data and to insure that the information meets the data quality guidelines and other security requirements.
b.	b.
c.	c.

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

Initial implementation: October 2010
Secondary implementation:
Tertiary implementation:
Other implementation:

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

☐ Yes
☒ No

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

At this time in the planning and development of the CFSR information system, the FSOG staff in OMD-FO does not anticipate that there will be any ancillary or auxillary information systems linked to the final development and implementation of the CFSR information system.