

Federal Communications Commission
Office of the Managing Director



Privacy Threshold Analysis (PTA)¹
Core Financial System Replacement (CFSR)

August 22, 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 form is used to determine whether this information system requires a Privacy Impact Assessment.

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

The E-Government Act of 2002 defines an information technology and/or system by reference to the definition sections of Titles 40 and 44 of the United States Code (U.S.C.). The following summarize these definitions:

- “Information Technology” means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. *See* 40 U.S.C. 11101(6).
- “Information System” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *See* 44 U.S.C. 3502(8).

It is important, therefore, that when the FCC develops or makes changes to its information systems, the FCC should analyze what information the system will collect and maintain to determine whether there are any privacy issues.

The purpose of the **Privacy Threshold Assessment** is to help the FCC’s bureaus/offices evaluate the information/data in the system and make the appropriate determination about how to treat the information/data, as required by the Privacy Act’s regulations.

Thus, the Privacy Threshold Assessment helps the bureaus and offices to determine if the data in the information system include information about individuals, *e.g.*, personally identifiable information (PII), which will require a **Privacy Impact Assessment** to be conducted.

Section 1.0 Information System’s Status:

1.1 Status of the Information System:

- New information system—Implementation 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:

OMD-FO is creating a new financial system, the Core Financial System Replacement (CFSR), to replace several existing financial systems and to make other updates as required. This new CFSR information system will include the electronic records that are linked to the U.S. Treasury, several of the FCC's contractors, and FCC internal financial operations. The CFSR information system may also store and administer paper records and other documents in other formats, *i.e.*, diskettes, electronic tape, *etc.*

If this is a new information system, please skip to Question 1.6.

1.2 Has this information system existed under another name, or has the name been changed or modified?

- Yes
- No

Please explain your response:

1.3 Has this information system existed previously or been operated under any other software program, information system medium, *i.e.*, electronic database or paper files, and/or other format?

- Yes
- No

Please explain your response:

1.4 Has this information system existed under a system of records notice (SORN) by itself, or was it ever part or component of another SORN?

- Yes
- No

Please explain your response:

1.5 Is this information system being changed or upgraded, and if so, what are the purposes for changing or upgrading the information system, and/or will any changes now include personally identifiable information (PII):

- Yes
- No

Please explain your response:

1.6 Why is the information being collected, *e.g.*, what are the information system's purposes, intended uses, and/or functions:

OMD-FO's new Core Financial System Replacement (CFSR) will maintain personally identifiable information (PII) for the FCC's staff travel data that can be retrieved from the E-2 System. The information will be used to make travel and vendor payments, *i.e.*, contractor working at the FCC, *etc.*

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

Information about FCC Employees:

- No FCC employee(s) data
- FCC employee's name
- Other names used, *i.e.*, maiden name, *etc.*
- FCC badge number (employee ID)
- SSN

- US Citizenship
- Non-US Citizenship
- Race/ethnicity
- Gender
- Biometric data
 - Fingerprints
 - 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)
- 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 CFSR information system will also collect the FCC employee's log-in name and Federal Financial System (FFS) employee number ("internal use only").

Information about FCC Contractors

- No FCC contractor information :
- Contractor's name
- Other names used, *i.e.*, maiden name, *etc.*
- FCC Contractor badge number (Contractor ID)
- SSN
- US Citizenship
- Non-US Citizenship
- Biometric data
 - Fingerprints
 - 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 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: Taxpayer Identification Number (TIN) may be substituted.
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional affiliations
- Business/office address
- Intra-business office address (office or cubical number)
- 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
- Personal clubs and affiliations
- Credit card number(s)
- Bank account(s)
- Other information:

“Non-personal” information obtained from FCC sources:

- Not applicable
- Economic data
- Engineering/scientific data
- Accounting/financial data
- Legal/regulatory/policy data
- Other information, please specify:

Miscellaneous Business, Technology, or Other Information:

- Not applicable
- Not publicly available business or technology data, *i.e.*, trade or propriety information
- Other information, please specify:

1.8 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: Businesses provide financial information that the FCC requires for payments, *etc.*
- Non-personal information from institutions and other non-profit entities: Institutions and non-profit entities provide financial information that the FCC requires for payments, *etc.*
- Non-personal information from farms:
- Non-personal information from Federal Government agencies: National Financial Center (NFC) and the U.S. Department of the Treasury (DOJ).
- Non-personal information from state, local, or tribal governments: States, localities, and tribal governments.
- Other sources, please specify: Foreign entities, *i.e.*, International Telecommunications Settlements (ITS).

1.9 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:

At this time the Financial Systems Operations Group (FSOG) staff in OMD-FO believes that the CSFR will handle information for travel from OMD-FO's E-2 System.

If this information system is a “stand alone” information system, *e.g.*, it does not use information from another system, and/or it is not linked to another information system, please skip to Question 1.13.

1.10 If the system uses information, including information about individuals (PII), from other information systems, what information will be used?

Information system name(s): National Finance Center (NFC), Procurement Desktop (PD), and Budget Execution and Accounting Management Systems (BEAMS).

- Individual's name
- Other names, *i.e.*, maiden name, *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)
- 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
- Non-FCC government badge or employee ID number(s), *e.g.*, contractor's badge number.
- Law enforcement data
- Background investigation history
- Military history
- National security data
- Foreign countries visited
- Other information:

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

- Not applicable
- Name of business contact/firm representative, customer, or others
- Business/corporate purpose(s)
- Other business/employment/job description(s)
- Professional/Personal clubs and/or affiliations
- Partial SSN
- Intra-business office address (office or workstation)
- Business/office address
- Business telephone number(s)
- Business cell phone number(s)

- Business fax number(s)
- Business pager number(s)
- Business e-mail address(es)
- Race/Ethnicity
- Customers' gender(s)
- 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)
- Credit report(s)
- Other information:

Miscellaneous Business Information:

- Not applicable
- Not publicly available business data, i.e., trade or propriety information
- Other information, please specify:

“Non-personal” information:

- Not applicable
- Economic data
- Engineering/scientific data
- Accounting/financial data
- Legal/regulatory/policy data
- Other information, please specify:

1.11 What are the sources for the information from the other information system(s) 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:

- 1.12 Will the information system derive new information or create previously unavailable information through aggregation or consolidation from the information that will now be collected, including information that is being shared or transferred from another information system?

Yes
 No

Please explain your response:

At this time the FSOG staff in OMD-FO believes that the CFSR will not derive new information, create previously unavailable information, or consolidate information; however, these options may change as OMD-FO develops the CFSR information system

- 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:

At this time the FSOG staff in OMD-FO believes that the CFSR information system is being designed to retrieve PII by a name or unique identifier such as an individual's name.

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

Yes
 No

Please explain your response:

At such time as the CFSR replaces the Revenue Management Information System (RMIS), the Financial Systems Operations Group (FSOG) staff in OMD-FO may decide whether the CFSR information system will have the capability to make a determination about whether an individual has made payments to the FCC.

If the information system does not contain information about individuals, please skip to Question 1.16.

- 1.15 What is the potential impact or “security risk” 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 CFSR will include such personally identifiable information (PII) as SSNs in the data it collects, maintains, and uses.

1.16. What is the potential impact or “security risk” for the information that is maintained in the information system if an unauthorized disclosure or misuse of information occurs?
(check one)

- Results in little or no harm, embarrassment, inconvenience, or unfairness.
- Results in moderate harm, embarrassment, inconvenience, or unfairness.
- Results in significant harm, embarrassment, inconvenient, or unfairness.

Please explain your response:

The CFSR will include not only PII such as SSNs in the data it collects, maintains, and uses, CFSR will also collect, maintain, and use confidential or sensitive financial data.

1.17 Is this impact level consistent with the guidelines as determined by the FIPS 199 assessment?

- Yes
- No

Please explain your response:

At this stage in its development, the CFSR has not received its FIPS 199 assessment.

1.18 When was “Certification and Accreditation” (C&A) last completed?

At this stage in its development, the CFSR has not received its C&A.

1.19 Has the Chief Information Officer (CIO) and/or the Chief Security Officer designated this information system as requiring an

- Independent risk assessment
- Independent security test and evaluation
- Other risk assessment and/or security testing procedure, *etc.*
- Not applicable.

Please explain your response:

At this stage in its development, with the CFSR information system still in the planning stages, neither the CIO nor the CSO has made any such designations for the CFSR.

1.20 Based on the information that you have provided thus far, if:

- The information you are collecting does not includes information about individuals if you answered **NO** to questions 1.5, 1.7, 1.8, 1.9, 1.10, 1.11, 1.13, 1.14 and/or 1.16, then:

The information system (IT application or paper files) does not contain information about individuals nor does it have shared links with other information systems that may also contain information about individuals that could constitute a privacy issue.

A Privacy Impact Assessment is **not required**.

- The information you are collecting does include information about individuals, and you answered **YES** to questions 1.5, 1.7, 1.8, 1.9, 1.10, 1.11, 1.13, 1.14, and /or 1.15, then:

The information system (IT application or paper files) does contain information about individuals, or it does have shared links with other information systems that may also contain information about individuals that could constitute a privacy issue.

The information system **requires** a Privacy Impact Assessment (PIA)