Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the webTA Information System

April 26, 2013

FCC Bureau/Office: Office of Managing Director (OMD)
Division: Human Resources Management (HRM)

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

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

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

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

Section 1.0 Information System's Contents:

1.1 Status of the Information System[2]:

☐ New information system—Implementation date:
☒ Revised or upgraded information system—Revision or upgrade date: March 2013

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

☒ Placed in existing information system—Implementation Date: March 2013
☐ Placed in new auxiliary/ancillary information system—Date:
☐ Other use(s)—Implementation Date:

Please explain your response:

The FCC's Human Resources Management (HRM) is upgrading the Time and Attendance Records ("TAR") information systems ("TAR system") to add the webTA information system ("webTA") as a subsystem. The webTA system provides an electronic template for inputting each FCC employee's time and attendance data. The personally identifiable information (PII) in TAR and the webTA subsystem webTA is being added as a subsystem that provides an electronic template for inputting each FCC employee's time and attendance data. The TAR systems. are covered by a FCC system of records, FCC/OMD-28, "Time and Attendance Records."

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

☐ Yes
Date:

☒ No

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

The FCC did not create a PTA because it was previously established in the FCC/OMD-16, "Pay and Leave" PIA that Time and Attendance Records ("TAR systems") information systems and any auxiliary and/or ancillary information systems and databases like the webTA subsystem will contain PII. The TAR systems, including webTA, are covered by a system of records notice, FCC/OMD-28, "Time and Attendance Records Leave Records," PIA.

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

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

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

☐ Yes
☒ No

Please explain your response:

As noted in Question 1.2, TAR system of which webTA is a subsystem, have been included in the FCC/OMD-16, "Pay and Leave" PIA.

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 addition of webTA has not made any substantive changes to the TAR system's format or operating system. WebTA has been added as a subsystem.

If there have been no changes to the information system's format or operating system(s), 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:

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

Please explain your response:

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

Information about FCC Employees:

☐ No FCC employee information
☒ FCC employee's name
☐ Other names used, *i.e.*, maiden name, *etc*.
☐ FCC badge number (employee ID)
☒ SSN
☐ Race/Ethnicity
☐ Gender
☐ U.S. Citizenship
☐ Non-U.S. Citizenship
☐ Biometric data
  ☐ Fingerprints
  ☐ Voiceprints
  ☐ Retina scans/prints
  ☐ Photographs
  ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
☒ Birth date/age

☐ Place of birth
☐ Medical data
☐ Marital status
☐ Spousal information
☐ Miscellaneous family information
☐ Home address
☐ Home address history
☐ Home telephone number(s)
☐ Personal cell phone number(s):
☐ Personal fax number(s)
☒ E-mail address(es): FCC e-mail address.
☐ 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: WebTA exchanges data between the FCC and the USDA and NFC payroll/personnel systems to administer the pay and leave information for FCC employees: work data--office/work station, bureau/office, timekeeper number, pay plan, number of hours worked, leave accrual rate, usage, and balances, and associated supporting documentation such as request for leave, credit hours earned, compensatory and overtime hours requested and earned, time off awards credited, leave transfer requests, leave donor forms, medical documentation to support advance of sick leave and leave transfer, tax, payroll allotment, and direct deposit forms, etc.

Information about FCC Contractors:

☒ No FCC contractor information
☐ Contractor's name
☐ Other name(s) used, *i.e.*, maiden name, *etc*.
☐ FCC Contractor badge number (Contractor ID)
☐ SSN
☐ U.S. Citizenship
☐ Non-U.S. Citizenship
☐ Race/Ethnicity
☐ Gender
☐ Biometric data
  ☐ Fingerprints
  ☐ Voiceprints
  ☐ Retina scans/prints
  ☐ Photographs
  ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
☐ Birth date/Age

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

Information about FCC Volunteers, Visitors, Customers, and other Individuals:

☒ Not applicable
☐ Individual's name:
☐ Other name(s) used, *i.e.*, maiden name, *etc*.
☐ FCC badge number (employee ID)
☐ SSN:
☐ Race/Ethnicity
☐ Gender
☐ Citizenship
☐ Non-U.S. Citizenship
☐ Biometric data
  ☐ Fingerprints
  ☐ Voiceprints
  ☐ Retina scans/prints
  ☐ Photographs
  ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
☐ Birth date/Age:
☐ Place of birth
☐ Medical data
☐ Marital status
☐ Spousal information
☐ Miscellaneous family information
☐ Home address
☐ Home address history

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

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:

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

- ☒ Personal information from FCC employees: PII in webTA, is obtained from current and former 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:

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

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

- ☒ The information system is a subsystem or other component of another information system or database that is operated by another FCC bureau/office or non-FCC entity (like the FBI, DOJ, National Finance Center, etc.);
- ☒ The information system transfers or receives information, including PII, between itself and another FCC or non-FCC information system or database: USDA's National Finance Center (NFC).
- ☒ The information system has other types of links or ties to other FCC or non-FCC information systems or databases;
- ☒ The information system has other characteristics that make it linked or connected to another FCC or non-FCC information system or database;
- ☐ The information system has no links to another information system (or database), *i.e.*, it does not share, transfer, and/or obtain data from another system.

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

As noted in Question 1.8, webTA is a subsystem of the TAR information systems that is used to administer HRM's payroll and personnel programs. These systems are linked electronically to information systems at the USDA and NFC payroll/personnel system(s). The FCC employees use webTA as the electronic template to input their weekly time and attendance data, which is then submitted to the NFC electronically.

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

- ☒ FCC information system and information system name(s): Information is obtained from systems associated with HRM's employee wage and benefits functions.
- ☒ Non-FCC information system and information system name(s): Information (as listed in Question 1.6) is obtained from the USDA and NFC payroll/personnel system.
- ☒ 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)
- ☒ E-mail address(es): FCC e-mail address.
- ☐ 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: WebTA exchanges data between the FCC and the USDA and NFC payroll/personnel systems to administer the pay and leave information for FCC employees: work data--office/work station, bureau/office, timekeeper number, pay plan, number of hours worked, leave accrual rate, usage, and balances, and associated supporting documentation such as request for leave, credit hours earned, compensatory and overtime hours requested and earned, time off awards credited, leave transfer requests, leave donor forms, medical documentation to support advance of sick leave and leave transfer, tax, payroll allotment, and direct deposit forms, etc.

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

- ☒ Not applicable
- ☐ Name of business contact/firm representative, customer, and/or others
- ☐ Race/Ethnicity
- ☐ Gender

☐ Full or partial SSN:
☐ Business/corporate purpose(s)
☐ Other business/employment/job description(s)
☐ Professional affiliations
☐ Intra-business office address (office or workstation)
☐ Business telephone number(s)
☐ Business cell phone number(s)
☐ Business fax number(s)
☐ Business e-mail address(es)
☐ Bill payee name
☐ Bank routing number(s)
☐ Income/Assets
☐ Web navigation habits
☐ Commercially obtained credit history data
☐ Commercially obtained buying habits
☐ Personal clubs and affiliations
☐ Credit card number(s)
☐ Bank account(s)
☐ Other information:

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

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

Does a SORN cover the PII in this information system?

☒ Yes: As noted above, webTA is a TAR subsystem.
☐ No

If yes, what is this SORN: FCC/OMD-28, "Time and Attendance Records."

Please provide the citation that was published in the *Federal Register* for the SORN: 76 FR 55388 (correction notice) and 76 FR 51975.

Section 2.0 System of Records Notice (SORN):

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

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

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

This system of records is located in Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

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

The records in this system consist of current and former employees of the Federal Communications Commission (FCC).

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

The categories of records in the TAR systems are used:

1. To administer the pay, leave, and garnishment requirements for FCC employees: FCC employee's name, work and home address, individual's Security Number (SSN), bureau/office, timekeeper number, salary, pay plan, number of hours worked, leave accrual rate, usage, and balances, and associated supporting documentation such as Request for Leave, Credit Hours earned, Compensatory and Overtime hours requested and earned, time off awards credited, leave transfer requests, leave donor forms, medical documentation to support advance of sick leave and leave transfer, tax, payroll allotment, and direct deposit forms, etc.; and
2. To administer garnishment and levy orders: Orders served upon the FCC for implementation, correspondence, and memorandum issued by a court of competent jurisdiction or by another government entity authorized to issue such an order for a FCC employee subject thereto.

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

1. To administer the pay and leave, and garnishment records: 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq. and 6301 et seq.; 28 U.S.C. 66a; 44 U.S.C. 2801 and 2802; 5 U.S.C. 6328-6340; Federal Employees Leave Sharing Act of 1988 and Amendments of 1993 (Pub. L. 103-103 and Pub. L. 100-566); Executive Order 9397, November 22, 1943; Pub. L. 100-202, Pub. L. 100-440, Pub. L. 101-509, and Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub. L. 104-193); and
2. To administer the garnishment and levy orders: 5 U.S.C. 5520a; 10 U.S.C. 1408; and 42 U.S.C. 659.

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

The Human Resources Management (HRM) uses the records in this system to:

1. Authorize payroll deductions, including but not limited to allotments, charitable contributions, and union dues;
2. Collect indebtedness, including but not limited to overpayment of salary and unpaid Internal Revenue Service (IRS) taxes and/or state taxes, etc.;
3. Pay income tax obligations, including but not limited to the Internal Revenue Service (IRS) and states' revenue departments;
4. Authorize the U.S. Department of the Agriculture's (USDA) National Finance Center (NFC) to issue salary checks;
5. Report gross wages and compensation information, including but not limited to unemployment compensation;
6. Pay any uncollected compensation, including but not limited to lump-sum payments of leave upon an employee's separation, such as retirement and resignation, or due to the beneficiaries of a deceased employee;

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

7. Determine leave balances, including but not limited to accrued and used leave, sick leave, eligibility for and/or authorize donations for the leave transfer program, and other types of leave categories;
8. Produce summary descriptive statistics and analytical studies in support of the FCC's Human Resource Management (HRM) functions;
9. Respond to general requests for statistical information (without disclosing any personally identifiable information (PII)) under the Freedom of Information Act (FOIA);
10. Locate specific individuals for Human Resource Management (HRM) functions; and
11. Direct the FCC's implementation of garnishment and levy orders served upon the Commission for implementation, correspondence, and memorandum, issued by a court of competent jurisdiction or by another government entity authorized to issue such an order for a Commission employee subject thereto.

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

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

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

Disclosure may be made from the TAR systems, the including webTA subsystem, to consumer reporting agencies as defined in the Fair Credit Reporting Act, 15 U.S.C. 1681a(f), or the Federal Claims Collection Act of 1966, 28 U.S.C. 3701(a)(3).

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

The information in the TAR systems includes paper documents, records, and files that stored in file cabinets in the HRM office suite, and electronic records, files, and data that are stored in the FCC's computer network databases. WebTA is a fully electronic subsystem of the TAR systems--it has no paper records, documents, or files.

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

The records in this system are indexed by the FCC employee's name.

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

The paper documents, files, and records, which are stored in file cabinets in the HRM office suite, are locked when not in use and/or at the end of the business day. These file cabinets are accessible only via card-coded security doors. Access is restricted to authorized HRM supervisors, staff, and contractors.

The electronic records, files, and data, including those for webTA subsystem, are housed in the FCC's computer network databases. Access to the electronic files is restricted to authorized HRM supervisors, staff, and contractors. Authorized staff and contractors in the FCC's Information Technology Center (ITC), who manage the FCC's computer network databases, also have access to the electronic files. Other FCC employees and contractors may be granted access on a "need-to-know" basis. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. The electronic information is backed-up routinely. Back-up tapes are stored on-site and at a secured, off-site location.

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

1. For Pay and Leave Records – the FCC maintains and disposes of these records in accordance with General Records Schedule 2 (GRS 2) issued by the National Archives and Records Administration (NARA). Under the GRS 2, records are retained for various periods. Generally, the records are kept from 3 to 56 years, depending on the type of record involved.

2. For Garnishment and Levy of Wages Records – the FCC retains these records until the expiration of the garnishment or levy order or until the employee leaves the Commission, whichever comes first. In some instances that are related to a garnishment or levy order, the information is destroyed three years after the termination of the garnishment or levy order.

Disposal of the paper documents, records, and files is by shredding. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

Individuals may request a copy of the (document) disposition instructions from the FCC Privacy Act Officer or access GRS 2 directly at http://www.archives.gov/records-mgmt/ardor/grs02.html.

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

The sources of the records in the TAR systems are FCC employees and FCC managers, bankruptcy courts, state domestic relations courts, state public health and welfare departments or agencies, Internal Revenue Service, and intra-agency memoranda.

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

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

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

3.2 Where will the information system be housed?

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

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

- ☒ FCC staff in this bureau/office exclusively: The supervisors and staff in HRM's Payroll and Benefits Service Center have responsibility for access and proper use of the information in the TAR systems, including webTA.
- ☐ FCC staff in other bureaus/offices:
- ☐ Information system administrator/Information system developers:
- ☐ Contractors:
- ☐ Other information system developers, *etc*:

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

As noted in Questions 2.11 and 3.3, access to the paper documents, files, and records, and the electronic records, files, and data in the TAR systems, including webTA subsystem, which are hosted on the FCC's computer network databases, is restricted to the HRM supervisors and staff in the Payroll and Benefits Service Center.

3.5 How much access will users have to data in the information system(s)?

- ☒ Access to all data: HRM supervisor and staff may access all data, as necessary to administer this system, including webTA subsystem.
- ☒ Restricted access to data, as determined by the information system manager, administrator, and/or developer: FCC employees and contractors may be granted access only on a "need-to-know" basis to this system, as dictated by their job duties and responsibilities.
- ☐ Other access policy:

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

- ☒ Information system managers: HRM supervisors and staff and ITC supervisors, staff, and contractors.
- ☒ Information system administrators: ITC supervisors, staff, and contractors.
- ☐ Information system developers:
- ☒ FCC staff in this bureau/office: HRM employees and contractors are granted access on a "need to know" basis.
- ☒ FCC staff in other bureaus/offices: Other FCC employees and contractors are granted access on a "need-to-know" basis.
- ☒ FCC staff in other bureaus/offices in FCC field offices: FCC employees and contractors are granted access based on a "need to know" basis.
- ☒ Contractors: Contractors working under HRM and ITC authority.
- ☒ Other Federal agencies: if the FCC approves request(s) under the routine use(s) (Federal agencies) and/or such routine uses and memoranda of understanding (M&O) already exist or are authorized.
- ☐ State and/or local agencies:
- ☐ Businesses, institutions, and other groups:
- ☐ International agencies:
- ☐ Individuals/general public:
- ☒ Other groups: if the FCC approves a request under a routine use (Foreign governments).

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

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

The ITC supervisors provide periodic privacy training to the ITC contractors who handle the PII that is contained in the TAR systems, including webTA subsystem.

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

The OGC staff has reviewed and signed-off on the Section M contracts for the ITC contractors who manage TAR, including webTA. As noted in Question 1.1 *et al*., the PII contained in these systems is covered by FCC/OMD-28, "Time and Attendance Records" SORN, as required by Sections 52.224-1 and 52.224-2 of the Federal Acquisition Regulation (FAR).

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

3.9 If the information system has links to other information systems (or databases), *i.e.*, it shares, transmits, or has other linkages, with what other non-FCC organizations, groups, and individuals will the information be shared?
(Check all that apply and provide a brief explanation)

- ☒ Other Federal agencies: USDA's NFC payroll/personnel system.
- ☐ State, local, or other government agencies:

☐ Businesses:
☐ Institutions:
☐ Individuals:
☐ Other groups:

Please explain your response:

WebTA is linked to the USDA's NFC payroll/personnel systems with which it exchanges FCC employee time and attendance data, *i.e.*, the NFC process the data and pays FCC employees.

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

☐ Yes
☒ No

Please explain your response:

As noted above, webTA is linked to the USDA's NFC systems. WebTA has no links to other internal FCC information systems. The USDA's NFC systems are covered by the Federal PIA requirements, *i.e.*, the PIA for the NFC systems would be done by the USDA .

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

The FCC has memoranda of understanding (MOU) and other security requirements, etc., to safeguard the transmission and receipt of information between the TAR systems, including webTA, and the USDA's NFC systems. The MOU/ISA between FCC and USDA NFC was signed on 05/01/2013.

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

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

The MOU/ISA between FCC and USDA NFC (signed on 5/1/2013) as written, complies with Federal statutes and OMB and NIST regulations.

3.13 Is this a new or a renewed matching agreement?

☐ New matching agreement
☒ Renewed matching agreement

Please explain your response:

The MOU/ISA between FCC and USDA NFC was signed on 05/01/2013. It is renewed on an annual basis.

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

☒ Yes; if yes, on what date was the agreement approved: Signed on 05/01/2013
☐ No

Please explain your response:

The Data Integrity Board will meet later in FY 2013.

3.15 Is the information that is covered by this SORN, which is transmitted or disclosed with the external organization(s), comply with the terms of the *MOU* or other "matching agreement?"

As noted above, the MOU/ISA between the FCC and the USDA NFC complies with Federal statutes and OMB and NIST regulations.

3.16 Is the shared information secured by the recipient under the *MOU*, or other "matching agreement to prevent potential information breaches?"

As noted above, the MOU/ISA between the FCC and the USDA NFC complies with Federal statutes and OMB and NIST regulations governing information transfer or exchanges with other Federal agencies.

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

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

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

☒ Information is processed and maintained only for the purposes for which it is collected.

☒ Information is reliable for its intended use(s).
☒ Information is accurate.
☒ Information is complete.
☒ Information is current.
☐ Not applicable:

Please explain any exceptions or clarifications:

The PII in webTA, is obtained from FCC employees and from USDA's NFC systems (non-FCC system). HRM performs routine checks to insure that this meets the Data Quality guidelines. FCC employees must adhere to the Data Quality guidelines in submitting their pay and leave data in webTA, *i.e.*, there is a notice that falsification of the information that employees input into webTA may lead to disciplinary action and/or criminal sanctions under 18 U.S.C. 1001.

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

4.2 If any information collected from non-FCC sources, how will the information sources be checked for accuracy and adherence to the Data Quality guidelines?
(Please check all that apply and provide an explanation)

☒ Yes, information is collected from non-FCC sources: As noted in Question 1.8, the webTA has electronic links to the USDA's NFC payroll/personnel system(s). HRM uses webTA to administer HRM's payroll and leave functions. The data are exchanged and/or transferred between webTA and the NFC systems on a regular basis.

☒ Information is processed and maintained only for the purposes for which it is collected:

☒ Information is reliable for its intended use(s):
☒ Information is accurate:
☒ Information is complete:
☒ Information is current:

☐ No information comes from non-FCC sources:

Please explain any exceptions or clarifications:

The data that webTA collects, stores, and uses are subject to the Data Quality guidelines--the NFC will also perform routine checks on the data to insure its compliance.

If the information that is covered by this SORN is not being aggregated or consolidated, please skip to Question 4.5.

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

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

FCC employees must certify that the number of hours and leave represented as their time and attendance bi-weekly totals that are input into webTA are accurate. Employees must also understand that falsification may lead to disciplinary action and/or criminal sanctions under 18 U.S.C. 1001.

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

HRM does periodic checks of the information, including the PII covered by FCC/OMD-28 SORN, which is collected, stored, maintained, transmitted, and used in the webTA subsystem to insure that it complies with the Data Quality guidelines.

Section 5.0 Safety and Security Requirements:

5.1 How are the records/information/data in the information system or database covered by this SORN stored and maintained?

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

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

☐ Yes
☒ No

Please explain your response:

The information in these systems, including webTA, is unique. It is used exclusively to compile the data that are used to administer the FCC employees' payroll/leave program.

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

As noted in Questions 5.2, the information, including the PII covered by FCC/OMD-28 SORN, which is in the TAR systems, including webTA subsystem, is unique and is used for the FCC's payroll and leave programs, as required by Federal regulations. These information systems are essential FCC systems, *i.e.*, their unavailability would prevent the timely performance of FCC operations.

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

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

Please explain your response:

As noted above, webTA is used to administer the FCC's payroll and leave programs.

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

☒ Yes
☐ No

Please explain your response:

As noted in Question 4.5, the TAR systems, including webTA, are used administer the FCC's payroll and leave programs, *i.e.*, these systems and subsystems collect and store information on employees' payroll and leave data. HRM uses this information to compile various reports on employee compensation and leave and related issues.

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

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

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

As noted in Question 5.5, the information, including the PII that is covered by FCC/OMD-28 SORN, in webTA, is collected to provide the necessary information for HRM to carry out its responsibilities as the FCC's payroll and leave programs, as required by Federal and state statutes.

5.7 Do individuals have the right to the following?

They may decline to provide their PII?

Yes ☐
No ☒

They may consent to particular uses of their PII?

Yes ☐
No ☒

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

FCC employees must provide their SSN, Date and Place of Birth, and other data which are requirements for Federal employment.

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

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

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

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

☐ The information system has a link to the FCC's Internet address at www.fcc.gov or other customer-facing URL;
☒ The information system has a customer-facing web site via the FCC Intranet for FCC employees;
☐ The information is collected from the individual by fax;
☐ The information is collected from the individual by e-mail;
☒ The information is collected from the individual by completing a FCC form, license, and/or other document: FCC employees complete the requisite OMB and FCC personnel forms so that HRM can process employees' payroll and related administrative and personnel deductions, etc.

☐ The information is collected from the individual by regular mail; and/or
☒ The information concerning individuals is collected by other methods: PII from the USDA, NFC is submitted to the FCC electronically, and by fax, mail, and other methods, as applicable. Information that is not transmitted electronically is input by HRM staff. The data are stored in the TAR systems, including the webTA subsystems.

Please explain your response:

HRM collects the applicable employee data that is contained in webTA, from FCC employees themselves and the NFC, which it to determine the appropriate payroll and leave benefits for each FCC employee.

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

☐ The system contains a link to the FCC's privacy policies for all users at the FCC's website www.fcc.gov:
☐ A Privacy Notice is displayed on the webpage:
☒ A Privacy Notice is printed at the end of the FCC form(s), license(s), and/or other Commission document(s): HRM collects information directly from FCC employees when they submit their bi-weekly payroll and leave data.
☐ The FCC Intranet site displays a Privacy Notice:
☐ The collection or input mechanism uses another method to provide individuals with the Privacy Notice:
☐ No Privacy Notice is provided:

5.12 If a Privacy Notice is provided, which of the following are included?

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

Please explain your response:

5.13 Will consumers have access to information and/or the information system on-line via www.FCC.gov?[4]

☐ Yes
☒ No

Please explain your response:

The PII in the webTA subsystem pertains exclusively to FCC employees and their bi-weekly work and leave data. WebTA is not accessible via the FCC's website--only via the FCC Intranet.

[4] The FCC's web policy does not allow anyone under 13 years of age to have access to the FCC website.

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

- ☒ Account name
- ☒ Passwords
  - ☒ Accounts are locked after a set period of inactivity
  - ☒ Passwords have security features to prevent unauthorized disclosure, *e.g.*, "hacking"
  - ☒ Accounts are locked after a set number of incorrect attempts
  - ☐ One time password token
  - ☐ Other security features:
- ☒ Firewall
- ☒ Virtual private network (VPN)
- ☐ Data encryption:
- ☒ Intrusion detection application (IDS)
- ☐ Common access cards (CAC)
- ☐ Smart cards:
- ☐ Biometrics
- ☐ Public key infrastructure (PKI)
- ☐ Locked file cabinets or fireproof safes
- ☐ Locked rooms, with restricted access when not in use
- ☐ Locked rooms, without restricted access
- ☐ Documents physically marked as "sensitive"
- ☒ Guards
  - ☒ Identification badges
  - ☒ Key cards
  - ☐ Cipher locks
  - ☐ Closed circuit TV (CCTV)
- ☐ Other:

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

All FCC employees and contractors are required to complete the FCC's annual Commission-wide privacy training. HRM also provides various notices and warnings to HRM employees and contractors who have access to this PII that it is not to be shared or disclosed without authorization.

5.16 How often are the security controls reviewed?

- ☐ Six months or less:
- ☒ One year: HRM conducts an annual security review for its paper document files. The HRM reviews its computer database records and files in cooperation with ITC.
- ☐ Two years
- ☐ Three years:
- ☐ Four years
- ☐ Five years
- ☐ Other:

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

- ☐ There is no training
- ☒ One year: As noted in Question 5.15, the FCC has an annual Commission-wide privacy training program that all FCC employees and contractors must complete. This annual privacy training annually was instituted in September 2006.
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other:

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

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

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

- ☐ Less than one year:
- ☐ One year:
- ☐ Two years
- ☒ Three or more years: ITC does a review at least every three years.
- ☒ Other re-certification procedures: The HRM management does periodic evaluations of their staff security clearance authorizations.

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

WebTA complies with the FISMA requirements.

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

5.21 What is the potential impact on individuals on whom the information is maintained in the information system(s) if unauthorized disclosure or misuse of information occurs? (check one)

- ☐ Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual.
- ☐ Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual.
- ☒ Results in significant harm, embarrassment, inconvenient, or unfairness to the individual.

Please explain your response:

WebTA subsystem does contain very sensitive PII, *e.g.*, SSN; however, the input template only requires employees to submit their bi-weekly time and attendance data. Unauthorized disclosure would create significant privacy issues for those whose PII was inadvertently disclosed.

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

The FIPS assessment level is "moderate."

5.23 When was the "Assessment and Authorization" (A&A) completed for the information system(s) covered this SORN—please provide the A&A completion date?

An Authorization to Operate (ATO) was issued for the webTA information system on March 6, 2013.

5.24 Has the Chief Information Officer (CIO) and/or the Chief Information Security Officer (CISO) 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:

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

WebTA is hosted on the FCC's computer network. WebTA, as a subsystem of TAR, includes various advanced security and safety features that provide improvements in HRM's payroll processing and other, related functions to prevent hacking and other unauthorized access to this PII.

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

The webTA subsystem only collects PII from FCC employees, *i.e.*, there are no impacts on contractors or the general public. As noted in Question 5.3, webTA is an essential FCC information system that performs all FCC payroll and leave functions. Without it, HRM could not function properly. The privacy impacts are limited to those that are necessary for the efficient functioning of the FCC's payroll and related HRM employee/personnel operations, as required by Federal regulations, etc.

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

WebTA is used solely to collect information that is used for payroll and leave functions. It has no other functions or IT capabilities.

If the information system does not include any monitoring capabilities, please skip to **Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):**

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

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

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

If this information system or database only affects FCC employees, please skip to Section 9.0[5]

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

☐ FCC forms, licenses, or other documentation;
☐ Participation in marketing, consumer, or customer satisfaction surveys or questionnaires;
☐ Recordkeeping or related activities.

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

☐ Yes, the information system includes any paperwork and/or recordkeeping requirements that non-FCC employees and contractors must complete.
☒ No, the information system does impose any paperwork and/or recordkeeping requirements, *i.e.*, the information it collects does not constitute an "information collection" as defined by the PRA.

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

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

☐ Yes
☐ No or Not applicable

Please explain your response:

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

[5] PRA requirements exclude information collections, *e.g.*, forms, surveys, questionnaires, etc., that pertain solely to Federal employees.

6.4 Are there are any FCC forms associated with the information system(s) covered by this SORN, and if so, do the forms carry the Privacy Act notice?

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

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

Individuals wishing to inquire whether FCC/OMD-28, "Time and Attendance Records" SORN, contains information about them may address their inquiries to the HRM system manager in OMD. This is consistent with FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act, as noted in this SORN.

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

Individuals who seek access to the information about them that is contained in FCC/OMD-28, "Time and Attendance Records" SORN, may address their inquiries to the HRM system manager in OMD. This is consistent with FCC policies and rules under 47 CFR §§ 0.554 – 0.555, as noted in the SORN.

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

Individuals seeking to correct or to amend information about in FCC/OMD-28, "Time and Attendance Records" SORN, may address their inquiries to the HRM system manager in OMD. This is consistent with FCC policies and rules under 47 CFR §§ 0.556 – 0.558, as noted in the SORN.

7.4 Does the FCC provide any redress to amend or correct information about an individual covered by this SORN, and if so, what alternatives are available to the individual, and are these consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

Individuals seeking any redress to amend or correct information about them in FCC/OMD-28, "Time and Attendance Records" SORN, may address their inquiries to the HRM system manager in OMD. This is consistent with FCC policies and rules under 47 CFR §§ 0.556 – 0.558, as noted in the SORN.

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

FCC/OMD-28, "Time and Attendance Records" SORN does not claim any exemption to the notification, access, and correction and/or amendment procedures, as they apply to individuals seeking information about themselves in this SORN.

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

The HRM staff issue periodic reminders to the staff who work with the information in this information system, including the PII that is covered by FCC/OMD-28 SORN, that it is "non public for internal use only," and that they should keep the information confidential and safeguard any printed materials.

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

- ☐ Six months or less
- ☐ One year
- ☐ Two years
- ☐ Three years:
- ☐ Four years
- ☐ Five years
- ☒ Other audit scheduling procedure(s): HRM conducts period reviews of webTA's functions.

Section 8.0 Consumer Satisfaction:

8.1 Is there a customer or consumer satisfaction survey included as part of the public access to the information covered by this information system or database??

- ☐ Yes
- ☐ No
- ☒ Not applicable

Please explain your response:

There is no consumer satisfaction survey attached to the TAR systems, including the webTA subsystem.

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:

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. WebTA is a fully electronic system; however HRM may occasionally use paper format documents for certain purposes. The paper documents are stored in file cabinets in the HRM office suite.	a. The paper format documents that contain PII are stored in file cabinets that are locked when not in use. These file cabinets are located in the HRM office suite, which is protected by card coded doors to minimize access to this suite. The building entrances have monitors to detect unauthorized individuals. Also, the presence of non-HRM staff in where the file cabinets are located would be easily observed background.
b. PII that is stored in webTA is housed in the FCC's computer network databases.	b. This information is protected by passwords and other security features and protocols to insure that unauthorized access is highly unlikely and would be easily detected.

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

Initial implementation: March 2013
Secondary implementation:
Tertiary implementation:
Other implementation:

9.3 Are there any ancillary and/or auxiliary information system(s) or database(s) linked to this information system that are covered by this SORN, which may also require a Privacy Impact Assessment (PIA)?

☒ Yes
☐ No

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

As noted in Question 1.7 *et al.*, webTA is a subset of the TAR systems, which are hosted on the FCC's computer network databases. The FCC is in the process of updating the PIA covering the TAR systems.