

Federal Communications Commission

System of Records Notices (SORNs), 2014-2015

Brought to you by AltGov2

www.altgov2.org/FOIALand

Federal Communications Commission (FCC)

Table of Contents

[Systems of Records Published Between January 2, 2014 and December 31, 2015](#)

[FCC /Central-1—Pay and Leave Records.](#)

[FCC /Central-1—Employee Locator System.](#)

[FCC /Central-5—Drug-Free Federal Workplace Program.](#)

[FCC /Central-6—Personal Investigation Records.](#)

[FCC /Central-7—Freedom of Information Act \(FOIA\) Case Files.](#)

[FCC /Central-8—Telephone Call Detail and Equipment Loan Records.](#)

[FCC /Central-9—Denial of Federal Benefits \(Drug Debarment List\).](#)

[FCC /Central-10—Access Control System.](#)

[FCC /Central-11—Inter-office \(GroupWise\) and Internet E-mail Systems.](#)

[FCC /Central-12—Garnishment and Levy of Wages.](#)

[FCC /CIB-1—Informal Complaints, Inquiries, and Requests for Dispute Assistance.](#)

[FCC /CGB-1—Informal Complaints and Inquiries.](#)

[FCC /CGB-2—Comment Filing System \(ECFS\).](#)

[FCC /CGB-3—National Deaf-Blind Equipment Distribution Program \(NDBEDP\).](#)

[FCC /CGB-4— Internet-based Telecommunications Relay Service-User Registration Database \(ITRS-URD\) Program.](#)

[FCC /EB-5—Enforcement Bureau Activity Tracking System \(EBATS\).](#)

[FCC /MB-1—Ownership Report for Commercial Broadcast Stations.](#)

[FCC /MB-2—Broadcast Station Public Inspection Files.](#)

[FCC /OCBO-1—Small Business Contacts Database.](#)

[FCC /OET-1—Experimental Radio Station License Files.](#)

[FCC /OET-2—Equipment Authorization Records and Files.](#)

[FCC /OGC-3—Adjudication of Internal Complaints against Employees.](#)

[FCC /OGC-5—Pending Civil Cases.](#)

[FCC /OGC-6—Private or Civil Injury Claimants.](#)

[FCC /OIG-3—Investigative Files.](#)

[FCC /OLA-1—Legislative Management Tracking System \(LMTS\).](#)

[FCC /OMD-2—Labor Relations and Employee Performance Files](#)

[FCC /OMD-3—Federal Advisory Committee Membership File \(FACA\).](#)

[FCC /OMD-6—Financial Accounting Systems \(FAS\).](#)

[FCC /OMD-7—FCC Employee Transit Benefit and Parking Permit Programs.](#)

[FCC /OMD-9—Commission Registration System \(CORES\).](#)

[FCC /OMD-12—Integrated Library System \(ILS\) Records.](#)

[FCC /OMD-13—Data Quality Comments.](#)

[FCC /OMD-15—Employee Locator System.](#)

[FCC /OMD-16—Personnel Security Files. Note: This system of records was formerly titled "Personnel Investigation Records."](#)

[FCC /OMD-17—Freedom of Information Act \(FOIA\) Case Files.](#)

[FCC /OMD-18—Telephone Call Detail.](#)

[FCC /OMD-19—Denial of Federal Benefits \(Drug Debarment List\).](#)

[FCC /OMD-20—Inter-office and Remote Access Internet E-mail Systems.](#)

[FCC /OMD-22—Equipment Loan Records.](#)

[FCC /OMD23—Cadapult Space Management System \(CSMS\).](#)

[FCC /OMD-24—Physical Access Control System \(PACS\). Note: This system of records was formerly titled "Access Control System."](#)

[FCC /OMD-8—Time and Attendance Records.](#)

[FCC /OMD-30—FCC Visitors Database.](#)

[FCC /PSHSB-1—FCC Emergency and Continuity Contacts System \(ECCS\).](#)

[FCC /PSHSB-2—PSHSB Contact Database.](#)

[FCC /OSP-1—Broadband Dead Zone Report and Consumer Broadband Test.](#)

[FCC /OWD-1—Reasonable Accommodation Requests under the Rehabilitation Act of 1973.](#)

[FCC /WTB-1—Wireless Services Licensing Records.](#)

[FCC /WTB-5—Application Review List for Present or Former Licensees, Operators, or Unlicensed Persons Operating Radio Equipment Improperly.](#)

[FCC /WTB-6—Archival Radio Operator Records.](#)

[FCC /WTB-7—Remedy Action Request System \(RARS\).](#)

[FCC /WCG-1—Lifeline Program](#)

[Privacy Act Regulations](#)

[\[Return to TOP\]](#)

Systems of Records Published Between January 2, 2014 and December 31, 2015

2014

[FCC/CGB-1, Informal Complaints, Inquiries, and Requests for Dispute Assistance : August 15](#)

2015

[FCC/CGB-4, Internet-based Telecommunications Relay Service-User Registration Database \(ITRS-URD\) Program: February 9](#)

[FCC/OMD-32, FCC Telework Program : March 26](#)

[\[Return to TOP\]](#)

FCC /Central-1

System Name:

Pay and Leave Records.

System Location(s):

Associate Managing Director, Human Resources Management, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW, Room 1-B104, Washington, DC 20554. See FCC telephone directory for field office addresses.

Categories of Individuals Covered by the System:

Employees of the Federal Communications Commission.

Categories of Records in the System:

This system contains various records, including Social Security Numbers, which are required to administer the pay and leave requirements of the Commission.

Authority for Maintenance of the System:

44 U.S.C. 3101, 3102, and 3309; 5 U.S.C. 6331-6340; Pub. L. 100-566, Leave Transfer Program; Executive Order 9397

(November 22, 1943), which authorizes the use of the Social Security Number; and Pub. L. 104-193, Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

Purpose(s):

1. To authorize payroll deductions for allotments, savings bonds, charitable contributions, union dues, health benefits, and life insurance; collect indebtedness for overpayment of salary and unpaid Internal Revenue taxes; pay income tax obligations to Internal Revenue Service; authorize issuing of salary checks by Treasury Department; report gross wages and separation information for unemployment compensation; pay any uncollected compensation due a deceased employee; provide for a periodic summary of employee payroll data and retirement contributions; and determine eligibility for and/or authorize donations for the leave transfer program.
2. As a data source for management information for production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related personnel management functions or manpower studies; may also be utilized to respond to general requests for statistical information (without personal identification of individuals) under the Freedom of Information Act or to locate specific individuals for personnel research or other personnel management functions.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

1. Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be referred to the appropriate federal, state, or local agency responsible for investigating or prosecuting a violation or for enforcing or implementing the statute, rule, regulation, or order.
2. A record from this system may be disclosed to request information from a federal, state, or local agency maintaining civil, criminal, or other relevant information enforcement information or other pertinent information, such as licenses, if necessary to obtain information relevant to a Commission decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.
3. A record from this system may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit.
4. A record on an individual in this system of records may be disclosed to a Congressional office in response to an inquiry the individual has made to the Congressional office.
5. A record from this system of records may be disclosed to GAO and NARA for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall not be used to make a determination about individuals.
6. A record on an individual in this system of records may be disclosed, where pertinent, in any legal proceeding to which the Commission is a party before a court or administrative body.
7. A record from this system of records may be disclosed to the Department of Justice or in a proceeding before a court or adjudicative body when:
 - (a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and
 - (b) The Commission determines that the disclosure is relevant or necessary to the litigation.
8. A record in this system of records may be disclosed to the Office of Personnel Management in order for it to carry out its legally authorized Government-wide functions and duties.

9. The names, social security numbers, home addresses, dates of birth, dates of hire, quarterly earnings, employer identifying information, and State of hire of employees may be disclosed to the Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services for the purposes of locating individuals to establish paternity, establishing and modifying orders of child support, identifying sources of income, and for other child support enforcement actions as required by the Personal Responsibility and Work Opportunity Reconciliation Act (Welfare Reform Law, Pub. L 104-193).

In each of these cases, the FCC will determine whether disclosure of the record is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in an automated personnel and payroll system and in files in folders, cards, magnetic tapes, and loose leaf binders.

Retrievability:

Records are indexed by name and social security number.

Safeguards:

Records are maintained in filing cabinets in an office that is locked when not occupied by staff. Automated and manual records are available only to authorized personnel whose duties require access. Data resident on network servers are backed-up daily to magnetic media. One week's worth of back-up tapes is stored on-site in fireproof safes. Each week, the previous week's backup tapes are sent to an off-site storage location. A maximum of ten week's tapes are kept and cycled in this fashion.

Retention and Disposal:

Records are maintained for varying periods of time from one year to permanently in accordance with General Records Schedules issued by the National Archives and Records Administration. Disposal is by shredding.

System Manager(s) and Address(es):

Associate Managing Director, Human Resources Management, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B104, Washington, DC 20554, or the appropriate administrative office in which the individual is employed.

Notification Procedure:

Address inquiries to the system manager. It is necessary to furnish the following information in order to identify the individual whose records are requested: Full name; Date of Birth; Social Security Number; and Mailing address to which the reply should be mailed.

Record Access Procedures:

Address inquiries to the system manager. Requesters should reasonably specify the record contents being contested.

Contesting Record Procedures:

Address inquiries to the system manager. Requesters should reasonably specify the record contents being contested.

Record Source Categories:

Information is provided by management officials and by the individuals on whom the record is maintained.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-1

System Name:

Employee Locator System.

Security Classification:

This system of records has not been given a security classification.

System Location(s):

Human Resources Management (AMD-HRM), Room 1-A100, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554 and 1270 Fairfield Road, Gettysburg, Pennsylvania 17325.

Categories of Individuals Covered by the System:

Current employees of the Federal Communications Commission (FCC).

Categories of Records in the System:

- 1.The FCC employee's name, Bureau/Office, floor, room number, work and home telephone numbers; and
2. The name(s), e-mail address(es), and telephone number(s) of the individual(s) to contact in the event of a medical or other emergency involving the FCC employee.

Authority for Maintenance of the System:

44 U.S.C. 3101.

Purpose(s):

The records in this system serve:

1. To identify the individual(s) to contact, should an emergency of a medical or other nature involving the Commission occur while the employee is on the job; and

2. To allow the FCC to contact an employee at home, or other designated location, to notify him/her when an emergency requires that he/she report/not report for duty Initial collection and requested periodic updates of information in the system are voluntary.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

A record on an individual in this system of records may be disclosed to emergency medical personnel, i.e., doctors, nurses, and/or paramedics, or to law enforcement officials in case of a medical or other emergency involving the FCC employee.

In each of these cases, the FCC will determine whether disclosure of the record is compatible with the purpose for which the records were collected.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

The records are not disclosed to consumer reporting agencies.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

STORAGE:

Electronic records are maintained in a network computer database.

Retrievability:

Records are retrieved by the employee's name, Bureau/Office, floor, and room number.

Safeguards:

Electronic records are maintained in a network computer database, which is secured through controlled access and passwords restricted to the employee, Human Resources Management (AMD-HRM) employees, administrative personnel, and emergency relocation site employees.

Retention and Disposal:

Records are maintained as long as the individual is a current employee of the Federal Communications Commission. The FCC will submit a request for records disposition authority to the National Archives and Records Administration's (NARA). Upon approval by NARA, the FCC will publish an amendment of this system of records notice in the *Federal Register*. In the interim, when an employee leaves the Commission, the Human Resources Management activity (AMD-HRM) will request NARA's approval to electronically remove the employee's records from the database.

System Manager(s) and Address(es):

Human Resources Management (AMD-HRM), Room 1-A100, Federal Communications Commission's (FCC), 445 12th Street, SW., Washington, DC 20554 and 1270 Fairfield Road, Gettysburg, Pennsylvania 17325.

Notification Procedure:

FCC employees wishing to inquire whether this system contains information about them should contact the Human Resources Management (AMD-HRM), Room 1-A100, Federal Communications Commission (FCC), 445 12th Street,

SW., Washington, DC 20554 and 1270 Fairfield Road, Gettysburg, Pennsylvania 17325.

Individuals must supply their full name in order for records to be located and identified.

Record Access Procedures:

Same as above.

Contesting Record Procedures:

Same as above.

Record Source Categories:

Individual on whom the record is maintained.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-5

System Name:

Drug-Free Federal Workplace Program.

System Location(s):

Associate Managing Director--Administrative Operations, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

FCC employees who seek guidance and counseling through the agency Drug-Free Federal Workplace Program.

Categories of Records in the System:

This system includes information on an employee's personal history as it relates to his/her problem. The system also contains records on employees referred for counseling.

Authority for Maintenance of the System:

5 U.S.C.

Purpose(s):

Reference material for the use of the Program Administrator and Counselors.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Records in this system of records contain reference material(s) for the use of the Program Administrator and Counselors. In each case, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are stored in locked metal cabinets in the Program Administrator's Office.

Retrievability:

Records are filed and retrieved by name of the employee.

Safeguards:

Records are maintained in an office that is locked when not occupied by the Program Administrator. They are maintained in strict confidence and are accorded the same security and accessibility restrictions provided for medical records.

Retention and Disposal:

Records are kept indefinitely or until the employee leaves the FCC, at which time they are destroyed by shredding.

System Manager(s) and Address(es):

Associate Managing Director--Administrative Operations, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Employee, employee's supervisor, and counselors.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-6

System Name:

Personal Investigation Records.

Security Classification:

There is no specific security classification for this system; however, data or records within the system may have national defense/ foreign policy classifications up through secret.

System Location(s):

Security Operations Center, Assistant Managing Director- Administrative Offices (AMD-AO), Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Categories of Individuals Covered by the System:

1. Current and former FCC employees, applicants for employment in the Federal service, and contractors.
2. Individuals considered for access to classified information or restricted areas and/or security determinations such as contractors, experts, instructors, and consultants to Federal programs.
3. Individuals who are neither applicants nor employees of the Federal Government, but who are or were involved in Federal programs under a co-operative agreement.

Categories of Records in the System:

1. Data needed to identify an individual and his/her security clearance for both FCC and contract employees: Individual's last, first, and middle names (filed alphabetically by last name); Social Security Number; date of birth; place of birth; Bureau/Office/ Contractor Company; position title; security classification; types and dates of investigations; agency conducting investigation, investigation dates, clearance level granted, and position sensitivity level; and remarks.
2. Data needed to investigate an individual's character, conduct, and behavior in the community where he or she lives or lived; arrests and convictions for violations against the law; reports of interviews with present and former supervisors, co-workers, associates, educators, etc; reports about the individual's qualifications for a position; reports of inquiries with law enforcement agencies, employers, and educational institutions attended; reports of action after OPM or FBI Section 8(d) Full Field Investigation; Notices of Security Investigation and other information developed from the above described Certificates of Clearance; and in some instances, a photograph of the subject.
3. Data to needed to investigate allegations of misconduct by an FCC employee;
4. Data needed to investigate miscellaneous complaints not covered by the FCC's formal or informal grievance procedure; and
5. Data needed to conduct inquiries under the "President's Program to Eliminate Waste and Fraud in Government."

6. Data needed to investigate violence, threats, harassment, intimidation, or other inappropriate behavior that causes an FCC employee or contractor to fear for his/her personal safety in the FCC workplace: case number; victim's name; office telephone number; room number; organization bureau/office/division/branch; duty station; position; supervisor; supervisor's telephone number; location of incident; activity at time of incident; circumstances surrounding the incident; perpetrator; name(s) and telephone number(s) of witness(es); injured party(s); medical treatment(s); medical report; property damages; report(s) to police and/or Federal Protective Services; and other miscellaneous information.

Authority for Maintenance of the System:

5 CFR part 5; 29 CFR part 1960; 47 CFR 19.735-107; 5 U.S.C. 1303, 1304, 3301, 7902; and Executive Orders 10450, 11222, 12065, and 12196.

Purpose(s):

FCC Security Officer and the Personnel Security Specialist of the Security Office use the records in this system to provide investigative information to determine compliance with Federal regulations and/or to make a determination about an individual's suitability and fitness for Federal employment, access to classified information or restricted areas, position sensitivity, security clearances, evaluations of qualifications, and loyalty to the U.S.; to evaluate qualifications and suitability to perform contractual services for the U.S. Government; to document such determinations; to respond to an inquiry conducted under the President's Program to Eliminate Waste and Fraud in the Government; to take action on, or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees; and to counsel employees.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

1. A record from this system of records may be referred to the appropriate Federal, state, or local agency responsible for investigating or prosecuting a violation or for enforcing or implementing the statute, rule, regulation, or order where there is an indication of a violation or potential violation of a statute, regulation, rule, or order.
2. A record on an individual in this system of records may be disclosed to a Congressional office in response to an inquiry an individual has made to the Congressional office.
3. A record for this system of records maybe disclosed to GSA and NARA for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall not be used to make a determination about individuals.
4. A record on an individual in this system of records may be disclosed, where pertinent, in any legal proceeding to which the Commission is a party before a court or administrative body.
5. A record from this system may be disclosed to designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government, and the District of Columbia Government, in response to their request, when such agency, office, or establishment conducts an investigation of the individual for the purpose of hiring, firing, or retention, granting a security clearance, making a determination of qualifications, suitability, or loyalty to the United States Government, or access to classified information or restricted areas, or classifying jobs, letting of a contract, or issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's purpose.
6. A record from this system of records may be disclosed to the Department of Justice or in a proceeding before a court or adjudicatory body when:
 - (a) The United States, the Commission, a component of the Commission, or when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Commission determines that the disclosure is relevant or necessary to the litigation.

7. A record from this system may be disclosed to the security officers of an agency in the executive, legislative, or judicial branch, or the District of Columbia Government, in response to their request(s) for verification of security clearances of FCC employees to have access to classified data or areas where their official duties require such access.

8. A record in this system may be disclosed to request information from a Federal, state, or local agency maintaining civil, criminal, or other relevant or pertinent enforcement information or records, such as licenses, if necessary to obtain information relevant to a Commission decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a grant or other benefit.

9. A record from this system may be disclosed to the Merit System Protection Board (MSPB) during the course of the MSPB's investigation of the individual's appeal, following the Commission's adverse action against the individual.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not applicable.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

STORAGE:

Records in this system of records include both paper and electronic records. Paper records are stored in file folders in security containers. The electronic records are maintained in a computer database.

Retrievability:

Records are retrieved by individual's name and Social Security Number.

Safeguards:

Paper records are maintained in file folders and stored in approved security containers, within a secure, access-controlled area with an intrusion alarm. Access is limited to approved security office and administrative personnel.

The electronic records are maintained in a "stand-alone" computer database, which is secured through controlled access and passwords restricted to security and administrative personnel on a "need to know" basis. The computers are located in a room with a simplex lock and intrusive alarm systems. The computer databases are maintained on a computer that is not connected to the FCC computer network. The databases are backed-up on a daily basis to floppy disk(s), which are then stored in a secured area.

Retention and Disposal:

Both paper and electronic records are retained during employment or while an individual is actively involved in federal programs. As appropriate, records are returned to investigating agencies after employment terminates; otherwise, the records are retained for five years from the date that the employee leaves the Commission.

Investigative files and the computer database, which show the completion of an investigation, are retained for 15 years, except for investigations involving potential actionable issue(s), which will be maintained for 25 years plus the current year from the date of the most recent investigative activity.

Paper records are destroyed by shredding. Electronic records are destroyed by electronic erasure.

System Manager(s) and Address(es):

Security Office, Associate Managing Director--Administrative Operations (AMD-AO), Security Operations Center, Federal Communications Commission (FCC), 445 12th Street, S.W., Room 1-B458, Washington, DC 20554.

Record Access Procedures:

This system is exempt from the requirement that the agency publish the procedures for notifying an individual, at his or her request, if the system contains a record pertaining to him/her, for gaining access to such record, and for contesting the contents of the record.

Record Source Categories:

This system is exempt from the requirement that the agency publish the categories of sources of records in this system.

Exemptions Claimed for the System:

This system of records is exempt from sections (c)(3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act.
2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act.
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

[\[Return to TOP\]](#)

FCC /Central-7

System Name:

Freedom of Information Act (FOIA) Case Files.

System Location(s):

FOIA Office, Federal Communications Commission (FCC), 445 12th Street, SW, Washington, DC.

Categories of Individuals Covered by the System:

Individuals or organizations requesting access to inspect and/or copy records of the Commission under provisions of the FOIA.

Categories of Records in the System:

Name, address, and other information about the requester and the records sought.

Authority for Maintenance of the System:

Freedom of Information Act (1994 and Supp. II 1996), 5 U.S.C. 552.

Purpose(s):

Records are available to FOIA staff involved in correspondence and investigative processes, including appeals officials and members of the FCC General Counsel staff.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

1. In the event the Commission deems it desirable or necessary, in determining whether particular records are required to be disclosed under the FOIA, disclosure may be made to the Department of Justice for the purpose of obtaining its advice.
2. Where the appropriate official of the Commission, pursuant to the Commission's FOIA Regulation determines that it is in the public interest to disclose a record which is otherwise exempt from mandatory disclosure, disclosure may be made from the system of records.
3. The Commission contracts with a private firm for the purpose of searching, duplicating, and distributing to the public the documents maintained by the Commission and available for inspection under the Act. The contractor is required to maintain Privacy Act safeguards on such records.
4. A record on an individual in this system may be disclosed to a Congressional office in response to an inquiry the individual has made to the Congressional office.
5. In the event of litigation where the defendant is:
 - (a) The Commission, or any employee of the Commission in his or her official capacity;
 - (b) The United States where the Commission determines that the claim, if successful, is likely to directly the Commission's operations; or
 - (c) Any Commission employee in his or her individual capacity where the Justice Department has agreed to represent such employee, the Commission may disclose such records as it deems desirable or necessary to the Department of Justice to enable that Department to present an effective defense.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

STORAGE:

Paper records maintained in case files (original or copy of incoming request and written response). Electronic records are maintained in an electronic database.

Retrievability:

Records are indexed by FOIA control number of individual requester.

Safeguards:

Paper records are maintained in locked file cabinets in the office of FOIA officer, with limited access. Electronic records are secured through controlled access and passwords to restricted office personnel. Data resident on network servers are backed-up daily to magnetic media. One week's worth of back-up tapes is stored on-site in fireproof safes. Each week, the previous week's backup tapes are sent to an off-site storage location. A maximum of ten week's tapes are kept and cycled in this fashion.

Retention and Disposal:

Individual case files are maintained for two years after the date of reply. Denied requests and appeals of denials may be retained for longer periods (up to six years after final action) in accordance with FOIA and FCC records control schedules.

System Manager(s) and Address(es):

FOIA Officer, Federal Communications Commission (FCC), 445 12th Street, SW, Washington, DC 20554.

Notification Procedure:

Address inquiries to the FOIA Officer.

Record Access Procedures:

Address inquiries to the FOIA Officer.

Contesting Record Procedures:

Address inquiries to the FOIA Officer.

Record Source Categories:

Individuals and organizations making requests under FOIA or from bureaus or offices of the Commission reporting on the handling of such requests for inclusion in the annual report to Congress.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-8

System Name:

Telephone Call Detail and Equipment Loan Records.

System Location(s):

Office of the Managing Director, Information Technology Center, Operations Group, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C361, Washington, DC 20554.

Categories of Individuals Covered by the System:

1. This system of records contains information concerning the following actions:
 - (a) Individuals originating calls from FCC telephones and individuals receiving such calls;
 - (b) Individuals placing calls to or charging calls to FCC telephones (including cellular telephones);
 - (c) Individuals receiving such calls, or accepting the charges; and
 - (d) Individuals who are loaned electronic equipment to use when their work requires them to work outside the office or to maintain close contact with the Commission staff, *i.e.*, laptops, pagers and cellular telephones.
2. The primary record subjects are current and former FCC employees, as well as individuals employed under any employment arrangement such as a contract or cooperative agreement; grantees; or other persons performing on behalf of the FCC.
3. Incidental to the coverage of the primary record subjects are non-employees who may be identified by telephone number during an inquiry or investigation relating to a potential improper or unofficial use of Government telephones or other illegal or improper activity by the primary record subject.

Categories of Records in the System:

1. Records in the system of records related to telephone calls placed to and from FCC phones, and the assignment of telephone numbers to employees and the location of the telephone in the FCC. Since this system includes cellular telephones, any local call to or from a cellular telephone would be included.
2. The records may include such information as the number called from, the number called, time and date of the call, duration, disposition, and the cost of the call and/or charges accepted, and the FCC component to which the relevant telephone numbers are assigned.
3. The system may also include copies of related records, *e.g.*, any periodic summaries which may have been compiled to reflect the total number of long distance calls.
4. The database(s) from which telephone numbers are retrieved contains the names of employees and their office locations, but no other personal identifiers such as social security numbers.
5. The CD-ROM files contain the agency telephone bills which provide details on all calls to and from the FCC telephones.
6. The paper files consist of a combination of the database and CD-ROM files.
7. Records in this system also include records of electronic equipment loaned to staff to use when their work requires them to work outside the office or to maintain close contact with the Commission staff, *i.e.*, laptops, cellular telephones, and pagers.
8. These records would contain the following information:
 - (a) Individual's name, FCC I.D. badge number, and Bureau/Office;
 - (b) Loaned equipment's barcode number; serial number; model number; and modem number.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Authority for Maintenance of the System:

1. 44 U.S.C. 3101, which authorizes agencies to create and preserve records documenting agency organizations, functions, procedures, and transactions;
2. 31 U.S.C. 1348b., which authorizes the use of appropriated funds to pay for long distance calls only if required for official business or necessary in the interests of the Government;
3. 47 U.S.C. 154(I), which authorizes the FCC to take actions necessary to execute its functions;
4. 5 CFR 2635.704a., which prohibits use of Government property for other than authorized purposes; and
5. 41 CFR 201-21.601 and 201-21.602, which require that the Government telecommunications systems be used for official purposes only, and authorizing agencies to collect for unauthorized calls.

Purpose(s):

1. This system of records is used to keep track of local and long-distance telephone calls placed to and from FCC phones, including cellular telephones and the records of the equipment loaned out and those who have borrowed it.
2. The telephone records may include such information as the number called from, the number called, time and date of the call, duration, disposition, the cost of the call and/or charges accepted, and the FCC component to which the relevant telephone numbers are assigned. By maintaining these records, the FCC can monitor the charges for long distance or cellular calls and also determine if such calls are being made for other than Commission-related purposes.
3. When wireless instruments are loaned, the individual staff must sign the FCC Wireless Telecommunications Statement of Understanding and fill out FCC Form A-476, Custodial Receipt for Sensitive FCC Property when the equipment loan is made.
4. The equipment loan records include the type of equipment borrowed, the borrower, and the duration of the loan.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

The FCC does not normally disclose records from this system of records. However, in the event it is appropriate, disclosure of relevant information may be made in accordance with the provisions of 5 U.S.C. 552(a)(b). Records and data may be disclosed as necessary pursuant to 5 U.S.C. 552(a)(b):

1. A record in this system of records may be disclosed to a member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained;
2. A record in this system of records may be disclosed to representatives of the General Services Administration or the National Archives and Records Administration who are conducting records management inspections under the authority of 44 U.S.C. 2904 and 2906;
3. A record in this system of records may be disclosed to the Department of Justice (DOJ) when:
 - (a) The agency or any component thereof; or any employee of the agency in his or her official capacity where the DOJ has agreed to represent the employee; or

(b) The United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

4. A record in this system of records may be disclosed to a court or adjudicative body in a proceeding when:

(a) The agency or any component thereof; any employee of the agency in his or her official capacity; or any employee of the agency in his or her official capacity where the agency has agreed to represent the employee; or

(b) The United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

5. A record in this system of records may be disclosed to law enforcement agencies when a record on its fact, or in conjunction with other records, indicates a violation or potential violation of the law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, state, local, or tribal, or other public authority responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prospective responsibility of the receiving entity;

6. A record in this system of records may be disclosed to agency contractors, grantees, experts, consultants, or volunteers who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a (m);

7. A record in this system of records may be disclosed to the National Finance Center (the FCC's designated payroll office), the Department of the Treasury Debt Management Services and/or a current employer to effect a salary, IRS tax refund, or administrative offset to satisfy an indebtedness incurred for unofficial telephone and cellular calls; and to Federal agencies to identify and locate former employees for the purposes of collecting such indebtedness, including through administrative, salary, or tax refund offsets. Identifying and locating former employees, and the subsequent referral to such agencies for offset purposes, may be accomplished through authorized computer matching programs. Disclosures will be made only when all procedural steps established by the Debt Collection Act of 1982 and the Debt Collection Improvement Act of 1996 or the Computer Matching and Privacy Protection Act of 1988 as appropriate, have been taken;

8. A record in this system of records may be disclosed to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit; and

9. A record in this system of records may be disclosed to a Federal, State, local, foreign, or tribal or other information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained electronically in one of three databases (PCS, cellular telephones, and pagers), on paper, and on CD-ROM. The databases are password protected and updated daily. Authorized individuals can check the current databases during sign out when individuals leave the FCC to ensure that the departing staff has returned any loaned equipment.

Retrievability:

Telephone call records are retrieved by bureau or office name, the employee name, name of recipient of telephone call, telephone number. Equipment loan records are retrieved by the employee name, equipment barcode number, serial number, and model or modem numbers.

Safeguards:

Paper and CD-ROM records are maintained in file cabinets in offices which are locked at the end of the business day. Information in the database is secured through controlled access and passwords restricted to administrative office personnel. Data resident on network servers are backed-up daily to magnetic media. One week's worth of back-up tapes is stored on-site in fireproof safes. Each week, the previous week's backup tapes are sent to an off-site storage location. A maximum of ten week's tapes are kept and cycled in this fashion.

Retention and Disposal:

Records are disposed of in accordance with General Records Schedule 12, National Archives and Records Administration.

System Manager(s) and Address(es):

Appropriate bureau or office chief and first line supervisors in the Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554. See FCC telephone directory for a list of field office telephone numbers or the commercial telephone directory under "U.S. Government."

Notification Procedure:

Ask for "Records Access Procedures" in making inquiries regarding this system. The inquiries should be addressed to the system manager, Office of Managing Director, Information Technology Center, Operations Group, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Telephone assignment records; call detail listings; results of administrative inquiries relating to assignment of responsibility for placement of specific long distance calls.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-9

System Name:

Denial of Federal Benefits (Drug Debarment List).

System Location(s):

Financial Operations Center, Associate Managing Director--Financial Operations (AMD-FO), Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A663, Washington, DC 20554.

Categories of Individuals Covered by the System:

Individuals convicted of offenses concerning the distribution or possession of controlled substances, who have been denied all Federal benefits or FCC benefits as part of their sentence pursuant to Section 5301 of the Anti-Drug Abuse Act of 1988, and who have also filed applications for any FCC professional or commercial license.

Categories of Records in the System:

The records within this system will consist of a database provided to the FCC from the Department of Justice (DOJ) regarding individuals who have been denied all Federal benefits or FCC benefits pursuant to section 5301 of the Anti-Drug Abuse Act of 1988.

1. The data elements to be used by the FCC are: DOJ identification number (ID) for the person denied Federal benefits, Person's name, Taxpayer Identification Number (TIN), and Starting and ending date of the denial of Federal benefits.
2. All other data elements in the database will be immediately discarded.
3. When there is a match of name and TIN from the database with the name and address of an application on file with the FCC, the FCC will then obtain from DOJ additional data elements: Person's name, address, and zip code. If also required by the FCC application, the person's date of birth.
4. If manual comparison of the application information with the information obtained from DOJ confirms a match, the FCC will prepare a confirmation report to be attached to the application. The confirmation report will reflect the identifying information obtained from the DOJ debarment entry, but it will not include the DOJ ID number for that debarment entry. Upon such a match, the FCC will initiate correspondence with the applicant, which will also be associated with the application. The confirmation report and any correspondence with the applicant will be among the records found in this system.

Authority for Maintenance of the System:

Section 5301 of the Anti-Drug Abuse Act of 1988, Pub. L. 100-690, as amended by section 1002(d) of the Crime

Control Act of 1990, Pub. L. 101-647 (21 U.S.C. 862), and sections 4(i) and 4(j) of the Communications Act of 1934 (47 U.S.C. 154(i) and 154(j)).

Purpose(s):

The records within the system will be used for the exchange of information between DOJ and the FCC in connection with the implementation of section 5301 of the Anti-Drug Abuse Act of 1988. This exchange of information permits the FCC to perform the General Services Administration (GSA) Debarment List check as provided for in the Office of National Drug Control Policy plan for implementation of section 5301 through use of information generated by DOJ. The automated records obtained from DOJ will only be used by the FCC to make an initial determination of whether an individual applicant is subject to a denial of all Federal benefits or FCC benefits imposed under section 5301 of the Anti-Drug Abuse Act of 1988.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

This system contains the following information: Department of Justice database provided to the FCC; the database retained by the FCC for use in the automated system; and the match reports; and any copies of the confirmation report that include the Department of Justice ID number will be routinely available for use or inspection by appropriate FCC officials.

The confirmation report (not including the DOJ ID Number) and any correspondence with the applicant will be associated with the applicant's application and will thus be made routinely available for public inspection.

In each case the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained electronically on a computer database.

Retrievability:

Records are retrieved by supplying the following information: Name of applicant, TIN, address (in some instances) and zip code, date of birth (in some instances), and FCC fee control number for the application.

Safeguards:

The data are provided to the FCC by the U.S. Department of Justice (DOJ) and will be protected from tampering, unauthorized disclosure, and will follow these procedures:

1. The database will be processed to extract the information to be used in the automated system, and the data elements not being used in the automated system will be electronically erased. The remaining data will be maintained at the main FCC building with a low risk of unauthorized access.
2. Access points are photo-monitored by security personnel; all employees are required to display photo ID badges; and all visitors must register and wear a visitor's badge. Access to the computer system on which the extracted database is stored requires use of a unique user ID with personal identifier, which is controlled through application and operating system security.

3. The extracted database is stored in a separate file in that system, and a separate password is required for entry to that file. The password is available to a limited number of persons based strictly on a "need to know" basis.

4. The reports of any automated matches containing the DOJ ID number will be made available only to the appropriate FCC officials.

Retention and Disposal:

1. The match reports will be retained by the FCC for only as long as it is necessary to obtain the debarment entry information and corresponding application for manual confirmation of the match. Thereafter, they will be destroyed. However, periodically, a match report will be randomly retained for a period of an additional 90 to 120 days to provide a quality check of the verification process.

2. Where the verification process establish that a match does not indicate that the applicant has been denied Federal benefits under section 5301, the debarment entry information used in that determination will be retained by the FCC for 30 days after the application has cleared the debarment check. However, as noted above, debarment entry information relating to match reports that are retained for quality control purposes will be retained until that quality check is completed.

3. Where a match is confirmed by the manual verification process, the debarment entry information will be retained for a period of at least 90 days after the date of the letter referred to above. If the application contests the determination that a section 5301 denial of Federal benefits bars a grant of the application, the debarment entry information will be retained until such time as the FCC's action on the application is no longer subject to review in any court.

System Manager(s) and Address(es):

Associate Managing Director-Financial Operations (AMD-FO), Managing Director, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the AMD-FO.

Record Access Procedures:

Address inquiries to the AMD-FO.

Contesting Record Procedures:

Address inquiries to the AMD-FO.

Record Source Categories:

Individuals making applications who have been convicted of certain drug offenses and who have been denied all Federal benefits or FCC benefits as part of their sentence.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-10

System Name:

Access Control System.

System Location(s):

Office of the Managing Director, Security Operations Center, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Categories of Individuals Covered by the System:

Current FCC employees, current contractors, frequent visitors, visitors, temporary hires, special parking access and day contractor.

Categories of Records in the System:

The system consists of computer databases, with all records containing the last and first name, filed alphabetically by last name, with a corresponding Badge Number.

1. The FCC employee/temporary hire database will include: First and last name, Telephone number, Bureau/Office, (Supervisor--delete), Room number, Date of issuance, and Parking (permit--delete) privilege (number--delete), if applicable, and property pass privilege if applicable.
2. The contractor database will include: First and last name, Contractor company name, Telephone number, FCC point of contact, Telephone number, and Date of issuance.
3. The Frequent Visitor's database will include: First and last name, Employer's name, Address, Telephone number, Point of contact at the employer, and Date of issuance.
4. The Visitor/day contractor database will include: First and last name along with numerical identifier.
5. The Special Parking Access database will include: First and last name, Telephone number, Employer, and Date of issuance.

Note: Proof of identity required through photographic identification is necessary prior to issuance of the contractor badge and the frequent visitor's badge and visitor's badge.

Authority for Maintenance of the System:

Presidential Directive based on Department of Justice report entitled "Vulnerability Assessment of Federal Facilities."

Purpose(s):

This system provides a method by which the FCC can control and account for all persons entering the Commission's facilities and by which the FCC may ascertain the times persons were in these facilities.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

1. Where there is an indication of a violation or potential of a statute, regulation, rule, or order, records from this system

may be referred to the appropriate Federal, state, or local agency responsible for investigating or prosecuting a violation or for enforcing or implementing the statute, rule, regulation, or order.

2. A record from this system may be disclosed to a request for information from a Federal, state, or local agency maintaining civil, criminal, or other relevant information or other pertinent information if necessary to obtain information relevant to an investigation.
3. A record on an individual in this system of records may be disclosed to a Congressional office in response to an inquiry the individual has made to the Congressional office.
4. A record from this system of records may be disclosed to GSA and NARA for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall not be used to make a determination about individuals.
5. Records from this system may be disclosed to FCC supervisors or management representatives to ascertain (either confirm or refute) the times employees were in the facility.

In each of these cases the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Records are maintained in a password protected computer database.

Retrievability:

Records are retrieved by the name of the individual on whom they are maintained by a limited number of authorized individuals.

Safeguards:

The computer terminals are stored within a secured area. The Security Office staff performs a backup operation on these files on a weekly--monthly basis on 1/4 data cartridge, which are stored/safeguarded in the Security Office.

Retention and Disposal:

1. When an employee/contractor/temporary hire/special parking access leaves the FCC, the file in the database is deleted.
2. Frequent visitor badges are given a two-year valid period, after which the card will automatically deactivate.
3. All returned visitor/day contractor cards will be reused on a daily basis.
4. Transaction data for all cards will be placed on backup discs and stored for one year in the FCC Security Office which is locked and alarmed.

System Manager(s) and Address(es):

Security Operations Center, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Notification Procedure:

Individuals wishing to inquire whether this system of records contains information about them should contact the system manager indicated above. Individuals must furnish their "Full Name" for their records to be located and identified.

Record Access Procedures:

Individuals wishing to request access to records about them should contact the system manager indicated above. Individuals must furnish their "Full Name" for their record to be located and identified. An individual requesting access must also follow FCC Privacy Act regulations regarding verification of identify and access to records. See 47 CFR 0.554-0.555.

Contesting Record Procedures:

Individuals wishing to request amendment of their records should contact the system manager indicated above. Individuals must furnish their "Full Name" for their record to be located and identified. An individual requesting amendment must also follow the FCC Privacy Act regulations regarding verification of identity and amendment of records. See 47 CFR 0.556-0.557.

Record Source Categories:

The individual to whom the information applies.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /Central-11

System Name:

Inter-office (GroupWise) and Internet E-mail Systems.

System Location(s):

Information Technology Center, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C266, Washington, DC 20554.

Categories of Individuals Covered by the System:

Employees and contractors of the Federal Communications Commission in Washington, DC and the field offices.

Categories of Records in the System:

Records in this system of records include the names, e-mail addresses, and passwords of all FCC employees and contractors.

Authority for Maintenance of the System:

1. Executive Orders 10450 and 12065;
2. 44 U.S.C. 3101, which authorizes agencies to create and preserve records documenting agency organizations, functions, procedures, and transactions;
3. 47 U.S.C. 154(i), which authorizes the FCC to take actions necessary to execute its functions;
4. 5 CFR 2635.704a., which prohibits use of Government property for other than authorized purposes; and
5. 41 CFR 201-21.601 and 201-21.602, which require that the Government Radio systems be used for official purposes only.

Purpose(s):

These records are maintained by the Information Technology Center staff to identify all users on the FCC's Inter-office and Internet E-mail systems, their locations, and their passwords. This information is necessary to insure that all users abide by the FCC's Intranet and Internet regulations and to identify possible abusers.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information in this system of records may be disclosed for the following reasons:

1. For disclosure to a Federal agency or the District of Columbia Government, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency.
2. For disclosure to the security officer of an agency in the executive, legislative, or judicial branch, or the District of Columbia Government, in response to its request for verification of security clearances, of FCC employees/contractors to have access to classified data or areas where their official duties require such access.
3. Where there is an indication or a violation or potential violation of a statute, regulation, rule, order may be referred to the appropriate Federal, state, or local agency responsible for investigating or prosecuting a violation or for enforcing or implementing the statute, rule, regulation or order.
4. A record from this system may be disclosure to request information from a Federal, state, local or foreign agency maintaining civil, criminal, or other relevant enforcement information, or other pertinent information records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance of a grant or other benefit.
5. A record on an individual in this system of records may be disclosed to a Congressional office in response to an inquiry the individual has made to a Congressional office.
6. A record from this system of records may be disclosed to GSA and NARA for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall not be used to make a determination about individuals.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in

the System:

Records are maintained in an electronic database.

Retrievability:

Records are retrieved by bureau or office name and the employee name and log-in name.

Safeguards:

Information in the database is secured through controlled access and passwords restricted to administrative office personnel. Data resident on network servers are backed-up daily to magnetic media. One week's worth of back-up tapes is stored on-site in fireproof safes. Each week, the previous week's backup tapes are sent to an off-site storage location. A maximum of ten week's tapes are kept and cycled in this fashion.

Retention and Disposal:

Records are until the employee or contract retires or leaves the FCC. The records are then disposed of in accordance with General Records Schedule 12, National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Operations Group, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C734, Washington, DC 20554.

Notification Procedure:

Ask for "Records Access Procedures" in making inquiries regarding this system. The inquiries should be addressed to the system manager, Office of Managing Director, Information Technology Center, Operations Group, Federal Communications Commission (FCC), 445 12th Street, SW., 1-C266, Washington, DC 20554.

Record Access Procedures:

Same as above.

Contesting Record Procedures:

Same as above.

Record Source Categories:

Same as above.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

System Name:

Garnishment and Levy of Wages.

System Location(s):

Associate Managing Director, Human Resources Management, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B104, Washington, DC 20554.

Categories of Individuals Covered by the System:

Any Commission employee who is the subject of a garnishment or levy order issued by a court of competent jurisdiction or by another government entity authorized to issue such order.

Categories of Records in the System:

Garnishment of levy orders served upon the agency for implementation, correspondence, memoranda.

Authority for Maintenance of the System:

5 U.S.C. 301.

Purpose(s):

Records are used by staff attorneys in the General Counsel's office in directing the agency's implementation of garnishment and levy orders.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

1. Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be referred to the appropriate Federal, state, or local agency responsible for investigating or prosecuting a violation or for enforcing or implementing the statute, rule regulation, or order.
2. A record on an individual in this system or records may be disclosed, where pertinent, in any legal proceeding to which the Commission is a party before a court or administrative body.
3. A record from this system of records may be disclosed to the Department of Justice or in a proceeding before a court or adjudicative body when:
 - (a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and
 - (b) The Commission determines that the disclosure is relevant or necessary to the litigation.
4. A record in this system of records which concerns information on pay and leave, benefits, retirement deductions, and any other pertinent information may be disclosed to the Office of Personnel Management in order for it to carry out its legally authorized Government-wide functions and duties.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Paper records are stored in file folders.

Retrievability:

Records are maintained by the name of the individual subject to garnishment or levy order.

Safeguards:

Records are kept in file cabinets in offices that are secured at the end of each business day. Because only one or two office persons have need to routinely access this system, unauthorized examinations would be easily detected.

Retention and Disposal:

Records are normally retained as long as the Commission remains under the obligation to implement the particular garnishment or levy order.

System Manager(s) and Address(es):

Associate Managing Director, Human Resources Management, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW Room 1-B104, Washington, DC. 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Bankruptcy courts, state domestic relations courts, state public health and welfare departments or agencies, Internal Revenue Service, and intra-agency memoranda.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

System Name:

Informal Complaints, Inquiries, and Requests for Dispute Assistance.

Security Classification:

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

System Location(s):

Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554 and 1270 Fairfield Road, Gettysburg, PA 17325.

Categories of Individuals Covered by the System:

The categories of individuals in this system include individuals, groups, and other entities who make or have made informal complaints, inquiries, or requests for dispute assistance on matters arising under the Communications Act of 1934, as amended, and the Rehabilitation Act.

Categories of Records in the System:

The categories of records in this system include both computerized information contained in a database and paper copies of inquiries, requests for dispute assistance, informal complaints, and related supporting information made by individuals, groups, or other entities; and company replies to complaints, requests, inquiries, and Commission letters regarding such complaints, requests, and inquiries.

The categories of records may also include submissions that individuals, groups, or other entities make, including, but not limited to, submissions made by letter, fax, telephone, e-mail, and via the FCC web portal at www.fcc.gov.

Authority for Maintenance of the System:

Sections 1, 4, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507, 710, 713, 716, 717, and 718 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507, 610, 613, 617, 618, and 619; Sections 504 and 508 of the Rehabilitation Act, 29 U.S.C. 794 and 794d; and 47 CFR 0.111, 0.141, 1.711 et seq., 14.30 et seq., 20.19, 64.604, 68.414 et seq., and 79.1 et seq.

Purpose(s):

The records in this system are used by Commission personnel to handle and process informal complaints, inquiries, and requests for dispute assistance received from individuals, groups, and other entities. Records in this system are available for public inspection after redaction of information that could identify the complainant or correspondent, such as the complainant's name, address, telephone number, fax number, and/or e-mail address.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Informal Complaints – When a record in this system involves an informal complaint filed against telecommunications providers, broadcasters, multi-channel video program distributors, voice-over-internet-protocol providers, and/or

wireless providers, the complaint may be forwarded to the subject company for a response, pursuant to Sections 4(i), 208, and 303(r) of the Communications Act of 1934, as amended.

2. **Informal Complaints, Inquiries, and Requests for Dispute Assistance about Accessibility for Individuals with Disabilities** – When a record in this system involves an informal complaint, inquiry, or request for dispute assistance involving or filed against a company (including telecommunications and advanced communications service providers and equipment manufacturers; video programming owners, providers, and distributors, including broadcasters and multichannel video programming distributors; and manufacturers of apparatus used to receive, play back, or record video programming) about accessibility for individuals with disabilities, the inquiry, request, or informal complaint may be forwarded to the subject company for a response, pursuant to Section 4(i), 208, and 303(r) of the Communications Act of 1934, as amended.

3. **FCC Enforcement Actions** – When an order or other Commission-issued document that includes consideration of informal complaints filed against telecommunications providers, broadcasters, multi-channel video program distributors, voice-over-internet-protocol providers, and/or wireless providers is entered by the FCC to implement or enforce the Communications Act, pertinent rule, regulation, or order of the FCC, the complainant’s name may be made public in that order or document. When an order or other Commission-issued document that includes consideration of an informal complaint about accessibility for individuals with disabilities filed against a company (including telecommunications and advanced communications service providers and equipment manufacturers; video programming owners, providers, and distributors, including broadcasters and multichannel video programming distributors; and manufacturers of apparatus used to receive, play back, or record video programming) is entered or released by the FCC to implement or enforce the Communications Act, pertinent rule, regulation, or order of the FCC, the complainant’s name may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests confidentiality of his or her name from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission’s ability to investigate and/or resolve the complaint.

4. **Law Enforcement and Investigation** – Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be referred to the appropriate Federal, state, Tribal, or local agency either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency.

5. **Adjudication and Litigation** – Where by careful review, the Commission determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the Commission to be for a purpose that is compatible with the purpose for which the Commission collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) the Commission or any component thereof; or (b) any employee of the Commission in his or her official capacity; or (c) any employee of the Commission in his or her individual capacity where the Commission has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation.

6. **Department of Justice** – A record from this system of records may be disclosed to the Department of Justice or in a proceeding before a court or adjudicative body when:

(a) the United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) the Commission determines that the disclosure is relevant or necessary to the litigation.

7. **Congressional Inquiries** – When requested by a congressional office in response to an inquiry by an individual made to the congressional office for the individual’s own records.

8. **Government-wide Program Management and Oversight** – When requested by the General Services Administration (GSA), the National Archives and Records Administration (NARA), and/or the Government Accountability Office (GAO) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906 (such disclosure(s) shall not be used to make a determination about individuals); when the Department of Justice (DOJ) is

contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

9. Breach of Federal Data – A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The Consumer and Governmental Affairs Bureau staff logs consumer informal complaints, inquiries, and requests for dispute assistance that it receives into its Complaint and Inquiry Management System (CIMS), Consolidated Complaint Management System (CCMS), and other electronic databases and network databases not specifically named here that are used to store consumer informal complaints and inquiries, including requests for dispute assistance. Each request for dispute assistance and informal complaint submission is automatically assigned a file identification number for future reference when the case is entered into one of the databases. This identification number tracks consumer submissions and assists with identification of duplicate filings, which occur when consumers file multiple submissions. Confidential paper submissions are moved to a locked storage room for safekeeping.

All records are kept in accordance with the agency records control schedule approved by NARA.

Retrievability:

Information in this system, including, but not limited to records, files, and data, may be retrieved by the individual's personal identifiers (such as the complainant's name, address, telephone number, fax number, and/or e-mail address), entity name, program name, date received and date closed, problem description field, and/or call sign.

Safeguards:

Electronic records that emanate from these informal complaint, inquiry submissions, and requests for dispute assistance are maintained in CIMS, CCMS, or other electronic and network computer databases not specifically named here, which are secured through controlled access and passwords restricted to a limited number of FCC employees or contractors working on informal complaints, inquiries, and requests for dispute assistance. These various safeguards comply with the FCC's IT security and privacy protocols. In addition, as an added security measure, the staff in the Consumer and Governmental Affairs Bureau, Enforcement Bureau, and other FCC bureaus and offices who are assigned responsibility for resolution of these records in CIMS are only allowed access to these records via a "license" that also tracks their use of the records. Confidential paper submissions are moved to a locked storage room for safekeeping.

Retention and Disposal:

The information in this system is limited to electronic data, paper files, and audio files, such as telephone call records. The information is retained at the FCC and then destroyed in accordance with the agency records control schedule N1-173-07-1, approved by the National Archives and Records Administration (NARA), which generally requires that source records are destroyed three years after data are entered into the system, and records in the master file are destroyed three years after the case is closed.

System Manager(s) and Address(es):

Address inquiries to the Privacy Analyst, Office of Managing Director or Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.

Notification Procedure:

Address inquiries to the Privacy Analyst, Office of Managing Director or Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.

Record Access Procedures:

Address inquiries to the Privacy Analyst, Office of Managing Director or Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.

An individual requesting access must follow FCC Privacy Act regulations regarding verification of identity and amendment of records. See 47 CFR 0.554-0.557.

Contesting Record Procedures:

Address inquiries to the Privacy Analyst, Office of Managing Director or Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.

Record Source Categories:

The sources for the information in this system include the complainants and subject entities.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /CGB-1

System Name:

Informal Complaints and Inquiries.

Security Classification:

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

System Location(s):

Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554 and 1270 Fairfield Road, Gettysburg, PA 17325.

Categories of Individuals Covered by the System:

The categories of individuals in this system include individuals, groups, and other entities who make or have made informal complaints or inquiries in any format, including, but not limited to, paper, telephone, and electronic submissions, including e-mail, Internet, and fax, etc., on matters arising under the Communications Act of 1934, as amended, and the Rehabilitation Act.

Categories of Records in the System:

The categories of records in this system include both computerized information contained in a database and paper copies of inquiries, informal complaints, and related supporting information made by individuals, groups, or other entities; and company replies to complaints, inquiries, and Commission letters regarding such complaints and inquiries.

The categories of records may also include submissions that individuals make using fax, voice (telephone calls), Internet e-mail, etc., and via the FCC Web portal at: <http://www.fcc.gov>.

Authority for Maintenance of the System:

Sections 151, 154, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507; Sections 504 and 508 of the Rehabilitation Act, 29 U.S.C. 794; and 47 CFR 1.711 *et seq.*, 6.15 *et seq.*, 7.15 *et seq.*, and 64.604.

Purpose(s):

The records in this system are used by Commission personnel to handle and process informal complaints received from individuals, groups, and other entities. Records in this system are available for public inspection after redaction of information that could identify the complainant or correspondent, such as the complainant's name, address, telephone number, fax number, and/or e-mail address.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. When a record in this system involves an informal complaint filed against telecommunications providers, broadcasters, multi-channel video program distributors, voice-over-Internet-protocol providers, and/or wireless providers, the complaint may be forwarded to the subject company for a response, pursuant to Sections 4(i), 208, and 303(r) of the Communications Act of 1934, as amended.
2. When an order or other Commission-issued document that includes consideration of informal complaints filed against telecommunications providers, broadcasters, multi-channel video program distributors, voice-over-Internet-protocol providers, and/or wireless providers is entered by the FCC to implement or enforce the Communications Act, pertinent rule, regulation, or order of the FCC, the complainant's name may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests that the bureau withhold his or her name from public disclosure, such a request will be granted and the complainant's name will not be disclosed in the Commission-issued order or document.

3. Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be referred to the appropriate Federal, State, Tribal, or local agency responsible for investigating or prosecuting a violation or for implementing or enforcing the statute, rule, regulation, or order.

4. A record on an individual in this system of records may be disclosed, where pertinent, in any legal proceeding to which the Commission is a party before a court or administrative body.

5. A record from this system of records may be disclosed to the Department of Justice or in a proceeding before a court or adjudicative body when:

(a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Commission determines that the disclosure is relevant or necessary to the litigation.

6. A record on an individual in this system of records may be disclosed to a Congressional office in response to an inquiry the individual has made to the Congressional office.

7. A record from this system of records may be disclosed to the Government Accountability Office (GAO) and the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall not be used to make a determination about individuals.

8. A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The Consumer and Governmental Affairs Bureau staff logs consumer informal complaints and inquiries that it receives into its Complaint and Inquiry Management System (CIMS), Consolidated Complaint Management System (CCMS), and other electronic databases and network databases not specifically named here that are used to store consumer informal complaints and inquiries. Each informal submission is automatically assigned a file identification number for future reference when the case is entered into one of the databases. This identification number tracks consumer submissions and assists with identification of duplicate filings, which occur when consumers file multiple submissions. Confidential paper submissions are moved to a locked storage room for safekeeping. All records are kept in accordance with the agency records control schedule approved by NARA.

Retrievability:

Information, *e.g.*, records, files, and data, etc., in this system may be retrieved by the individual's personal identifiers, (*i.e.*, name, street address, e-mail address, and phone number), entity name, program name, date received and date closed, problem description field, and/or call sign.

Safeguards:

Electronic records that emanate from these informal complaint and inquiry submissions are maintained in CIMS, CCMS or other electronic and network computer databases not specifically named here, which are secured through controlled access and passwords restricted to a limited number of FCC employees or contractors working on informal complaints and inquiries. In addition, as an added security measure, the staff in the Consumer and Governmental Affairs Bureau, Enforcement Bureau, and other FCC bureaus and offices who are assigned responsibility for resolution of these records in CIMS are only allowed access to these records via a "license" that also tracks their use of the records. Confidential paper submissions are moved to a locked storage room for safekeeping.

Retention and Disposal:

The information in this system is limited to electronic data, paper files, and audio files, *e.g.*, telephone call records, etc. The information is retained at the FCC and then destroyed in accordance with the agency records control schedule N1-173-07-1, approved by NARA, which generally requires that source records are destroyed three years after data is entered into the system, and records in the masterfile are destroyed three years after the case is closed.

System Manager(s) and Address(es):

Address inquiries to the Office of Managing Director or the Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Office of Managing Director or the Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Office of Managing Director or Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554.

An individual requesting access must follow FCC Privacy Act regulations regarding verification of identity and amendment of records. *See* 47 CFR 0.554-0.557.

Contesting Record Procedures:

Address inquiries to the Office of Managing Director or Consumer and Governmental Affairs Bureau, Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in this system include the complainants and subject entities.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /CGB-2

System Name:

Comment Filing System (ECFS).

Security Classification:

None.

System Location(s):

Chief, Consumer and Governmental Affairs Bureau, Room 5-C758, Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554 and 1270 Fairfield Road, Gettysburg, PA 17325.

Categories of Individuals Covered by the System:

Individuals who have filed comments relative to Federal Communications Commission (FCC) rulemakings and docketed proceedings or other matters arising under the Communications Act of 1934, as amended, and the Rehabilitation Act.

Categories of Records in the System:

1. Comments received by the FCC, whether electronically through the Electronic Comment Filing System (ECFS), via the Internet, e-mail, mailed, or delivered by paper copy. This includes information provided via FCC Forms 475 and 501.
2. The system also contains files and records submitted in response to Commission rulemakings and docketed proceedings, and by the FCC's administrative law staff as the repository for official records arising out of the conduct of administrative proceedings.

Authority for Maintenance of the System:

44 U.S.C. Chapter 36; 47 U.S.C. 151 and 154; and Sections 504 and 508 of the Rehabilitation Act, 29 U.S.C. 794 *et al.*

Purpose(s):

In order to comply with the requirements of various statutes and regulations, the FCC offers multiple avenues through which the public can be involved in its decision-making process and can inform the FCC of concerns regarding compliance with FCC rules and requirements. Collecting and maintaining these types of information allows the FCC to be fully informed in decision-making, implementation, and enforcement endeavors. Such a system also allows staff access to documents and improves staff efficiency. Records in this system are available for public inspection.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Additionally, information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public Access--under the rules of the Commission, public comments on rulemakings are routinely available to the public--unless confidentiality is requested (47 CFR 0.459)--via either the Commission's electronic comment filing system (ECFS) at <http://www.fcc.gov/cgb/ecfs/> or the public Reference Information Center (RIC) at <http://www.fcc.gov/cgb/ric.html>;
2. Enforcement--when a record in this system involves an informal complaint filed against telecommunications providers, the complaint may be forwarded to the defendant provider for a response, pursuant to Section 208 of the Communications Act of 1934, as amended, and other applicable rules. When an order or other Commission-issued document that includes consideration of informal complaints filed against telecommunications providers is entered by the FCC to implement or to enforce the Communications Act, pertinent rule, regulation, or order of the FCC, the complainant's name may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests that the FCC withhold his or her name from public disclosure, such a request will be granted and the complainant's name will not be disclosed in the Commission-issued order or document;
3. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
4. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to an FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
5. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
6. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Paper copies of records in this system of records are maintained in file folders. The electronic files are located in computer databases on the FCC internal network.

Retrievability:

Records are retrieved by individual name, entity name, rulemaking number, and/or docket number.

Safeguards:

Records are available over the Internet 24 hours a day, seven days a week. Paper copies representing one third of the records are maintained in the Reference Information Center (RIC). Back-up of the data in ECFS is the responsibility of the FCC's Information Technology Center of the Office of Managing Director and is performed nightly.

Retention and Disposal:

The retention schedule for this system of records has not yet been determined. No records will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Chief, Reference Information Center, Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street, Room CY-B533, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Commenters and subject entities.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /CGB-3

System Name:

National Deaf-Blind Equipment Distribution Program (NDBEDP).

Security Classification:

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

System Location(s):

Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554 and 1270 Fairfield Road, Gettysburg, PA 17325.

Categories of Individuals Covered by the System:

The categories of individuals in this system include:

1. Individuals who request or receive the NDBEDP equipment;
2. Individuals who attest to the disability of the individual receiving the NDBEDP equipment and/or matters related to the eligibility requirements, qualifications, and regulations, etc., for those seeking to participate in NDBEDP; and
3. Individuals who may file complaints, including but not limited to both formal and informal complaints, and inquiries on behalf of themselves or NDBEDP participants and matters related to NDBEDP rules and regulations.

Categories of Records in the System:

The categories of records in this system include:

1. The name and contact information, including street address and email addresses, and phone number for the individuals requesting or receiving the NDBEDP equipment;
2. The name and contact information, including street and email addresses, phone number(s), and fax number(s) for the individuals attesting to the disability of the individual who is deaf-blind;
3. Other miscellaneous PII related to the individuals who participate in this program, *e.g.*, response data for equipment requests, users' complaints, evaluation of the users' needs, user training data, outreach activities, equipment request denial data, and medical attestations or records regarding disability qualifications and eligibility requirements;
4. The name and contact information, including street and email addresses, phone number(s), and fax number(s) for individuals who make or have made formal and informal complaints and inquiries (including related supporting information) in any format (including but not limited to paper, telephone, TTY, recording, Braille, and electronic submissions, such as email, Internet, and fax, *etc.*) on behalf of themselves or NDBEDP participants;
5. Commission correspondence, *e.g.*, letters and related communications regarding formal and informal complaints and inquiries (which may include PII and related information) that pertain to the NDBEDP programs, the NDBEDP individual participants, and the certification and participation of each entity approved by the Commission to participate in the NDBEDP.

Authority for Maintenance of the System:

47 U.S.C. 154, 254(k); Sections 403(b)(2)(B), (c) Public Law 104-104, 110 Stat. 56. Interpret or apply 47 U.S.C. 201, 218, 222, 225, 226, 228, 254(k), and 620.

Purpose(s):

The Commission's CGB will use the information, *e.g.*, records, in this system, which is submitted by the certified equipment distribution program in each state, as required by the NDBEDP, to maintain each state's certification to participate in this program.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Informal Complaints--When a record in this system involves a formal or informal complaint, and/or inquiry filed against an NDBEDP certified program and related entities, the complaint or inquiry may be forwarded to the subject certified program for that state, the appropriate State and Federal medical boards, certifying associations, and related groups, and personal physicians (who may determine whether an individual meets the eligibility criteria for participation in the NDBEDP) for a response, as required under FCC rules;
2. Medical Records--A medical attestation or record (including but not limited to third party attestations, certifications, and declarations of disability) from this system may be disclosed to appropriate entities, including but not limited to the subject certified program for that state, the appropriate State and Federal medical boards, certifying associations, and related groups, and personal physicians for the purposes of determining whether an individual meets the eligibility criteria of being deaf-blind required to participate in the NDBEDP program;
3. Income Eligibility Records--A record from this system may be disclosed to appropriate entities, including but not limited to the subject certified program for that state, the appropriate State and Federal certifying boards and authorities for the purposes of determining whether an individual meets the income eligibility criteria required to participate in the NDBEDP program;
4. Law Enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
5. Adjudication and Litigation--Where by careful review, the Agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
6. Department of Justice--A record from this system of records may be disclosed to the Department of Justice (DOJ) or in a proceeding before a court or adjudicative body when:
 - (a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and
 - (b) The Commission determines that the disclosure is relevant or necessary to the litigation;
7. Congressional Inquiries--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;
8. Government-wide Program Management and Oversight--When requested by the General Services Administration (GSA), the National Archives and Records Administration (NARA), and/or the Government Accountability Office (GAO) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906 (such disclosure(s) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
9. Breach of Federal Data--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or

entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm; and

10. FCC Enforcement Actions--When a record in this system involves a formal and/or informal complaint or inquiry filed alleging a violation of FCC Rules and Regulations by an applicant, licensee, certified or regulated entity or an unlicensed person or entity, the complaint may be provided to the alleged violator for a response. When an order or other Commission-issued document that includes consideration of a formal or informal complaint or complaints or inquiries is issued by the FCC to implement or to enforce FCC Rules and Regulations, the complainant's name or other PII may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests confidentiality of his or her name or other PII from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission's ability to investigate and/or resolve the complaint.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information in the NDBEDP system includes electronic data, records, and files that are stored in the FCC's computer network databases, and paper documents, records, and files that are stored in file cabinets in the CGB office suite.

Retrievability:

Information in the electronic NDBEDP databases can be retrieved by categories of information, including but not limited to the individual's contact information, including the individual's name(s), street address, email address(es), and landline phone and cell phone number(s), complainant(s), and description fields.

The paper documents in the NDBEDP files are assigned a file identification name and/or number for future reference.

Safeguards:

Access to the information, *e.g.*, electronic records, files, and data, in the NDBEDP, which is housed in the FCC computer network databases, is restricted to authorized CGB supervisors and staff and to the supervisors, staff, and contractors in the FCC's Information Technology Center (ITC), who maintain these computer databases. 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. Information resident on the database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured location.

The paper documents are maintained in file cabinets that are located in the CGB office suite, whose access is through a card-coded main door. Access to these files is restricted to authorized CGB supervisors and staff.

Retention and Disposal:

The FCC will retain these records until a records schedule has been approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Address inquiries to the Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in this system include the individuals who request or receive the NDBEDP equipment; individuals, groups, and other entities who attest to the disability of the individual requesting or receiving the equipment; and other individuals, groups, and other entities who have a connection to the NDBEDP and its participants, *e.g.*, those filing formal and informal complaints or inquiries on behalf of the participants.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /CGB-4

System Name:

Internet-based Telecommunications Relay Service-User Registration Database (ITRS-URD) Program.

Security Classification:

The FCC's CIO team will provide a security classification to this system based on NIST FIPS-199 standards.

System Location(s):

TRS Fund Program Coordinator, Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

Categories of Individuals Covered by the System:

Categories of Records in the System:

Authority for Maintenance of the System:

47 U.S.C. 141-154, 225, 255, 303(r), 616, and 620; 47 CFR Parts 64, Subpart F, Telecommunications Relay Services and Related Customer Premises Equipment for Persons With Disabilities (VRS Reform Order).

Purpose(s):

1. The information that is used to determine whether an individual who is applying for the ITRS-URD Program's services is eligible to register to participate in/subscribe to the ITRS-URD Program's services.
2. The information that the ITRS-URD Program's administrator uses to determine whether information with respect to its registered users already in the ITRS-URD Program's database(s) is correct and complete. These ITRS-URD Program's VRS providers must furnish the ITRS-URD Program's administrator with a subscriber list containing PII that includes the individual's full name (first, middle, and last names), parent or guardian's name of the registered subscriber who is a minor, full residential address, date of birth, last four digits of social security number (or alternative proof of identification for those who do not have a social security number), ten digit telephone number(s) assigned in the TRS number directory and associated URI information, user's registered location information for emergency calling purposes, eligibility certification (digital copy) for ITRS-URD Program's service(s) and date obtained from provider, VRS provider and ITRS-URD Program's initiation date and termination date, ITRS-URD Program support received per month, date of the provision of ITRS-URD Program support (if applicable), ITRS-URD Program user password, and date on which user last placed a point-to-point or relay call, call detail records registry for all forms of ITRS-URD Program's services, including CDRs supporting requests for reimbursement of VRS, IPCTS, and IP Relay service, monitoring and reporting information on data abnormalities, errors, and potential sources of fraud subscriber;
3. The information that the ITRS-URD Program's administrator will use to implement a system for automated validation of the registration information that has been submitted and ensure that the authorized VRS providers are unable to register individuals who do not pass the identification verification check conducted through the ITRS-URD Program. The ITRS-URD Program's Third Party contractor and subcontractors will establish the verification protocol to ensure that each individual has proven his/her eligibility to use the service with their desired default VRS provider;
4. The information VRS providers must request to validate each individual who seeks to register that he/she is an actual person living or visiting in the United States;
5. The information for a user signed up with multiple providers for different VRS services. Each company acting as the default provider will have access to their users' information as it pertains only to their service; and
6. The information that is contained in the records of the inquiries that the ITRS-URD Program's VRS providers will make available to the ITRS-URD Program's administrator's Third Party contractor and subcontractors who manages the database [verification/call/service center(s)] to verify that individuals who are deaf, deaf-blind, hard of hearing, and/or have speech disabilities and who are eligible under the ADA to participate in the ITRS-URD Program's services.

Records in the ITRS-URD Program's system of records are available for public inspection after redaction of information that could identify the individual ITRS-URD Program's participant/subscriber, such as the individual's name(s), date of birth, last four digits of social security number (including alternative proof of identification or other unique ID for those individuals who do not have a social security number), tribal ID number, telephone number(s), emergency location, and/or other PII that validates their participation in this program.

Categories of Records in the System:

Information about individuals in this system of records may routinely be disclosed under the following conditions. The FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected in each of these cases.

1. **FCC Program Management** – A record from this system may be accessed and used by the FCC and the ITRS-URD Program Administrator and Program contractor’s employees (including employees of subcontractors) to conduct official duties associated with the management and operation of the ITRS-URD Program, as directed by the Commission. The FCC may routinely have access to the information in the ITRS-URD Program’s database(s), which includes, but is not limited to audits, oversight, and/or investigations of the ITRS-URD Program’s database(s) for the purposes of managing and/or eliminating waste, fraud, and abuse in the ITRS services and ITRS-URD Program. The information may be shared with the FCC’s Enforcement Bureau (EB), Consumer and Governmental Affairs Bureau (CGB), Office of Managing Director (OMD), Office of Inspector General (OIG), Telecommunications Relay Services (TRS) Fund Administrator and Program contractor(s) (and subcontractors), and the FCC TRS Fund Program Administrator, as necessary;

2. **Third Party Contractors** – A record from this system may be disclosed to an employee of a third-party contractor (and subcontractors, as required) to conduct the verification process that allows the ITRS-URD Program’s administrator to determine the accuracy of the PII provided by the ITRS-URD Program’s registrants to the system of records, i.e., when an employee of a third-party contractor (and/or subcontractor), responsible for management registration and fraud prevention, verifies the eligibility of the participant/registrant/subscriber;

3. **State Agencies and Authorized Entities**– A record from this system may be disclosed to designated state agencies and other authorized entities, which include, but are not limited to state public utility commissions, and their agents, as is consistent with applicable Federal and State laws, to administer the ITRS-URD Program in that state and to perform other management and oversight duties and responsibilities. When necessary, this may include the transfer of data to and/or from the Third Party Contractor (and subcontractors) to determine or verify the accuracy of the PII provided by the ITRS-URD Program’s registrants;

4. **FCC Enforcement Actions** – When a record in this system involves an informal complaint filed with the FCC alleging a violation of FCC Rules and Regulations by an ITRS-URD Program’s applicant/subscriber/registrant, licensee, certified or regulated entity or an unlicensed person or entity, the complaint may be served to the alleged violator for a response through the FCC’s normal course of complaint handling process. When an order or other Commission-issued document that includes consideration of an informal complaint or complaints is issued by the FCC for resolution or to enforce FCC Rules and Regulations, the complainant’s name may be made public in that order or letter document. Where a complainant in filing his or her complaint explicitly requests that confidentiality of his or her name from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission’s ability to investigate and/or resolve the complaint;

5. **Congressional Investigations and Inquiries** – A record from this system may be disclosed to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, for the purposes of an official Congressional investigation, including but not limited to information concerning ITRS and the ITRS-URD Program’s services, ITRS-URD Program’s Administrator (and Third Party Contractors and subcontractors) and ITRS-URD Program participants/subscribers/registrants, and/or in response to an inquiry made by an individual to the Congressional office for the individual’s own records;

6. **Government-wide Program Management and Oversight** – When requested by the National Archives and Records Administration (NARA), the Office of Personnel Management (OPM), the General Services Administration (GSA), and/or the Government Accountability Office (GAO) for the purpose of records management studies conducted under authority of 44 U.S.C. 2904 and 2906 (such disclosure(s) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department’s advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office’s advice regarding obligations under the Privacy Act;

7. ADA Eligibility Verification Data – A record from this system may be disclosed to the appropriate Federal and/or State authorities (including transfers of PII data to/from the ITRS Program’s Administrators, contractors, and subcontractors, as required) for the purposes of verifying whether individuals who are deaf, deaf-blind, hard of hearing and/or have speech disabilities are eligible under the ADA to register to participate in/subscribe to the ITRS-URD Program;

8. Law Enforcement and Investigation – Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate federal, state, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another (federal or state) agency to investigate program participation by VRS providers;

9. Adjudication and Litigation – Where by careful review, the Agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

10. Department of Justice – A record from this system of records may be disclosed to the Department of Justice (DOJ) or in a proceeding before a court or adjudicative body when:

(a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Commission determines that the disclosure is relevant or necessary to the litigation; and

11. Breach of Federal Data – A record from this system may be disclosed to appropriate agencies, entities (including the ITRS-URD Program’s administrator and its employees), and persons when: (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

1. ITRS providers to populate and update subscriber information and to query to verify the subscriber’s status;

2. The FCC to perform oversight, performance, investigations, and/or audit functions, and

3. The ITRS-URD Program administrator or the TRS Fund Administrator to retrieve records and to obtain/transfer data from the Third Party Contractor and subcontractor, when required for the verification process.

Any paper documents will be stored in filing cabinets in the secured areas in the ITRS-URD Program’s administrator’s office and at the FCC for oversight, performance, investigations, and/or audit purposes.

Retrievability:

Information in the ITRS-URD Program may be retrieved by various identifiers, including, but not limited to the individual's name, last four digits of the social security number (SSN), date of birth, phone number, and residential address and other identifiers listed in the "CATEGORIES OF RECORDS IN THE SYSTEM."

Safeguards:

1 Access to the electronic files is restricted to:

- a. Authorized and credentialed the ITRS-URD Program's administrator's employees;
- b. TRS Fund Administrator (and the TRS Third Party Contractor(s) and subcontractor(s)); and
- c. Authorized FCC employees and contractors including, but not limited to the FCC TRS Fund Program Administrator, Enforcement Bureau (EB), Office of Inspector General (OIG), Consumer and Governmental Affairs Bureau (CGB), and Office of Managing Director (OMD), Information Technology (IT), and other bureaus and offices (B/Os), as required, to perform oversight, performance, auditing, and related management functions, duties, and responsibilities.

The FCC requires that parties with authorized access to the ITRS-URD Program's databases, including but not limited to the ITRS Administrator, employees, Third Party contractors and subcontractors, must maintain compliance with the FCC's computer and information security requirements, including those in the Federal Information Security Management Act (FISMA). In addition, an Independent Verification and Validation (IV&V) shall be performed to certify that functional and security requirements were met. IV&V will be conducted by a third-party vendor to ensure reliability, accessibility, validity, compatibility, traceability, security, and ease of use of the application within the environment.

2. The paper documents are maintained in file cabinets that are located in the ITRS-URD Program's administrator's office suites (and the Third Party contractor and subcontractor, as required), and at the FCC for oversight, performance, investigations, and/or audit purposes. The file cabinets are locked when not in use and at the end of the business day.

Access to these files is restricted to:

- a. Authorized ITRS-URD Program's administrator's employees (and contractors and subcontractors); and
- b. The TRS Fund Administrator and authorized FCC employees and contractors including, but not limited to the FCC TRS Fund Program Administrator, Enforcement Bureau (EB), Office of Inspector General (OIG), Consumer and Governmental Affairs Bureau (CGB), and Office of Managing Director (OMD), Information Technology Center (ITC), and other bureaus and offices (B/Os), as required, to perform oversight, performance, auditing, and related management functions, duties, and responsibilities.

Retention and Disposal:

1. The data in the ITRS-URD Program's database(s) (including the information maintained by the Third Party Contractor and subcontractors who perform the verification processes) are the property of the Federal Government, but will be treated as proprietary information of the contractor as the default provider; and
2. A log of all actions (queries and modifications) shall be maintained for a period of no less than five years (or for such other period as directed by the Commission. See Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities, CG Docket Nos. 03-123 & 10-51, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 8618 (2013)(ITRS Order).

Disposal of obsolete or out-of-date paper documents and files is by shredding. Electronic data, files, and records are

destroyed by electronic erasure.

System Manager(s) and Address(es):

TRS Fund Program Coordinator, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554; and

Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

Notification Procedure:

TRS Fund Program Coordinator, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554;

Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554; or

Privacy Analyst, Information Technology (IT), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

Record Access Procedures:

TRS Fund Administrator;

TRS Fund Program Coordinator, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554;

Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554; or

Privacy Analyst, Information Technology (IT), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

Contesting Record Procedures:

TRS Fund Program Coordinator, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554; Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554; or

Privacy Analyst, Information Technology (IT), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

Record Source Categories:

1. The information that the ITRS Program providers must furnish prior to registering ITRS subscribers/participants, and/or to re-certifying ITRS subscribers for participation in the ITRS Program; and
2. The information that individuals who are deaf, deaf-blind, hard of hearing and have speech disabilities and who are eligible under the ADA must provide to determine their eligibility for participation in the ITRS-URD Program.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /EB-5

System Name:

Enforcement Bureau Activity Tracking System (EBATS).

Security Classification:

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

System Location(s):

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

Secondary: Various field facilities. Information about FCC Field Offices can also be found at <http://www.fcc.gov/eb/rfo>.

Categories of Individuals Covered by the System:

The records in this system include:

1. Individuals, including FCC employees, who have filed complaints alleging violations of the Communications Act of 1934, as amended (the "Communications Act"); FCC regulations; other statutes and regulations subject to the FCC's jurisdiction; and/or international treaties (collectively referred to hereafter as "FCC Rules and Regulations") by FCC licensees or regulates, or individuals who have filed such complaints on behalf of business(es), institution(s), etc., and who may have included their personally identifiable information (PII) in the complaint;
2. Individuals who are or have been the subjects of Federal Communications Commission (FCC) field monitoring, inspection, and/or investigation, etc., for possible violations of FCC Rules and Regulations;
3. Licensees, applicants, regulatees, and unlicensed individuals about whom there are questions of compliance with FCC Rules and Regulations; and
4. FCC employees, contractors, and interns who perform work on behalf of the Enforcement Bureau.

Categories of Records in the System:

The categories of records in this system include:

1. Information that is associated with those individuals who file complaints or who are being investigated for possible enforcement actions, *e.g.*, violators, *etc.* The information may include:
 - (a) An individual's name, Social Security Number (SSN) or Taxpayer Identification Number (TIN), gender, race/ethnicity, birth date/age, place of birth, biometric data (photograph(s)), marital status, spousal data, miscellaneous family data, home address, home address history, home telephone number(s), personal cell phone number(s), personal fax number(s), personal e-mail address(es), credit card number(s), driver license number(s), bank account data, financial data, law enforcement data, background investigatory data, national security data, employment and/or employer data, and other miscellaneous materials, documents, and files, etc., which are used for background information and data

verification, *etc.*;

(b) Inspection reports, audit reports, complaints, referrals, monitoring reports, inspection cases, referral memos, correspondence, discrepancy notifications, warning notices, and forfeiture actions, *etc.*; and

(c) Miscellaneous materials, documents, files, and records that are used for background information and data verification concerning individuals who may be accused or have violated the Commission's rules and regulations.

2. The information that is associated with the same or similar current enforcement cases and historic records and other archival, background, and research data and materials that are stored for reference in enforcement actions, *i.e.*, inspection reports, complaints, monitoring reports, investigative cases, referral memos, correspondence, discrepancy notifications, warning notices, and forfeiture actions; and

3. Other, miscellaneous information that complainants may have included on FCC Forms 475B, 501, 1088, and/or 2000, as well as any additional FCC forms that may be used from time to time to report possible violations of FCC Rules and Regulations (as defined above) to the FCC or associated with case files.

Authority for Maintenance of the System:

47 U.S.C. 101, 102, 104, 301, 303, 309(e), 312, 315, 318, 362, 364, 386, 501, 502, 503, 507, and 510.

Purpose(s):

The Enforcement Bureau uses the information in this information system:

1. To track the status of enforcement cases of entities (including individuals) that have been identified as possible violators of the FCC's Rules and Regulations (as defined above);

2. To determine the levels of compliance among FCC licensees, and other regulatees;

3. To document Commission monitoring, audits, inspections and investigations for compliance and enforcement purposes;

4. To provide a basis for the various administrative and civil, or criminal actions against violators by the Enforcement Bureau (EB), other appropriate Commission bureaus or offices, and/or other government agencies;

5. To gather background information for reference materials from various external databases and resources, *etc.*, to insure that the information that is being compiled is accurate and up-to-date ("cross-checking") in the course of investigating consumer complaints and/or enforcement cases;

6. To maintain archival information (paper documents and files) for reference in enforcement investigations and other actions; and

7. To prevent duplication of FCC's enforcement actions, *e.g.*, for cross-reference purposes, *etc.*

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. *Public Access*--Copies of FCC enforcement actions are available for public inspection via the Internet at <http://www.fcc.gov/eb/>, and in the FCC's Reference Information Center at <http://www.fcc.gov/cgb/ric.html>;

2. *Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the Agency*--Disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records,

other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

3. *Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by an Entity other than the Agency*--Disclosure may be made to a Federal, State, local, foreign, Tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the Agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action;

4. *Adjudication and Litigation*--Where by careful review, the Agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

5. *Law enforcement and Investigation*--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

6. *Congressional Inquiries*--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

7. *Government-wide Program Management and Oversight*--When requested by the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

8. *FCC Enforcement Actions*--When a record in this system involves an informal complaint filed alleging a violation of FCC Rules and Regulations (as defined above) by an applicant, licensee, regulated entity or an unlicensed person or entity, the complaint may be provided to the alleged violator for a response. When an order or other Commission-issued document that includes consideration of an informal complaint or complaints is issued by the FCC to implement or to enforce FCC Rules and Regulations (as defined above), the complainant's name may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests that confidentiality of his or her name from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission's ability to investigate and/or resolve the complaint;

9. *Breach of Federal Data*--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

10. *Due Diligence Inquiries*--Where there is an indication of a violation or potential violation of FCC Rules and Regulations (as defined above), records from this system may be shared with a requesting individual, or representative

thereof, for purposes of obtaining such information so long as relevant to a pending transaction of a FCC-issued license.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in this information system consists of electronic records, files, and data that are stored in the FCC's computer network databases, at headquarters and in the field offices, and paper records, documents, and files that are stored in filing cabinets in the EB office suites at headquarters and in field offices.

Retrievability:

1. Information in the electronic database information can be retrieved by the name(s) of the individual(s) who filed the complaint(s), the individual who is subject of the complaint, and by a unique case number assigned to each type of activity conducted by the Bureau, *e.g.*, inspections, audits, investigations, hearings, due diligence requests, *etc.*
2. Information in the central files, *e.g.*, paper documents, records, and files, *etc.*, includes all the other information pertaining to these complainant investigations and/or cases, *i.e.*, name, address, telephone number, *etc.*, and is maintained for reference and archival purposes. This information is retrieved by a unique identification number assigned to each complainant investigation and/or case.

Safeguards:

The paper files, documents, and records are stored in file cabinets in non-public areas in the EB office suites at headquarters and in field offices. The file cabinets are locked at the end of each business day or when not in use.

The electronic records, data, and files are maintained in the FCC computer network databases at headquarters and in the field offices. Access to both the paper files and the electronic files is restricted to authorized EB supervisors and staff. Authorized staff and contractors in the FCC's Information Technology Center (ITC) have access to the electronic files. Other employees, interns, and contractors may be granted access to the paper files and/or the electronic files 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. Information resident on the database servers is backed-up routinely onto magnetic media. Backup tapes are stored on-site and at a secured, off-site location. The information that is stored in the computer databases in the EB field offices is protected by similar security protocols and safeguards.

Retention and Disposal:

The retention schedule for this system of records has not yet been determined. No records will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA). [check with Records Management]

System Manager(s) and Address(es):

Enforcement Bureau (EB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR Section 0.561) that this system of records is exempt from disclosing its notification procedure for this system of records.

Record Access Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR Section 0.561) that this system of records is exempt from disclosing its record access procedure for this system of records.

Contesting Record Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR Section 0.561) that this system of records is exempt from disclosing its contesting record procedure for this system of records.

Record Source Categories:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR Section 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

Exemptions Claimed for the System:

This system of records is exempt from sections (c)(3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;
2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act; and
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

[\[Return to TOP\]](#)

FCC /MB-1

System Name:

Ownership Report for Commercial Broadcast Stations.

Security Classification:

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

System Location(s):

Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

- (1) Licensees, permittees, and respondents, and other individuals or entities with interests therein that are required to be reported on the Form 323 (as described below) who must either file FCC Form 323 or have their interests reported on Form 323 under 47 CFR 73.3615, 73.6026, and 74.797;
- (2) Contact individuals, *e.g.*, representatives, relating to commercial AM, FM, and TV broadcast stations, and/or newspapers that are subject to the Commission's media ownership rules, as required under 47 CFR 73.3555, etc.;
- (3) Individuals with ownership or attributable interests in media companies subject to the Commission's ownership rules or otherwise required to be reported on FCC Form 323;
- (4) Individuals who are married to or otherwise related, *i.e.*, parent-child or siblings, etc., to other individuals who have attributable, reportable, and/or ownership interests and who must either file FCC Form 323 or have their interests reported on FCC Form 323.

Categories of Records in the System:

- (1) Information that is required to be submitted on FCC Form 323, "Ownership Report for Commercial Broadcast Stations," including the ownership or other interests of the licensee/permittee/respondent, home mailing address, home telephone number, home e-mail address, listing type, relationship to licensee/permittee/respondent/other interest holder, positional interest, marital/familial relationship, and gender, ethnicity, race, and citizenship, etc.;
- (2) All exhibits, organizational charts, correspondence, *i.e.*, letters, etc., supporting documentation, and other materials, etc., which are associated with processing the FCC Form 323, "Ownership Report for Commercial Broadcast Station," submission(s); and
- (3) Any other records that are submitted in connection with or created as the result of the filing of FCC Form 323.

Authority for Maintenance of the System:

47 CFR 73.3555, 73.3615, 73.6026, and 74.797.

Purpose(s):

The records are kept to administer the Federal Communications Commission's (FCC) regulatory responsibilities that relate to ownership of commercial broadcast stations, including AM and FM radio and television, as well as to interests in daily newspapers that are subject to the Commission's media ownership rules. The Commission uses these records in this system:

- (1) To address the data contained in responses to FCC Form 323, "Ownership Report for Commercial Broadcast Stations," which the Commission uses to evaluate licensees' or permittees' compliance with the Commission's media ownership rules, etc. This form is filed:
 - (a) To satisfy the biennial filing requirement (Biennial Ownership Report);
 - (b) As a validation or resubmission of a previously filed Biennial Report;
 - (c) In connection with the transfer of control or assignment of a broadcast station;
 - (d) By a permittee (within 30 days of the grant of a construction permit grant) ("Permittee Report") and on the date that it files its license application;

(e) As an update or certification of accuracy of the initial Permittee Report; or

(f) As an amendment of a previously filed Ownership Report.

(2) To undertake studies of minority and female ownership that support its diversity policy goals and other ownership studies to support its statutory requirement to review the media ownership goals quadrennially to determine whether they are necessary in the public interest as the result of competition.

(3) Any other uses of FCC Form 323 within the Commission's authority.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public Access--under the rules of the Commission, documents filed under CDBS are publicly available;

2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Financial Obligations under the Debt Collection Acts--a record from this system may be disclosed to other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996. A record from this system may be disclosed to any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government. A record from this system may be used to prepare information on items considered income for taxation purposes to be disclosed to Federal, state, and local governments;

4. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

5. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

6. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act; and

7. Breach Notification--a record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for

which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The Broadcast Station Ownership database is the repository for all electronically filed ownership reports and associated information, including exhibits (*e.g.*, organizational charts, appendices, scanned images, and all other supplementary documents and materials, etc.). All Form 323 filings must be submitted electronically (*e.g.*, paper copy filings are not acceptable) via the Media Bureau Electronic Filing system at: <http://www.fcc.gov/mb/elecfile.html>.

Retrievability:

Information in this system is publicly retrievable. The information may be viewed via the "Public Access" Search functionality in the Consolidated Database System (CDBS) at: <http://www.fcc.gov/mb/elecfile.html> by clicking on the "Ownership Search" link. Information may be retrieved by searching electronically using a variety of parameters including the call sign, facility ID number, service, file number, application type, channel, frequency, community of license city and state, name of the licensee/permittee, or name/address of the person or entity holding the interest reported on Form 323. All ownership data can also be downloaded via a set of files that correspond to database tables from the Media Bureau Public CDBS Database Files Web site: <http://www.fcc.gov/mb/databases/cdbs>. Information is retrieved internally via database commands by authorized FCC staff and contractors who have been granted permission to access the data.

Safeguards:

Information in these records and files is available to the public via the FCC Internet portal at: <http://www.fcc.gov/mb/elecfile.html>. Access to the ownership records housed in the CDBS databases is restricted to authorized MB supervisory and staff and ITC staff and contractors. Other employees and contractors may be granted access on a "need-to-know" basis. The CDBS network computer databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. Information resident on the CDBS database server is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured location.

Retention and Disposal:

The information in this system is limited to electronic files, records, and data, which includes:

- (1) The information that pertains to current filing requirements; and
- (2) The information that pertains to historical records, which is used for archival purposes.

Until the National Archives and Records Administration (NARA) approves the retention and disposal schedule, these records will be treated as permanent.

System Manager(s) and Address(es):

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in this system include all entities that are required to file an ownership report, either biennially or at other occasions, under §§ 73.3615, 73.6026, and 74.797 of the Commission's rules. These entities include, but are not limited to:

- (1) Licensees, permittees, and respondents, and other individuals or entities with interests therein that are required to be reported on the Form 323 (as described below) who must either file FCC Form 323 or have their interests reported on Form 323 under 47 CFR 73.3615, 73.6026, and 74.797;
- (2) Contact individuals, *e.g.*, representatives, relating to commercial AM, FM, and TV broadcast stations, and/or newspapers that are subject to the Commission's media ownership rules, as required under 47 CFR 73.3555, etc.;
- (3) Individuals with ownership or attributable interests in media companies subject to the Commission's ownership rules or otherwise required to be reported on FCC Form 323; and
- (4) Individuals who are married to or otherwise related, *i.e.*, parent-child or siblings, etc., to other individuals who have attributable, reportable, and/or ownership interests and who must either file FCC Form 323 or have their interests reported on FCC Form 323.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /MB-2

System Name:

Broadcast Station Public Inspection Files.

Security Classification:

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

System Location(s):

Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in this system include, but are not limited to:

1. Individuals who are required to file personal information pertaining to their political campaigns and other requirements; and
2. Individuals who are associated with a television broadcast station license and are required to submit information under 47 CFR 73.3526 and 73.3527.

Categories of Records in the System:

The categories of records in this system may include, but are not limited to an individual's name, home address, home telephone number, personal cell phone number, personal email address(es), personal fax number, bank check routing number, credit card number, and other personal information (*i.e.*, personally identifiable information (PII)) that stations may include in their public files, and which may be included in the PII contained in the documents, files, and records that television broadcast stations and certain individuals are required to submit to the FCC to be posted in the FCC's on-line Broadcast Station Public Inspection Files. FCC Rules do not require submission of bank check routing numbers and credit card numbers, but the broadcast stations may choose to include such information in their public files as a means of indicating fulfillment of contracts.

Authority for Maintenance of the System:

47 U.S.C. 151, 152, 154(i), 303, 307, and 315.

Purpose(s):

The Commission will be hosting all Broadcast Station Public Inspection Files in an online database. Stations have been required to maintain their public files at their main studios for decades, pursuant to 47 CFR 73.3526 and 73.3527. The Commission will now begin hosting such files online in order to make the files more accessible to the public. Records in this system are available for public inspection.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public Access--Under the rules of the Commission, documents filed under the Consolidated Database System (CDBS) or in the online Broadcast Station Public Inspection Files are available for public inspection;
2. Public Access--Copies of FCC enforcement actions are available for public inspection via the Internet at <http://www.fcc.gov/eb/> and in the FCC's Reference Information Center at <http://www.fcc.gov/cgb/ric.html>
3. Law Enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Adjudication and Litigation--Where by careful review, the Agency determines that the records are both relevant and

necessary to litigation and the use of such records is deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

5. Department of Justice--A record from this system of records may be disclosed to the Department of Justice (DOJ) or in a proceeding before a court or adjudicative body when:

(a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Commission determines that the disclosure is relevant or necessary to the litigation;

6. Congressional Inquiries--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;

7. Government-wide Program Management and Oversight--When requested by the General Services Administration (GSA), the National Archives and Records Administration (NARA), and/or the Government Accountability Office (GAO) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906 (such disclosure(s) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

8. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when:

(1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

9. FCC Enforcement Actions--When a record in this system involves a formal and/or informal complaint or inquiry filed alleging a violation of FCC Rules and Regulations by an applicant, licensee, certified or regulated entity or an unlicensed person or entity, the complaint may be provided to the alleged violator for a response. When an order or other Commission-issued document that includes consideration of a formal or informal complaint or complaints or inquiries is issued by the FCC to implement or to enforce FCC Rules and Regulations, the complainant's name or other PII may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests confidentiality of his or her name or other PII from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission's ability to investigate and/or resolve the complaint;

10. Due Diligence Inquiries--Where there is an indication of a violation or potential violation of FCC Rules and Regulations (as defined above), records from this system may be shared with a requesting individual, or representative thereof, for purposes of obtaining such information so long as relevant to a pending transaction of a FCC-issued license; and

11. Financial Obligations under the Debt Collection Acts--A record from this system may be disclosed to other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996. A record from this system may be disclosed to any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government. A record from this system may be used to prepare information on items considered income for taxation

purposes to be disclosed to Federal, state, and local governments.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose(s) for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information in the Broadcast Station Public Inspection Files includes electronic data, records, and files that are stored in the FCC's computer network databases.

Retrievability:

Information in the Broadcast Station Public Inspection Files electronic databases can be retrieved by categories of information that each individual must provide as required by 47 CFR 73.3526 and 73.3527, including the individual's name(s), street address, email address(es), landline phone and cell phone number(s), complainant(s), and file identification name and/or number, etc.

Safeguards:

Access to the information, *e.g.*, electronic records, files, and data, in the Broadcast Station Public Inspection Files, which is housed in the FCC computer network databases, is posted on the Internet to be publicly accessible. Only the broadcast stations who upload information into the broadcast station files can alter their information. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other IT security features and requirements. Information resident on the database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured off-site location.

Retention and Disposal:

The FCC will retain these records until a records schedule has been approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Media Bureau (MB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in the Broadcast Station Public Inspection Files include, but are not limited to the PII that may be included in the documents, records, and files that television broadcasters are required to submit to the FCC for posting in the FCC's on-line Broadcast Station Public Inspection Files as required by 47 U.S.C. 315; 47 CFR 73.3526 and 73.3527.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OCBO-1

System Name:

Small Business Contacts Database.

Security Classification:

None.

System Location(s):

Director, Office of Communications Business Opportunities (OCBO), Federal Communications Commission (FCC), 445 12th Street, SW., Room 4-A760 Washington, DC 20554.

Categories of Individuals Covered by the System:

Information includes small, minority, and women-owned communications' business owners and employees, as well as other individuals who work or communicate with this segment of the population.

Categories of Records in the System:

Contact information, where available, such as the individual's name, phone number(s), and address(es).

Authority for Maintenance of the System:

Sections 151, 152, 155, 257, 303 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 155, 257; and 5 U.S.C. 602(c) and 609(a)(3).

Purpose(s):

This system of records serves as a repository of contact information that FCC employees use to further the FCC's outreach mission to small, women, and minority-owned businesses.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

This is an electronic system of records that resides on the FCC's internal storage servers, which are backed-up daily.

Retrievability:

Records in this system of records can be retrieved by any category field, *e.g.*, first name or zip code.

Safeguards:

This system of records, which resides on the FCC's internal storage servers, is protected by the FCC's firewall and appropriate-level security protocols that prevent access to the system of records to all but those needing access to the same.

Retention and Disposal:

The retention schedule for this system of records has not yet been determined. No records will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Allan K. Manuel, Chief of Staff, Office of Communications Business Opportunities (OCBO), Federal Communications Commission (FCC), 445 12th Street, SW., Room 4-A665, Washington, DC 20554.

Notification Procedure:

Address inquiries to system manager.

Record Access Procedures:

Address inquiries to system manager.

Contesting Record Procedures:

Address inquiries to system manager.

Record Source Categories:

Information provided to the FCC by individuals and gathered during the course of outreach activities.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OET-1

System Name:

Experimental Radio Station License Files.

Security Classification:

There is no specific security classification for this system; however, data or records within the system may have national defense/foreign policy classifications up through secret.

System Location(s):

Office of Engineering and Technology (OET), Federal Communications Commission, 445 12th Street, SW., Room 7-A303, Washington, DC 20554.

Categories of Individuals Covered by the System:

Those who have been granted a license to operate an experimental radio station under Part 5 of the Federal

Communications Commission's (FCC) rules.

Categories of Records in the System:

1. This system includes the following FCC Forms, any supporting exhibits submitted by the applicant(s), and related documentation:

(a) FCC Form 442, Application for a New or Modified Station;

(b) FCC Form 405, Application for Renewal of Station License;

(c) FCC Form 702, Application for Consent to Assignment of Radio Station Construction Authorization or License;

(d) FCC Form 703, Application for Consent to Transfer Control of Corporation Holding Station License; and

(e) Any supporting exhibits submitted by the applicant(s).

2. This system of records may include experimental project reports submitted by the applicant as required by FCC rules, part 5.

3. The system also includes comments from other Commission bureaus on interference potential of operation.

Authority for Maintenance of the System:

47 U.S.C. 308.

Purpose(s):

FCC employees use these records to determine:

1. An applicant's eligibility to operate a station in the experimental radio service;

2. Interference potential to other radio services within the Commission; and

3. If the project or experimentation is valid, as well as the possible use in rulemakings.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public Access--information from this system may be disclosed to other FCC bureaus, Federal agencies, or to the public, in response to a request, in connection with new experimentation being conducted and the impact that this experimentation may have on the public. The information may not be disclosed if it is not routinely available for public inspection under 47 CFR 0.457(d)(1)(ii) of the Commission's rules, or a request that the information be given confidential treatment is pending or has been granted under 47 CFR 0.459.

2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute,

regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in this system of records includes paper records maintained in file folders, electronically scanned images of paper records, electronic records of data elements of both paper filed and electronically filed applications, and electronic copies of licenses granted after November 16, 1998. Per 47 CFR 5.55(b) all applications for experimental licensing must be filed electronically via the Internet.

Retrievability:

Paper files are retrieved by license name. If there is more than one station per licensee, then the files may also be retrieved by call sign. Scanned images, electronic records of data elements, and electronic copies of licenses may be retrieved from the OET Experimental Licensing Branch Reports World Wide Web electronic filing and reporting site at <https://gullfoss2.fcc.gov/prod/oet/cf/els/index.cfm>.

Safeguards:

All files are available to the public except files not routinely available for public inspection as defined in 47 CFR 0.457(d)(1)(ii) and files that have been submitted in compliance with the confidentiality request requirements of 47 CFR 0.459. Files not routinely available and files pending or granted confidentiality are marked "NOT FOR PUBLIC INSPECTION" and may only be accessed by FCC employees who have a need to know the information. Data resident on network servers are backed-up routinely onto magnetic media. These back-up tapes are stored both on-site and in secured off-site storage locations.

Retention and Disposal:

These records are maintained for two years after expiration of the license. They are then disposed by shredding. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Chief, Experimental Licensing Branch, Office of Engineering and Technology (OET), Federal Communications Commission, 445 12th Street, SW., Room 7-A267, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

The majority of information in these records comes from individual applicants. Other information comes from coordination with other FCC bureaus and from data that are generated with the Spectrum Coordination Branch during the normal processing of the application.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OET-2

System Name:

Equipment Authorization Records and Files.

Security Classification:

None.

System Location(s):

Office of Engineering and Technology (OET), Laboratory Division, Federal Communications Commission (FCC), 7435 Oakland Mills Road, Columbia, MD 21046.

Categories of Individuals Covered by the System:

Individuals who have applied for or been granted an authorization to market equipment using the RF spectrum, in accordance with Part 2 of the Federal Communications Commission's (FCC) rules.

Categories of Records in the System:

1. This system includes the following FCC Forms, any supporting exhibits submitted by the applicant(s), and related documentation:

- (a) FCC Form 731, Application for Equipment Authorization;
- (b) Any supporting exhibits submitted by the applicant(s).

2. This system of records may include test reports and other supporting documentation that demonstrates compliance with the technical rules for licensed transmitters and unlicensed devices as required by FCC Rules, parts 15 and 18.

Authority for Maintenance of the System:

47 U.S.C. 308.

Purpose(s):

These records are used to make a determination of compliance of equipment proposed for marketing with the administrative and technical requirements of the FCC as they relate to equipment using the RF spectrum; and to determine the interference potential of equipment proposed for marketing to equipment operating in both the licensed and unlicensed radio services.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--information from this system on granted equipment authorizations may be disclosed to the public if it is routinely available for public inspection under 47 CFR 0.457(d)(1)(ii) and a request has not been made or granted to give the information confidential treatment under 47 CFR 0.459. Pending equipment authorization requests are specifically excluded from disclosure prior to the effective date of the authorization, as specified in 0.457(d)(1)(ii).

2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to an FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each case the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The equipment authorization database is the repository for all electronically filed applications for equipment authorization and associated information. Per 47 CFR 2.913(a), all applications for equipment authorization must be filed electronically via the Internet.

Retrievability:

Scanned images, electronic records of data elements, and electronic copies of granted licenses may be retrieved from the OET Equipment Authorization Electronic Filing World Wide Web site at <https://gulfoss2.fcc.gov/prod/oet/cf/eas/index.cfm> by clicking on the desired link in the Reports section on the left hand side of the page.

Safeguards:

All files are available to the public except files not routinely made publicly available under 47 CFR 0.457 or those where a request for confidentiality is pending or has been granted under 47 CFR 0.459. Files which are not routinely made publicly available and those with a pending or granted request for confidentiality may only be accessed by Commission employees who have a need to know the information. Data resident on the database server at the OET Laboratory are backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at the FCC Headquarters location.

Retention and Disposal:

The retention schedule for this system of records has not yet been determined. No records will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Chief, Laboratory Division, Office of Engineering and Technology (OET), Federal Communications Commission (FCC), 7435 Oakland Mills Road, Columbia, MD 21046.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Information supplied by individuals wishing to receive equipment authorization.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OGC-3

System Name:

Adjudication of Internal Complaints against Employees.

Security Classification:

None.

System Location(s):

Office of General Counsel (OGC), Federal Communications Commission (FCC), 445 12th Street, SW., Room 8-C743, Washington, DC 20554.

Categories of Individuals Covered by the System:

Any Federal Communications Commission (FCC) employee who is the subject of a complaint investigation involving internal personnel actions or activities, *i.e.*, discrimination, grievance, political activity, separation, or adverse action.

Categories of Records in the System:

Records involve internal personnel disputes that have reached the hearing stage, and may include correspondence, memoranda, transcripts of hearings, briefs, pleadings, investigative reports, and decisions of hearing examiners and Commissioners.

Authority for Maintenance of the System:

5 U.S.C. 301.

Purpose(s):

These records are used by staff attorneys in the General Counsel's office in settlement negotiations with opposing parties; records are also used in preparation for hearings before an administrative body or a court of appropriate jurisdiction.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.
5. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;
6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, foreign, tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action; and
7. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions. In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information is stored in file folders.

Retrievability:

Records are retrieved by the name of the subject individual in the investigation.

Safeguards:

Records are maintained in file cabinets in an office that is secured at the end of each business day. Since only one or two staff persons routinely access this record system, unauthorized examination during business hours would be easily detected.

Retention and Disposal:

Records are kept for five years after the closure of each case. They are then shredded.

System Manager(s) and Address(es):

Office of General Counsel (OGC), Federal Communications Commission (FCC), 445 12th Street, SW., Room 8-C743, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Claimants, co-workers of subject individual, other supervisors, classification experts, and other persons involved in the case.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OGC-5

System Name:

Pending Civil Cases.

Security Classification:

None.

System Location(s):

Office of General Counsel (OGC), Federal Communications Commission (FCC), 445 12th Street, SW., Room 8-C743, Washington, DC 20554.

Categories of Individuals Covered by the System:

Any individual who has a miscellaneous case involving the Federal Communications Commission (FCC) before any District Court, before any Court of Appeals, and before the Supreme Court.

Categories of Records in the System:

Letters, memoranda, pleadings, briefs, and bankruptcy papers.

Authority for Maintenance of the System:

47 U.S.C. 401 and 402.

Purpose(s):

Information in this system of records is used by Commission attorneys to update information or furnish additional data for the Government agency handling the case.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--the records contained in this system are available for public inspection to the extent that they do not contain information usually exempt from mandatory disclosure under Exemption 5 of the FOIA, 5 U.S.C. 552(b)(5).
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in this system of records consists of paper records that are stored in file folders.

Retrievability:

Records are retrieved by the name of the individual filing the claim.

Safeguards:

Records are maintained in file cabinets that are secured at the end of each business day.

Retention and Disposal:

The records are destroyed by shredding when no longer needed or after five years, whichever occurs first.

System Manager(s) and Address(es):

Office of General Counsel (OGC), Federal Communications Commission (FCC), 445 12th Street, SW., Room 8-C743, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Justice Department: U.S. Attorneys; other Federal agencies: U.S. District Courts; and parties to the proceedings.

Exemptions Claimed for the System:

None.

FCC /OGC-6

System Name:

Private or Civil Injury Claimants.

Security Classification:

None.

System Location(s):

Office of General Counsel (OGC), Federal Communications Commission (FCC), 445 12th Street, SW., Room 8-C743, Washington, DC 20554.

Categories of Individuals Covered by the System:

Any individual who files a damage claim against the Federal Communications Commission (FCC) or commits a tort against a FCC employee.

Categories of Records in the System:

Information in this system of records includes accident reports, tort claim vouchers, correspondence, memoranda, medical and payment receipts, repair and payment receipts, and pictures.

Authority for Maintenance of the System:

28 U.S.C. 2672.

Purpose(s):

Information in these records is used by attorneys in the Office of General Counsel to determine whether a damage claim filed against the FCC should be paid and for reference purposes when similar cases arise. If it is determined that the claim should not be paid or if the FCC cannot make the final determination whether or not to pay a claim, the record is routinely transferred to the appropriate agency charged with the responsibility of disposition.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--the records contained in this system are available for public inspection to the extent that they do not contain information usually exempt from mandatory disclosure under Exemption 5 of the FOIA, 5 U.S.C. 552(b)(5).
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent

the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information is stored in file folders.

Retrievability:

Records are retrieved by the name of the individual who filed the claim.

Safeguards:

Records are kept in a file cabinet that is locked at the end of each business day. Since only one or two office persons routinely access this system, unauthorized examination during business hours would be easily detected.

Retention and Disposal:

Records are destroyed by shredding five years after the closure of the case.

System Manager(s) and Address(es):

Office of General Counsel (OGC), Federal Communications Commission (FCC), 445 12th Street, SW., Room 8-C743, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Witnesses: Office of General Counsel; Office of Managing Director: claimants; and employees.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OIG-3

System Name:

Investigative Files.

Security Classification:

Sensitive, but not Classified.

System Location(s):

Office of Inspector General (OIG), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

Included in this system are records on:

1. Individuals who are or have been the subjects of investigations conducted by the OIG; and
2. Individuals who are: witnesses, complainants, informants, suspects, defendants, parties identified by the OIG or by other agencies, constituent units of the FCC and members of the general public in connection with the authorized functions of the OIG.

Categories of Records in the System:

The categories of records in this system include:

1. Files developed during investigations of known or alleged fraud, waste, and abuse, or other irregularities or violations of laws and regulations;

2. Files related to programs and operations administered or financed by the FCC, including contractors and others doing business with the FCC;
3. Files relating to FCC employees' hotline complaints and other miscellaneous complaints; and
4. Investigative reports and related documents, such as correspondence, notes, attachments, and working papers.

Authority for Maintenance of the System:

Inspector General Act of 1978, as amended.

Purpose(s):

Pursuant to the Inspector General Act of 1978, as amended, the system is maintained for the purposes of:

1. Conducting and documenting investigations initiated and/or referred by or to the OIG or other investigative agencies regarding FCC programs and operations and reporting the results of investigations to other Federal agencies, other public authorities or professional organizations that have the authority to bring criminal prosecutions or civil or administrative actions, or to impose other disciplinary sanctions;
2. Documenting the outcome of OIG investigations;
3. Maintaining a record of the activities that were the subject of investigations;
4. Reporting investigative findings to the Commission management about problems and deficiencies in the FCC's programs and operations or to suggest corrective action in reference to identified irregularities, problems or deficiencies;
5. Maintaining a record of complaints and allegations received relative to FCC programs and operations and documenting the outcome of OIG reviews of those complaints and allegations;
6. Coordinating relationships with other Federal agencies, State and local governmental agencies, and nongovernmental entities in matters relating to the statutory responsibilities of the OIG; and
7. Acting as a repository and source for information necessary to fulfill the reporting requirements of the Inspector General Act of 1978, as amended.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

The OIG may disclose information contained in a record in this system of records under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected:

1. Law Enforcement and Investigation--The OIG may disclose information from this system of records to any Federal, State, local, Tribal, or foreign agency or other public authority or professional organization responsible for administering, enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulations if that information is relevant to any remedial, enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity;
2. Disclosure to Public and Private Entities to Obtain Information Relevant to FCC Functions and Duties--The OIG may disclose information from this system to public or private sources to the extent necessary to obtain information from those sources relevant to an OIG investigation or inspection;
3. Adjudication and Litigation--The OIG may disclose a record from this system to the United States Department of Justice (DOJ), or other Federal, state, local or other authorities responsible for litigation or adjudication if relevant and

necessary to litigation or adjudication and disclosure is compatible with the purpose for which the records were collected. The OIG may make such a disclosure in the event that the one of the following parties is involved in the litigation or adjudication or has an interest in the litigation:

- (a) The FCC or any component or program of the FCC;
- (b) Any employee or agent of the FCC in his or her official capacity;
- (c) Any employee of the FCC in his or her individual capacity if the DOJ has agreed to represent the employee or in connection with a request for that representation; or
- (d) The United States, if the OIG determines that the litigation or adjudication is likely to affect the FCC;

4. Disclosure to Contractors and Consultants--The OIG may disclose a record from this system to the employees of any entity or individual with whom or with which the FCC contracts for the purpose of performing any functions or analyses that facilitate or are relevant to an OIG investigation, audit, inspection, or other inquiry. Before entering into such a contract, the OIG shall require the contractor to maintain Privacy Act safeguards, as required under the Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1 and 24.2) and include the specified contract clauses (Parts 52.224-1 and 52.224-2), as appropriate, to ensure that personal information by contractors who work on FCC-owned systems of records and the system data are protected as mandated;

5. Debarment and Suspension Disclosure--The OIG may disclose information from this system to the FCC or another Federal agency considering suspension or debarment action if the information is relevant to the suspension or debarment action. The OIG also may disclose information to the FCC or another agency to gain information in support of the FCC's own debarment and suspension actions.

6. Government-Wide Program Management and Oversight--The OIG may disclose a record from this system to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act or any other matter relevant to the FCC's programs or operations; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

7. Benefit Program Disclosure--The OIG may disclose a record from this system to any Federal, State, local, or other public authority, if relevant to the prevention or detection of fraud and abuse in benefit programs administered by any agency or public authority.

8. Financial Obligations Under the Debt Collection Acts--The OIG may disclose a record from this system to: other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996; any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government; prepare information on items considered income for taxation purposes to be disclosed to Federal, state, and local governments; or any Federal, State, local, or foreign agency, or other public authority, if relevant to the collection of other debts and overpayments owed to any agency or public authority.

9. Disclosure to the President's Council on Integrity and Efficiency (PCIE)--The OIG may disclose a record from this system to members and employees of the PCIE for the preparation of reports to the President and Congress on the activities of the Inspectors General;

10. Disclosure for Qualitative Assessment Reviews--The OIG may disclose a record from this system to members of the PCIE, the DOJ, the U.S. Marshals Service, or any Federal agency for the purpose of conducting qualitative assessment reviews of the investigative operations of the OIG to ensure that adequate internal safeguards and management procedures are maintained;

11. Breach of Federal Data--The OIG may disclose a record from this system to appropriate agencies, entities, and persons when (1) the OIG suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the OIG has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the FCC or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the OIG's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm; and

In each of these cases, the OIG will determine whether disclosure of the records is compatible with the purpose(s) for which the records were collected, *i.e.*, the OIG may make these disclosures on a case-by-case basis or, if the OIG has met the requirements of the Computer Matching and Privacy Protection Act, under a computer matching agreement.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in this information system consists of paper records, documents, and files in file folders and electronic records, files, and data that are stored in the OIG databases that are part of the FCC's computer network.

Retrievability:

Records, including both paper documents and files and electronic files and data, are filed alphabetically by name of the subject of the investigation or by a unique file number assigned to each investigation.

Safeguards:

The paper, diskette, and records contained in other media are kept in locked storage that is further secured at the end of each business day. Limited access to these records is permitted by those persons whose official duties require such access; thus, unauthorized examination during business hours would be easily detected.

The electronic records, files, and data are maintained in the FCC computer network databases. Access to the electronic files is restricted to authorized OIG supervisors and staff. Authorized OIG staff and OIG contractors and authorized staff and contractors in the FCC's Information Technology Center (ITC) have access to the electronic files on an "as needed" basis. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features to prevent unauthorized users from gaining access to the data and system resources. Backup tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

Investigative and other files are retained and disposed of in accordance with OIG's Records Retention Policy.

System Manager(s) and Address(es):

Office of Inspector General (OIG), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from the notification procedure for this system of records.

Record Access Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record access procedures for this system of records.

Contesting Record Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its contesting record procedures for this system of records.

Record Source Categories:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

Exemptions Claimed for the System:

This system of records is exempt from sections (c)(3), (d), (e)(4)(G), (e)(4)(H), and (e)(4)(I), and (f) of the *Privacy Act of 1974*, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the types of materials described in section (k) of the Privacy Act.

[\[Return to TOP\]](#)

FCC /OLA-1

System Name:

Legislative Management Tracking System (LMTS).

Security Classification:

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

System Location(s):

Office of Legislative Affairs (OLA), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in the Legislative Management Tracking System (LMTS) include members of the U.S. House of Representatives and the U.S. Senate, the President of the United States, the Vice President of the United States, members of the public at large, and FCC employees.

Categories of Records in the System:

The categories of records in the Legislative Management Tracking System (LMTS), including any attachments, may include:

1. Members of the public at large: individual's name, home address, home telephone number(s), personal cell phone number(s), account number(s) for telephone, cell phone, cable television, and satellite television services, and other, miscellaneous information that an individual may include in his/her Congressional (constituent) complaint(s) and/or consumer complaints, *etc.*; and
2. FCC employees: individual's name, home address, home telephone number(s), personal cell phone number(s), FCC employment records, and other miscellaneous, information that a Commission employee may include in a complaint to his/her Senator(s) and/or Congressional representative(s) and/or to the President and/or Vice President.

Authority for Maintenance of the System:

5 U.S.C. 301; 44 U.S.C. 3101; and 47 U.S.C. 154(i), (j), and (k), and 47 U.S.C. 155(a).

Purpose(s):

OLA uses the Legislative Management Tracking System (LMTS) to store, track, and manage correspondence from the members of the U.S. House of Representatives and the U.S. Senate and the President of the United States and the Vice President of the United States. This correspondence may include attachments that could contain PII from individuals (members of the public at large) who contacted their Congressional Representative(s) and/or Senator(s) and/or the President and/or the Vice President concerning various telecommunications issues affecting them, *e.g.*, telephone and cable bills, *etc.* In addition, FCC employees may be seeking Congressional assistance with their personal employment issues at the Commission, *e.g.*, hiring and promotion matters, *etc.*

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Congressional Inquiries--When requested by a Congressional office in response to an inquiry that an individual made to the Congressional office for his/her own records or for the adjudication of consumer complaints, *e.g.*, telephone and/or cable bills, *etc.*, or other miscellaneous FCC-related matters, such as licensing issues, *etc.*;
2. Executive Branch Inquiries--When requested by the Executive Branch of the U.S. Government in response to an inquiry that an individual made to the President of the United States and/or the Vice President of the United States in response to an inquiry that the individual made to the Executive Branch for assistance with various telecommunications issues affecting them;
3. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act; and
4. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely

upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information in the Legislative Management Tracking System (LMTS) includes paper documents, records, and files that are stored in file cabinets in the OLA office suite, and electronic records, files, and data that are stored in the FCC's computer network databases.

Retrievability:

Information in the Legislative Management Tracking System (LMTS) is retrieved by the correspondence log-in file number, Congressional Representative's name, and/or type of complaint, *etc.* Regardless of the circumstances, OLA always redacts the Social Security Number and birthdate before entering a document into LMTS. Other personally identifiable information (PII) in an attachment may also be redacted prior to filing the correspondence if it is not relevant to the complaint or inquiry.

Safeguards:

The paper documents are maintained in file cabinets that are located in the OLA office suite, whose access is through a card-coded main door. Access to these files is restricted to authorized OLA supervisors and staff.

Access to the electronic files, which are housed in the FCC's computer network databases, is restricted to authorized OLA supervisors and staff and to the Information Technology Center (ITC) staff and contractors, who maintain the FCC's computer network. 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. Information resident on the OLA database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

Pursuant to FCC records schedule N1-173-03-2, item 5, information in the Legislative Management Tracking System (LMTS) is retained at the FCC for three years after cut-off at the end of each calendar year. The documents relating to FCC policy, *e.g.*, Chairman correspondence, *etc.*, are then transferred to the National Archives and Records Administration (NARA). The paper documents, records, and files are destroyed by shredding. The electronic records, data, and files (electronic storage media) are destroyed physically or by electronic erasure.

System Manager(s) and Address(es):

Address inquiries to the Office of Legislative Affairs (OLA), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Office of Legislative Affairs (OLA), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Office of Legislative Affairs (OLA), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Office of Legislative Affairs (OLA), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in the Legislative Management Tracking System are the Congressional and Executive Branch correspondence, including attachments, which may include complaints related to telephone, wireless, and cable billing or service; licensing inquiries; or other inquiries on issues under FCC jurisdiction, *etc.*, submitted by constituents (members of the public at large); or personnel actions or complaints from constituents who are FCC employees.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-2

System Name:

Labor Relations and Employee Performance Files

Security Classification:

None.

System Location(s):

Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B104, Washington, DC 20554.

Categories of Individuals Covered by the System:

Current and former Federal Communications Commission (FCC) employees.

Categories of Records in the System:

This system contains a variety of records relating to formal and informal actions based on conduct or performance and also includes files dealing with grievances filed under the negotiated or administrative grievance procedures, requests for reconsideration, arbitrations, appeals, and miscellaneous inquiries and complaints. These records may include:

1. Case number, employee name, Social Security Number, grade, job title, and employment history; and
2. Copies of notices of proposed actions; materials relied on by the agency to support the proposed action; statements of witnesses; employee responses or appeals; transcripts; and agency decisions.

Authority for Maintenance of the System:

5 U.S.C. 35, 43, 61, 63, 71, 73, 75, and 77.

Purpose(s):

These records provide a method by which the FCC can maintain appropriate information on Commission employees for purposes such as litigation, law enforcement, congressional inquiries, labor organization inquiries, and government-wide program oversight.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
5. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit;
6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, foreign, tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization

may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action; and

7. Labor Relations--a record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions. In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

These records are maintained in file folders.

Retrievability:

These records are retrieved preliminarily by case number. An examination of case logs will disclose the name of an employee associated with a case number.

Safeguards:

These records are maintained in secured metal filing cabinets to which only authorized personnel have access.

Retention and Disposal:

Records in the following categories are disposed of at the end of the first fiscal year following completion of the fiscal year in which the action was taken:

1. Informal actions based on conduct or performance;
2. Oral admonishments confirmed in writing; and
3. Written reprimands.

Records pertaining to the following are disposed of at the end of the third fiscal year following completing of the fiscal year in which the action was taken:

1. Grievances processed under the negotiated or administrative grievance procedures;
2. Appeals;
3. Request for restoration of annual leave; and
4. Requests for admission to the agency's leave transfer program.

Records pertaining to the following matters are disposed of at the end of the fourth fiscal year following completion of the fiscal year in which the action was taken:

1. Within-grade increase denials/postponements;
2. Suspensions, removals, furloughs taken under authority of 5 U.S.C. chapters 35 and 75; and
3. Requests for reconsideration/review.

Records pertaining to the following matters are disposed of at the end of the fifth fiscal year following completion of the fiscal year in which the action was taken:

1. Removals, demotions, and reassignments based on unacceptable performance;
2. Arbitrations; and
3. Unfair labor practices.

Disposal is by shredding or burning.

System Manager(s) and Address(es):

Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B104, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Information in this system of records is provided by an individual on whom the record is maintained; testimony of witnesses; supervisors and managers; union officials; and arbitrators and other third-parties, *e.g.*, Department of Labor, Federal Labor Relations Authority, and Merit System Protection Board.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-3

System Name:

Federal Advisory Committee Membership File (FACA).

Security Classification:

None.

System Location(s):

1. General Files: Associate Managing Director--PERM, Office of Managing Director, Federal Communications Commission, 445 12th Street, SW., Room 1-C848, Washington, DC 20554.
2. Financial Disclosure Files: Office of General Counsel (OGC), 202-418-1712.
3. Committee-Specific Files: Files with more specific information are kept in the offices of the following Designated Federal Officials (DFO):
 - a. Advisory Committee for the 2007 World Radiocommunication Conference (WRC-2007): Designated Federal Officer (DFO: International Bureau; (202-418-7501).
 - b. Advisory Committee on Diversity for Communications in the Digital Age (Diversity): Designated Federal Officer (DFO: Vacant).
 - c. Consumer Advisory Committee (CAC): Designated Federal Officer (DFO: Consumer and Governmental Affairs Bureau; 202-418-2809).
 - d. Media Security and Reliability Council (MSRC): Designated Federal Officer (DFO: Media Bureau; 202-418-1600).
 - e. Network Reliability and Interoperability Council (NRIC): Designated Federal Officer (DFO: Office of Engineering and Technology; 202-418-1096).
 - f. North American Numbering Council (NANC): Designated Federal Officer (DFO: Wireline Competition Bureau; 202-418-0792).
 - g. Technological Advisory Council (TAC): Designated Federal Officer (DFO: Office of Engineering and Technology; 202-418-1096).
 - h. Katrina Independent Panel (Independent Panel): Designated Federal Officer (DFO: Enforcement Bureau; 202-418-7452).

Categories of Individuals Covered by the System:

Individuals who are members of Federal Advisory Committees sponsored or co-sponsored by the Federal Communications Commission (FCC).

Categories of Records in the System:

1. Individual advisory committee members' names, business addresses, e-mail addresses, business telephone numbers, and occupations or titles are kept with the members' respective advisory committee.
2. Copies or original financial disclosure forms (OGE-450), whenever they are necessary to be filed by committee members.

Authority for Maintenance of the System:

Federal Advisory Committee Act (5 U.S.C., Appendix).

Purpose(s):

This system of records is maintained in order to have current contact information about the members of the FCC's Federal Advisory Committees so that the FCC can communicate effectively and promptly with these individuals. The information in this system of records may also be used to complete mandatory reports to the Congress and GSA about Federal Advisory Committee matters. Finally, the information in this system of records may also be used by FCC employees to ensure compliance with all ethical and conflict-of-interest requirements relevant to the members of the FCC's Federal Advisory Committees.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Committee communication and reporting--a record in this system may be used to distribute information to members of each committee for purposes of conducting meetings and general committee business or to prepare reports on the membership and work of the committee;
2. Public Access--the public can access information about the FCC, and all other, Federal Advisory Committees with the searchable database found on the Government Service Administration's Web site at http://www.gsa.gov/Portal/gsa/ep/contentView.do?P=MC&contentId=14451&contentType=GSA_BASIC;
3. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
4. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
5. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
6. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in

the System:

Storage:

Paper records are maintained in file folders. Electronic data are stored on computer diskettes or in the FCC's computer database system.

Retrievability:

Records are grouped primarily by name of committee or subcommittee. Under this filing hierarchy, records can then be retrieved by name of committee member.

Safeguards:

Paper records are maintained in file cabinets, which are locked at the end of each business day. Electronic data are stored on computer diskettes in locked cabinets in offices, which are locked at the end of the business day, or in the FCC's computer database system, which is secured by passwords that are available only to authorized personnel whose duties require access.

Retention and Disposal:

Records are retained for six years following the dissolution of the Committee and then destroyed by shredding. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Associate Managing Director--PERM, Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C848, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Information provided by Committee members; developed as the result of the work of the Committees; and Designated Federal Officer (DFO) reporting on Committee membership and activities.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-6

System Name:

Financial Accounting Systems (FAS).

Security Classification:

None.

System Location(s):

Financial Operations Center, Associate Managing Director Financial Operations (AMD-FO), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A663, Washington, DC 20554.

Categories of Individuals Covered by the System:

Information from all Federal Communications Commission (FCC) databases that provide financial accounting data. These databases include, but are not limited to, the FCC's older Revenue Accounting Management Information System (RAMIS) and the newer Federal Financial System (FFS). The data include information on:

1. Individuals making payments to cover forfeitures assessed, fees collected, services rendered, and direct loans; refunds for incorrect payments or overpayments (including application processing fees, travel advances, advanced sick leave, and advanced annual leave);
2. Individuals receiving payments for services rendered and reimbursement of expenses incurred on FCC business, *e.g.*, travel costs;
3. Billing and collection of bad checks; and
4. Miscellaneous monies received by the Commission (including reimbursement authorized under the Travel Reimbursement Program covered by the government-wide systems of records: GSA/GOVT-3 and GSA/GOVT-4).

Categories of Records in the System:

Record categories include: individual's name, Social Security Numbers (SSN), Individual Taxpayer Information Numbers (ITIN), FCC Registration Numbers (FRN), telephone numbers, addresses of individuals, records of services rendered, loan payment information, forfeitures assessed and collected, amounts, dates, check numbers, bank deposit information, transaction type information, United States Treasury deposit numbers, and information substantiating fees collected, refunds issued, and interest, penalties, and administrative charges assessed to individuals. Forms associated with this system of records are FCC Forms 159, 159-W, and 1070.

Authority for Maintenance of the System:

5 U.S.C. Chapter 57; 31 U.S.C. 3302(e); 44 U.S.C. 3101, 3102, and 3309; the Debt Collection Act as amended by the Debt Collection Improvement Act of 1996; Section 639 of the Consolidated Appropriations Act of 2005 (P.L. 108-447) 31 U.S.C. 3302(e); Federal Financial Management Improvement Act of 1996; Chief Financial Officers Act of 1990; Federal Managers Financial Integrity Act of 1982; and Executive Order 9397.

Purpose(s):

These records are used:

1. To account for all monies paid and received by the FCC from the public and refunded to the public;
2. To compute vouchers to determine amounts claimed and reimbursed; and
3. To account for all advances given to employees.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--when using the automated reporting tools of Fee Filer and the Red Light Display System, individuals conducting business with the FCC can--using their FCC Registration Number and a password--access their own records in the Financial Accounting Systems to determine what fees they owe;
2. Financial obligations under the Debt Collection Acts--a record from this system may be disclosed to other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996. A record from this system may be disclosed to any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government. A record from this system may be used to prepare information on items considered income for taxation purposes to be disclosed to Federal, state, and local governments;
3. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
4. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
5. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
6. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;
8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--

disclosure may be made to a Federal, State, local, foreign, tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action; and

9. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions. In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

Disclosures pursuant to 5 U.S.C. 552a (b)(12): The Department of Treasury may disclose to a consumer reporting agency information regarding a claim by the Commission which is determined to be valid and overdue as follows: The name, address, SSN or ITIN, and other information necessary to establish the identity of the individual or organization responsible for the claim;

1. The amount, status, and history of the claim; and
2. The program under which the claim arose.

The Commission may disclose the information specified in this paragraph under 5 U.S.C. 552a (b)(12) and the procedures contained in subsection 31 U.S.C. 3711(e). A consumer reporting agency to which these disclosures may be made is defined at 31 U.S.C. 3701(a)(3).

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in paper files, computer printouts, microfilm, microfiche, magnetic disc and magnetic tape.

Retrievability:

Records in this system of records can be retrieved by name and/or type of transaction, call sign, processing number, SSN, ITIN, FRN, vendor code, Soundex number, fee control number, payment ID number, or sequential number.

Safeguards:

Records are located in secured metal file cabinets and metal vaults in secured rooms or secured premises, with access limited to those individuals whose official duties required access. Electronic record files are secured by passwords, which are available only to authorized personnel whose duties require access.

Retention and Disposal:

These records are retained at the FCC for two years following the end of the current fiscal year. They are then transferred to the Federal Records Center and destroyed by shredding when 6 years and 3 months old. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Financial Operations Center, Associate Managing Director--Financial Operations (AMD-FO), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A663, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Subject individual, Federal Reserve Bank, agent of subject, and Attorney-at-Law of the subject individual.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-7

System Name:

FCC Employee Transit Benefit and Parking Permit Programs.

Security Classification:

None.

System Location(s):

Administrative Services Center (ASC), Associate Managing Director--Administrative Operations (AMD-AO), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room TW-C201, Washington, DC 20554.

Information related to those employees who participate in the SmarTrip portion of the benefits program is also stored in a database administered by the Washington Metropolitan Area Transit Authority, headquartered at 600 Fifth Street, NW., Washington, DC 20001.

Categories of Individuals Covered by the System:

FCC employees who apply for and participate in the FCC Transit Benefit and Parking Permit Programs, *e.g.*, holders of parking permits and members of carpools and vanpools; recipients with handicap status for parking assignments; and applicants and recipients of fare subsidies issued by FCC.

Categories of Records in the System:

Information required to administer the Transit Benefit and Parking Permit Programs that serves to determine the applicant's qualification based on handicap status, to determine their mode of transportation to and from work, and to certify their monthly commuting cost to and from work. These records include the following:

1. Employee Transit Benefit Program applications, Transit Benefit certifications, change of information on Employee Transit Benefit Program application of the transit benefit recipients, parking applications, vanpool and carpool verification, employee parking rosters, employee handicap verification, and executive staff information.
2. Data regarding the organizational location, telephone number, FCC badge number, home address, vehicle make/model, license plate number, handicap status documents, van/carpool information, executive status, mode of transportation and monthly cost of transportation of any applicant who has submitted an application for the Transit Benefit and/or Parking Permit Programs.
3. Records and reports of disbursements to transit benefit recipients, parking permit recipients, handicap status, and information on local public mass transit facilities.

Forms associated with this system of records include A-27, A-75, and A-75A.

Authority for Maintenance of the System:

Statutory authority to provide public transportation, parking records, and handicap parking services is derived from 5 U.S.C. 7901 and 7905, 5 U.S.C. 301, and Executive Order 13105.

Purpose(s):

1. These records are used to support the FCC's program that provides allowed transportation and parking subsidies to Federal employees.
2. This information is also used for auditing purposes to ensure the accuracy and integrity of the program, to qualify and to certify beneficiaries of the program, and to prepare listings and reports for use by the FCC and the other Federal, state, and local agencies charged with oversight of or contribution to the program.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Financial obligations as required by the National Finance Center *et al.*--when the National Finance Center (the FCC's designated payroll office), the Department of the Treasury Debt Management Services, and/or a current employer to effect a salary, IRS tax refund, or administrative offset to satisfy an indebtedness; and to Federal agencies to identify and locate former employees for the purposes of collecting such indebtedness, including through administrative, salary, or tax refund offsets. Identifying and locating former employees, and the subsequent referral to such agencies for offset purposes, may be accomplished through authorized computer matching programs. Disclosures will be made only when all procedural steps established by the Debt Collection Act of 1982 and the Debt Collection Improvement Act of 1996 or the Computer Matching and Privacy Protection Act of 1988 as appropriate, have been taken;
2. Program partner--when information is disclosed to the Washington Metropolitan Area Transit Authority (WMATA) in connection with employees participating in their SmarTrip program (<http://www.wmata.com/riding/smartrip.cfm>);

3. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act; and

6. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in file folders, in the transit benefit and parking permit computer databases, and in the Washington Metropolitan Area Transit Authority database associated with the SmartTrip program.

Retrievability:

Records are retrieved by the employee's name, or by the FCC Badge identification number, tag, and/or permit number.

Safeguards:

Records are maintained in a secured area and are available only to authorized personnel, *e.g.*, FCC and contract personnel, whose duties require access. Computer databases are setup with a secured password. File cabinets where the records are stored are controlled by on-site personnel when unlocked and locked when not in use. All transit benefits and parking permits are kept in a locked cash box contained in a (cylinder lock) drawer. At close of business, the cash box is secured in a government issued safe with a combination lock.

Retention and Disposal:

Records under the control of the FCC are retained for three years in accordance with the General Records Schedule 6 established by the National Archives and Records Administration at <http://www.archives.gov/records-mgmt/ardor/grs06.html>. Records are then shredded. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Administrative Services Center (ASC), Associate Managing Director-Administrative Operations (AMD-AO), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room TW-C201, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Information is obtained from applications submitted by individuals for the Transit Benefit and Parking Permit Programs.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-9

System Name:

Commission Registration System (CORES).

Security Classification:

None.

System Location(s):

Financial Operations Center, Associate Managing Director--Financial Operations (AMD-FO), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A625, Washington, DC 20554.

Categories of Individuals Covered by the System:

Information on individuals who have requested a Federal Communications Commission (FCC) Registration Number (FRN) from the Commission Registration System (CORES). A FRN is mandatory for those wishing to conduct business with the Federal Communications Commission.

Categories of Records in the System:

Records include: names, address(es), Social Security Numbers (SSN), Individual Taxpayer Identification Numbers (ITIN), FCC Registration Numbers (FRN), telephone number(s), fax number(s), and e-mail address(es). The FRN paper-based registration forms are FCC Forms 160, 161, and 162.

Authority for Maintenance of the System:

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; the Federal Financial Management Improvement Act of 1996; the Chief Financial Officers Act of 1990; and the Federal Managers Financial Integrity Act of 1982.

Purpose(s):

The primary use of the records contained in this database is to develop and maintain a Commission-wide method of recognizing and interacting with those individuals who are doing business with the Commission as defined in 31 U.S.C. 7701(c)(2) and who incur application or regulatory fee obligations. This FRN registration number collaterally allows the Commission to ensure that monies paid are properly matched with debts and obligations due (see FCC/OMD-6 for the system of records covering these activities).

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--a search on the Commission's CORES Web site at <https://svartifoss2.fcc.gov/coresWeb/publicHome.do> can be conducted by using an individual's last name and would result in a list of all those registered with the FCC under that last name, as well as the associated FRN, address, and registration date unless such information is routinely withheld under 47 CFR 0.457 or a request has been made or granted to give the information confidential treatment under 47 CFR 0.459;
2. Financial obligations under the Debt Collection Acts--a record from this system may be disclosed to other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996. A record from this system may be disclosed to any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government. A record from this system may be used to prepare information on items considered income for taxation purposes to be disclosed to Federal, state, and local governments;
3. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
4. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute,

regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

5. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

6. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

CORES is a computer database. Information in this system of records is stored primarily on computer hard drives. Secondly, some information from this system of records may also be maintained in paper files, computer printouts, or magnetic tape.

Retrievability:

Records in this system of records can be retrieved by name and/or type of transaction, processing number, SSN, ITIN, FRN, or sequential number.

Safeguards:

Records are located in secured metal file cabinets, metal vaults, and in metal file cabinets in secured rooms or secured premises, with access limited to those individuals whose official duties required access. Electronic record files are secured by passwords, which are available only to authorized personnel whose duties require access. Data resident on network servers are backed-up daily to magnetic media. One week's worth of back-up tapes is stored on-site in fireproof safes. Each week, the previous week's backup tapes are sent to an off-site storage location. A maximum of ten week's tapes are kept and cycled in this fashion.

Retention and Disposal:

Records are retained for two years following the end of the current fiscal year; then transferred to the Federal Records Center where they are destroyed by shredding when 6 years and 3 months old. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Financial Operations Center, Associate Managing Director--Financial Operations (AMD-FO), Office of Managing

Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A663, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Subject individual, agent of subject, and Attorney-at-Law of the subject individual.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-12

System Name:

Integrated Library System (ILS) Records.

Security Classification:

None.

System Location(s):

FCC Library, Office of the Secretary, Office of Managing Director (OMD), 445-12th Street, SW., Room TW-B505, Washington, DC 20554.

Categories of Individuals Covered by the System:

Information on current Federal Communications Commission (FCC) employees who have registered as library users.

Categories of Records in the System:

Information on checked-out and/or checked-in items contained in the FCC Library collection. The records may include such information as the individual's name, organizational unit, telephone number, room number, building access badge number, library barcode identifier, and position title.

Authority for Maintenance of the System:

44 U.S.C. 3101 and 47 U.S.C. 154(I).

Purpose(s):

The information is maintained and used to keep track of items borrowed by registered users from the FCC Library's collection and to ensure that all items are returned to the FCC Library in a timely manner and/or upon a FCC employee's resignation from the Commission.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to an FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained electronically in the Integrated Library System (ILS) database. The database is password protected and updated daily.

Retrievability:

The system records of borrowed items may be retrieved by the patron's name, bureau/office, office telephone number,

room number, barcode number, and position title.

Safeguards:

Information in the Integrated Library System (ILS) is secured through controlled access and passwords restricted to administrative office personnel. Data resident on network servers are backed-up routinely onto magnetic media. Back-up tapes are stored on onsite and at an off site storage location.

Retention and Disposal:

The retention schedule for this system of records has not yet been determined. No records will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Assistant Secretary, Office of the Secretary, Office of Managing Director (OMD), 445 12th Street, SW., Room TW-B505, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

FCC employees who provide contact information in order to checkout materials from the FCC library and the FCC Library collection inventory.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-13

System Name:

Data Quality Comments.

Security Classification:

None.

System Location(s):

Associate Managing Director--Performance Evaluation and Records Management (AMD-PERM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A838, Washington, DC 20554.

Categories of Individuals Covered by the System:

Members of the public who have submitted comments or questions through the Data Quality comments process.

Categories of Records in the System:

Comments received through the FCC's Data Quality Comment process and, where appropriate, materials that are associated with the resolution of those comments.

Authority for Maintenance of the System:

Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554).

Purpose(s):

The Data Quality Act of 2001 and OMB's implementing regulations mandate that agencies develop and make public guidelines for commenting on information disseminated by that Federal agency. Further, OMB requires that Federal agencies publicly post on their Web sites the comments deemed to meet the agency standards and the resolution of those comments. This system of records maintains the comments received from the public since the inception of this requirement in FY03.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--in accordance with OMB's requirements (OMB Memorandum from John Graham, August 30, 2004, "Posting of Information Quality Correction Requests and Responses" found at http://www.whitehouse.gov/omb/inforeg/info_quality_posting_083004.pdf), the complete set of correspondence with a qualifying Data Quality commenter is available on the FCC's Data Quality Internet site at: <http://www.fcc.gov/omd/dataquality/>.
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The paper copy of comments is kept in a manila folder in a private office. The electronic copy of actual comments is posted on the FCC Web site.

Retrievability:

Records are retrievable primarily by date of submittal. Under this hierarchy, records are retrievable by name of individual requester.

Safeguards:

Paper records are kept in a private office that is locked at the end of the day. Electronic records are posted on the FCC web site, and thus, are publicly available.

Retention and Disposal:

The retention schedule for this system of records has not yet been determined. No records will be destroyed until a disposal schedule is approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Associate Managing Director--Performance Evaluation and Records Management (AMD-PERM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A838, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Data Quality comments submitted by members of the public; correspondence involved in resolving comments; and annual reports to OMB.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-15

System Name:

Employee Locator System.

Security Classification:

None.

System Location(s):

Assistant Managing Director--Human Resources Management (AMD-HRM), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A100, Washington, DC 20554.

Categories of Individuals Covered by the System:

Employees of the Federal Communications Commission (FCC) and the persons they list as their "emergency contacts."

Categories of Records in the System:

The information includes:

1. The names of FCC employees along with contact information on their organizational unit, physical location (floor, room number), and work telephone number(s); and
2. The name(s), e-mail address(es), and telephone number(s) of the individual(s) to contact in the event of a medical or other emergency involving the FCC employee.

Authority for Maintenance of the System:

Homeland Security Act of 2002 (P.L. 107-296, 2002); Executive Order (EO) 12656, Assignment of Emergency Preparedness Responsibilities, November 18, 1988; and Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government Operations, October 21, 1998.

Purpose(s):

The information serves to identify the individual(s) to contact should an emergency of a medical or other nature involving the Commission employee occur while the employee is on the job.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Emergency Response--A record on an individual in this system of records may be disclosed to emergency medical personnel, *e.g.*, doctors, nurses, and/or paramedics, or to law enforcement officials in case of a medical or other emergency involving the FCC employee without the subsequent notification to the individual identified in 5 U.S.C. 552a(b)(8);
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Electronic records are maintained in a network computer database.

Retrievability:

Records are retrieved by the employee's name, organizational unit, floor, and room number.

Safeguards:

Electronic records are maintained in a network computer database, which is secured through controlled access and passwords restricted to the employee, Human Resources Management employees, administrative personnel, and emergency relocation site employees.

Retention and Disposal:

Records kept by the FCC are maintained and disposed of in accordance with General Records Schedule 1 issued by the National Archives and Records Administration (NARA). Under terms of this Schedule, records are destroyed on separation or transfer of the employee by means of shredding. Electronic records are destroyed physically (electronic storage media) or by electronic erasure. Individuals may request a copy of the disposition instructions from the FCC Privacy Act Officer or access this Schedule at <http://www.archives.gov/records-mgmt/ardor/grs01.html>.

System Manager(s) and Address(es):

Associate Managing Director--Human Resources Management (AMD-HRM), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A100, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Subject employees.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-16

System Name:

Personnel Security Files. Note: This system of records was formerly titled "Personnel Investigation Records."

Security Classification:

Most personnel identity verification records are not classified. However, in some cases, records of certain individuals, or portions of some records may have national defense/foreign policy classifications.

System Location(s):

Security Operations Center, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Categories of Individuals Covered by the System:

Information includes:

1. Current and former Federal Communications Commission (FCC) employees, including Commission retirees and those who resigned from the Commission, other Federal employees, applicants for employment in the Federal service or contracts, contractors of the FCC, experts, instructors, consultants to FCC and other Federal programs, visitors, and all others who may require regular, on-going access to FCC and other Federal facilities, information technology systems, or information classified in the interest of national security, and individuals formerly in any of these positions;
2. Individuals who are authorized to perform or to use services provide in FCC facilities, *e.g.*, FCC credit union and employee assistance program staff (EAP); and
3. Individuals who are neither applicants nor employees of the Federal Government, but who are or were involved in Federal programs under a co-operative agreement, *e.g.*, students and interns.

Categories of Records in the System:

Information includes:

1. Data needed to identify an individual, including: Individual's last, first, middle names (filed alphabetically by last name), and former name(s) (as applicable); Social Security Number; date of birth; birthplace; home address; home telephone number(s); residential history; organizational unit; position title;
2. Individual's citizenship; security classification; types and dates of investigations; and agency conducting investigation, investigation dates, security clearance(s) and grant date(s), and position sensitivity level(s); and miscellaneous investigation comments;
3. Names of relatives; birth date(s), home address, and citizenship; relatives who work for the Federal government;
4. Reports about the individual's qualifications for a position, *e.g.*, employee/applicant's employment/work history, summary report of investigation, results of suitability decisions, employment references and contact information; and educational/training institutions attended, degrees and certifications earned, and educational and training references;
5. Information needed to investigate an individual's character, conduct, and behavior in the community where he or she lives or lived; criminal history, *e.g.*, arrests and convictions for violations against the law; mental health history; drug use; financial information, *e.g.*, income tax return information and credit reports; reports of interviews with present and former supervisors, co-workers, associates, educators, and other related personal references and contact information;
6. Reports of inquiries with law enforcement agencies, employers, and reports of action after the Office of Personnel Management or FBI Section 8(d) Full Field Investigation; Notices of Security Investigation and other information developed from the above described Certificates of Clearance, *e.g.*, date of security clearances, requests for appeals, witness statements, investigator's notes, security violations, circumstances of violations, and agency action(s) taken;
7. Information needed to investigate allegations of FCC employee's misconduct;
8. Information needed to investigate miscellaneous complaints not covered by the FCC's formal or informal grievance procedure;

9. Information needed to conduct inquiries under the "President's Program to Eliminate Waste and Fraud in Government;" and

10. Information needed to investigate violence, threats, harassment, intimidation, or other inappropriate behavior causing an FCC employee, contractor, or visitor(s) to fear for his/her personal safety in the FCC workplace: Case number, victim's name, office telephone number, room number, organizational unit, duty station, position, supervisor, supervisor's telephone number, location of incident, activity at time of incident, circumstances surrounding the incident, perpetrator, name(s) and telephone number(s) of witness(es), injured party(s), medical treatment(s), medical report, property damages, report(s) to police and/or Federal Protective Services, and related miscellaneous information.

11. Information obtained from SF-85, SF-85P, SF-86, and SF-87 forms; summary reports from OPM or another Federal agency conducting background investigations; and results of adjudications and security violations. (**Note:** This system of records does not duplicate or supersede the Office of Personnel Management (OPM) Central-9 system of records, which covers the investigations OPM and its contractors conduct on behalf of other agencies.)

Authority for Maintenance of the System:

Depending upon the purpose(s) for the investigation, the U.S. government is authorized to ask for this information under 5 U.S.C. 1303, 1304, 3301, 7902, 9101; 42 U.S.C. 2165 and 2201; 50 U.S.C. 781 to 887; 5 CFR Parts 5, 732, and 736; Executive Orders 9397, 10450, 10865, 12196, 12333, 12356, and 12674; and Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

Purpose(s):

FCC Security Officer and the Personnel Security Specialist use this information to document and support decisions:

1. To determine compliance with Federal regulations and/or to make a determination about an individual's suitability, eligibility, and fitness for Federal employment, access to classified information or restricted areas, position sensitivity, security clearances, evaluations of qualifications, and loyalty to the United States, and to document such determinations;
2. To evaluate an applicant's qualifications and suitability to perform contractual services for the U.S. Government and to document such determinations;
3. To evaluate the eligibility and suitability of students, interns, or volunteers to the extent that their duties require access to FCC and other Federal facilities, information, systems, or applications, and to document such determinations;
4. To respond to a written inquiry conducted under the "President's Program to Eliminate Waste and Fraud in the Government;"
5. To take action on, or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees, and to counsel employees; and
6. To document security violations and supervisory actions taken.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Litigation by the Department of Justice--when (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose

compatible with the purpose for which the FCC collected the records.

2. A Court or Adjudicative Body--in a proceeding when: (a) The FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;

3. Law Enforcement and Investigation--except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, otherwise, responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity.

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration or the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act, or when necessary to the review of private relief legislation pursuant to OMB Circular A-19;

6. Contract Services, Grants, or Cooperative Agreements--a record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, or local government maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the FCC or to another Federal agency for criminal, civil, administrative personnel, or regulatory action;

8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, or tribal government, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the FCC or to another Federal agency for criminal, civil, administrative personnel, or regulatory action.

9. Labor Relations--disclosure may be made to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

10. National Security and Intelligence Matters--disclosure of these records may be disclosed to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign government in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information is stored on paper records, which are stored in file folders in security containers, and in electronic records that are maintained in a stand-alone computer database.

Retrievability:

Records are retrieved by an individual's name or Social Security Number (SSN).

Safeguards:

Comprehensive paper records are maintained in file folders and stored in approved security containers, which are locked and located within a secure, access-controlled area. Access is limited to approved security office and administrative personnel who have a need for them in the performance of their official duties, *e.g.*, who have responsibility for suitability determinations. Paper records limited (in number and scope) are kept in the FCC's regional offices and laboratory facilities in locked metal file cabinets in locked rooms.

Comprehensive electronic records are maintained in networked computer database(s). The computer database is secured through controlled access and passwords restricted to Federal employee and contractor security and administrative personnel on a "need to know" basis, *e.g.*, who have a need for them in the performance of their official duties, *e.g.*, who have responsibility for suitability determinations. Access to the records is restricted to those with a specific role in the Personal Identification Verification (PIV) process that requires access to background investigation forms to perform their duties, and who have been given a password to access that part of the system including background investigation records. The FCC Security Office staff maintains an audit trail. Individuals given roles in the PIV process must complete training specific to their roles to ensure that they are knowledgeable about how to protect individually identifiable information. The databases are backed-up on a daily basis to floppy disk(s), which are then stored in a secured area.

Retention and Disposal:

These records are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by the National Archives and Records Administration (NARA). Both paper and electronic records are retained during employment or while an individual is actively involved in Federal programs. As appropriate, records are returned to investigating agencies after employment terminates; otherwise, the records are destroyed upon notification of death or not later than five years after the employee's retirement or separation from the FCC, or the employee's transfer to

another Federal agency or department, whichever is applicable.

In accordance with NARA guidelines, the FCC destroys paper records by shredding; and electronic records are destroyed by electronic erasure. Individuals interested in further information about retention and disposal may request a copy of the disposition instructions from the FCC Privacy Act Officer.

System Manager(s) and Address(es):

Security Operations Center, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Notification Procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its notification procedure for this system of records.

Record Access Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record access procedures for this system of records.

Contesting Record Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its contesting record procedure for this system of records.

Record Source Categories:

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

Exemptions Claimed for the System:

This system of records is exempt from sections (c)(3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;
2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act; and
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended. (Information will be withheld to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the background investigation.)

[\[Return to TOP\]](#)

System Name:

Freedom of Information Act (FOIA) Case Files.

Security Classification:

None.

System Location(s):

FOIA Public Liaison, Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C, Washington, DC.

Categories of Individuals Covered by the System:

Individuals who have requested access to inspect and/or copy records of the Commission under provisions of the FOIA.

Categories of Records in the System:

Records in this system include names, addresses, the information requested under FOIA, and communications between the Federal Communications Commission (FCC) and the individual who makes the FOIA request ("requester").

Authority for Maintenance of the System:

Freedom of Information Act (1994 and Supp. II 1996), 5 U.S.C. 552, Executive Order (EO) 13392.

Purpose(s):

These records are collected and maintained so that the FCC can effectively, efficiently, responsively, and appropriately respond to FOIA requests. These records are also crucial for adjudication of FOIA appeals and for providing mandatory statistical reports to Congress, the Department of Justice, and the Office of Management and Budget. These records also advise Commission decisions on what records should be routinely made public and thus available with FOIA requests.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--where the appropriate official of the Commission, pursuant to the Commission's FOIA Regulations determines that it is in the public interest to disclose a record, which is otherwise exempt from mandatory disclosure, disclosure may be made from the system of records.
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for

investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information includes both paper files and electronic data. The information is maintained in case files and in databases located in both the FOIA Officer's organizational unit and the organizational units of the FCC staff providing the substantive answer to the request.

Retrievability:

Records are primarily indexed and retrieved by the FOIA control number assigned to each requester. In addition, records can be retrieved by name of requester, date of request, subject of request, and type of request.

Safeguards:

Paper records are maintained in file cabinets located in the organizational unit of those involved in responding to the FOIA request. Electronic records and databases are secured through controlled access and passwords, which is restricted to approved personnel in the bureaus and offices.

Retention and Disposal:

Individual case files are maintained for two years after the date of reply. Denied requests and appeals of denials may be retained for longer periods (up to six years after final action) in accordance with FOIA and FCC records control schedules. Individuals may request a copy of the disposition instructions from the FCC Privacy Act Officer.

System Manager(s) and Address(es):

FOIA Public Liaison, Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A827, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Individuals making requests under FOIA; communication between FCC organizational units and the requester; and investigative materials and decisions involved in appeals of FOIA responses.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-18

System Name:

Telephone Call Detail.

Security Classification:

None.

System Location(s):

Information Technology Center, Associate Managing Director--Information Technology (AMD-IT), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C361, Washington, DC 20554.

Categories of Individuals Covered by the System:

Information includes the following:

1. Individuals, including current and former employees, contractors, and visitors, who originate calls from Federal Communications Commission (FCC) telephones, including both wireline and cellular telephones, and individuals receiving such calls;
2. Individuals placing calls to or charging calls to FCC telephones (wired or cellular);
3. Individuals receiving such calls, or accepting the charges; and
4. Employees assigned FCC telephone numbers from both wireline and cellular telephones.

Categories of Records in the System:

Records in the system include:

1. Records of telephone calls placed to and from FCC phones (wired or cellular);
2. Telephone numbers, including both wireline and cellular telephones, assigned to current employees;
3. The physical location of FCC telephones, including both wireline and cellular telephones;
4. Numbers called from, the numbers called to, time and date of calls, duration, disposition, and the cost of the call and/or charges accepted, and the FCC organizational unit to which the relevant telephone numbers are assigned;
5. Copies of related records, *e.g.*, any periodic summaries which may have been compiled to reflect the total number of long distance calls; and
6. Names of employees and their office locations, but no other personal identifiers such as social security numbers.

Authority for Maintenance of the System:

44 U.S.C. 3101 and 47 U.S.C. 154(I).

Purpose(s):

Information is collected so that the FCC can meet its statutory and regulatory duties to ensure that government property is used only for allowed purposes and to ensure that the FCC operates efficiently and effectively.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Financial obligations as required by the National Finance Center *et al.*--when the National Finance Center (the FCC's designated payroll office), the Department of the Treasury Debt Management Services, and/or a current employer to effect a salary, IRS tax refund, or administrative offset to satisfy an indebtedness incurred for unofficial telephone and cellular calls; and to Federal agencies to identify and locate former employees for the purposes of collecting such indebtedness, including through administrative, salary, or tax refund offsets. Identifying and locating former employees, and the subsequent referral to such agencies for offset purposes, may be accomplished through authorized computer matching programs. Disclosures will be made only when all procedural steps established by the Debt Collection Act of 1982 and the Debt Collection Improvement Act of 1996 or the Computer Matching and Privacy Protection Act of 1988 as appropriate, have been taken;
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, foreign, or tribal or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action; and

8. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in electronic databases, in paper files, and on CD-ROM. The electronic databases are password protected and updated daily.

Retrievability:

Telephone call records are retrieved by organizational unit, the employee name, name of recipient of telephone call, and the telephone number.

Safeguards:

Paper and CD-ROM records are maintained in file cabinets, which are locked at the end of the business day. Information in the electronic databases is secured through controlled access and passwords restricted to administrative office personnel. Data resident on network servers are backed-up daily to magnetic media. Back-up tapes are stored on-site and at an off-site storage location.

Retention and Disposal:

Records kept by the FCC are maintained and disposed of in accordance with General Records Schedule 12 issued by the National Archives and Records Administration (NARA). Disposition is done by shredding when records are from 6 months to 3 years old, depending on the Schedule. Electronic records are destroyed physically (electronic storage media) or by electronic erasure. Individuals may request a copy of the disposition instructions from the FCC Privacy Act Officer or directly access the Schedule at <http://www.archives.gov/records-mgmt/ardor/grs12.html>.

System Manager(s) and Address(es):

Information Technology Center, Associate Managing Director--Information Technology (AMD-IT), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C361, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Telephone assignment records; call detail listings; and the results of administrative inquiries relating to assignment of responsibility for placement of specific long distance calls.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-19

System Name:

Denial of Federal Benefits (Drug Debarment List).

Security Classification:

None.

System Location(s):

Financial Operations Center, Associate Managing Director--Financial Operations (AMD-FO), Office of Managing

Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A663, Washington, DC 20554.

Categories of Individuals Covered by the System:

Individuals convicted of offenses concerning the distribution or possession of controlled substances, who have been denied all Federal benefits or Federal Communications Commission (FCC) benefits as part of their sentence pursuant to Section 5301 of the Anti-Drug Abuse Act of 1988, and who have also filed applications for any FCC professional or commercial license.

Categories of Records in the System:

The records within this system come from a database of individuals who have been denied all Federal benefits pursuant to Section 5301 of the Anti-Drug Abuse Act of 1988. This database is provided to the FCC by the Department of Justice (DOJ). These records include:

1. DOJ identification number (ID) for the person denied Federal benefits;
2. Name of individual;
3. Individual Taxpayer Identification Number (ITIN); and
4. Starting and ending date of the denial of Federal benefits.

All other data elements in the database are immediately discarded by the FCC.

When there is a preliminary match of name and ITIN from the database with the name of an application on file with the FCC, the FCC will then obtain from DOJ additional data elements, *e.g.*, address, zip code, and, if required by the FCC application, date of birth, in order to determine if there is an actual match.

If manual comparison of the application information with the information obtained from DOJ confirms an actual match, the FCC will prepare a confirmation report to be attached to the application. The confirmation report will reflect the identifying information obtained from the DOJ debarment entry, but it will not include the DOJ ID number for that debarment entry.

Upon such a match, the FCC will initiate correspondence with the applicant, which will also be associated with the application. The confirmation report and any correspondence with the applicant will be among the records found in this system.

Authority for Maintenance of the System:

Section 5301 of the Anti-Drug Abuse Act of 1988 (P.L. 100-690), as amended by section 1002(d) of the Crime Control Act of 1990 (P.L. 101-647), and 47 U.S.C. 154(i) and 154(j).

Purpose(s):

Information is used for the exchange of information between DOJ and the FCC in connection with the implementation of section 5301 of the Anti-Drug Abuse Act of 1988. This exchange of information permits the FCC to perform the General Services Administration (GSA) Debarment List check as provided for in the Office of National Drug Control Policy plan for implementation of section 5301 through use of information generated by DOJ. The automated records obtained from DOJ is only used by the FCC to make an initial determination of whether an individual applicant is subject to a denial of all Federal benefits or FCC benefits imposed under section 5301 of the Anti-Drug Abuse Act of 1988.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public Access--any report resulting from a confirmed match between a FCC applicant and an individual on the DOJ Drug Disbarment List (not including the DOJ ID Number) and any correspondence with the applicant regarding this match will be associated with the applicant's application and thus, will be made routinely available (with redactions for date of birth and Social Security Number) for public inspection as part of the FCC application file;
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained electronically on a computer database, and a paper copy of each record is stored in file folders.

Retrievability:

Records are retrieved by supplying the following information: Name of applicant, ITIN, address (in some instances) and zip code, date of birth (in some instances), and FCC fee control number for the application.

Safeguards:

The data are provided to the FCC by the U.S. Department of Justice (DOJ) and will be protected from tampering, unauthorized disclosure, and will follow these procedures:

1. The database will be processed to extract the information to be used in the automated system, and the data elements not being used in the automated system will be electronically erased.
2. The remaining data will be maintained at the main FCC building with a low risk of unauthorized access.
3. Access points are photo-monitored by security personnel; all employees are required to display photo ID badges; and all visitors must register and wear a visitor's badge.
4. Access to the computer system on which the extracted database is stored requires use of a unique user ID with personal identifier.
5. The extracted database is stored in a separate file in that system, and a separate password is required for entry to that file.
6. The password is available to a limited number of persons based strictly on a "need to know" basis.
7. The reports of any automated matches containing the DOJ ID number will be made available only to the appropriate FCC officials.

Retention and Disposal:

The match reports are retained by the FCC for only as long as it is necessary to obtain the debarment entry information and corresponding application for manual confirmation of the match. Thereafter, the match reports will be shredded.

However, periodically, a match report will be randomly retained for a period of an additional 90 to 120 days to provide a quality check of the verification process. Where the verification process establishes that a match does not indicate that the applicant has been denied Federal benefits under section 5301, the debarment entry information used in that determination will be retained by the FCC for 30 days after the application has cleared the debarment check. However, as noted above, debarment entry information relating to match reports that are retained for quality control purposes will be retained until that quality check is completed.

Where a match is confirmed by the manual verification process, the debarment entry information will be retained for a period of at least 90 days after the date of the letter referred to above. If the individual applicant contests the determination that a section 5301 denial of Federal benefits bars a grant of the application, the debarment entry information will be retained until such time as the FCC's action on the application is no longer subject to review in any court.

Individuals may request a copy of the disposition instructions from the FCC Privacy Act Officer.

System Manager(s) and Address(es):

Associate Managing Director--Financial Operations (AMD-FO), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-A623, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

DOJ Drug Disbarment Database; and individuals making applications to the FCC who have been matched with the Drug Disbarment Database.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-20

System Name:

Inter-office and Remote Access Internet E-mail Systems.

Security Classification:

None.

System Location(s):

Information Technology Center, Associate Managing Director--Information Technology (AMD-IT), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C266, Washington, DC 20554.

Categories of Individuals Covered by the System:

Employees and contractors of the Federal Communications Commission (FCC).

Categories of Records in the System:

Information includes the names, e-mail addresses, passwords, and badge numbers of all FCC employees and contractors.

Authority for Maintenance of the System:

47 U.S.C. 154(i).

Purpose(s):

These records are used to insure that all users of the FCC's Inter-office and Internet E-mail systems abide by the FCC's Intranet and Internet regulations. The records can also be used to identify possible abusers.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
5. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;
6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, foreign, tribal or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action; and
7. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in an electronic database.

Retrievability:

Records can be retrieved by organizational unit, employee name, and employee computer system log-in name.

Safeguards:

Information in the database is secured through controlled access and passwords restricted to administrative office personnel. Data resident on network servers are backed-up daily to magnetic media. Back-up tapes are stored on-site and at an off-site storage location.

Retention and Disposal:

Records kept by the FCC are maintained and disposed of in accordance with General Records Schedule 12 issued by the National Archives and Records Administration (NARA). Records are retained until an employee or contractor leaves the FCC and then shredded. Electronic records are destroyed physically (electronic storage media) or by electronic erasure. Individuals may request a copy of the disposition instructions from the FCC Privacy Act Officer or access the Schedule directly at <http://www.archives.gov/records-mgmt/ardor/grs12.html>.

System Manager(s) and Address(es):

Information Technology Center, Associate Managing Director--Information Technology (AMD-IT), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C266, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Access by employees and contractors to the FCC's Inter-office and Internet E-mail systems.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

System Name:

Equipment Loan Records.

Security Classification:

None.

System Location(s):

Information Technology Center, Associate Managing Director--Information Technology (AMD-IT), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C361, Washington, DC 20554.

Categories of Individuals Covered by the System:

Information concerning any individual loaned electronic equipment, *e.g.*, laptops, pagers, cellular telephones, and RSA Secure Tokens by the Federal Communications Commission (FCC) for use in carrying out FCC business.

Categories of Records in the System:

Information includes the following:

1. Individual's name, FCC I.D. badge number, and organizational unit; and
2. Loaned equipment's barcode number, serial number, model number, and modem number.

Authority for Maintenance of the System:

44 U.S.C. 3101 and 47 U.S.C. 154(I).

Purpose(s):

These records allow the FCC to meet its statutory and regulatory duties to ensure that government property is used only for allowed purposes; to ensure that government-purchased property is properly inventoried and accounted for; and to ensure that the FCC operates efficiently and effectively.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Financial obligations as required by the National Finance Center *et al.*--when the National Finance Center (the FCC's designated payroll office), the Department of the Treasury Debt Management Services, and/or a current employer to effect a salary, IRS tax refund, or administrative offset to satisfy an indebtedness incurred for unofficial telephone and cellular calls; and to Federal agencies to identify and locate former employees for the purposes of collecting such indebtedness, including through administrative, salary, or tax refund offsets. Identifying and locating former employees, and the subsequent referral to such agencies for offset purposes, may be accomplished through authorized computer matching programs. Disclosures will be made only when all procedural steps established by the Debt Collection Act of 1982 and the Debt Collection Improvement Act of 1996 or the Computer Matching and Privacy Protection Act of 1988 as appropriate, have been taken;

2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, foreign, tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action; and

8. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in paper files and in electronic databases. The databases are password protected and updated daily.

Retrievability:

Equipment loan records are retrieved by the employee name, equipment barcode number, serial number, and model or modem numbers.

Safeguards:

Paper and CD-ROM records are maintained in file cabinets that are locked at the end of the business day. Information in the databases is secured through controlled access and passwords restricted to administrative office personnel. Data resident on network servers are backed-up daily to magnetic media. Back-up tapes are stored on-site and at an off-site storage location.

Retention and Disposal:

Records kept by the FCC are maintained and disposed of in accordance with General Records Schedule 12 issued by the National Archives and Records Administration (NARA). Records are retained until an employee or contractor leaves the FCC and then shredded. Electronic records are destroyed physically (electronic storage media) or by electronic erasure. Individuals may request a copy of the disposition instructions from the FCC Privacy Act Officer or access the Schedule directly at <http://www.archives.gov/records-mgmt/ardor/grs12.html>.

System Manager(s) and Address(es):

Information Technology Center, Associate Managing Director--Information Technology (AMD-IT), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-C361, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Individual requests to check out loaned equipment; and inventory databases tracking current status of loaned equipment.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

System Name:

Cadapult Space Management System (CSMS).

Security Classification:

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

System Location(s):

Space Management Center (SMC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in this system are the FCC employees and contractors.

Categories of Records in the System:

The categories of records in this system include each FCC employee and/or contractor's organization (bureau/office/division), pay type, grade, supervisory status, bargaining unit, workspace location (office or workstation), work telephone number, and barcode(s) on information technology (IT) equipment assigned to the employee or contractor.

Authority for Maintenance of the System:

5 U.S.C. 301, 44 U.S.C. 3101, Executive Order 12411, Government Work Space Management Reforms, Section 486 of Title 40 of the United States Code, and the NTEU/FCC Basic Negotiated Agreement, Article 9, Employee Space and Facilities.

Purpose(s):

Space Management Center (SMC) uses the CSMS information system to allocate the offices, workstations, and facility workspaces for FCC employees and contractors following the FCC/National Treasury Union (NTEU) space assignment policy. In the event of an emergency, the SMC staff will devise a "Reconstitution Plan" in which they will extract information from the CSMS information system to create the space requirements for alternative work location(s) in other buildings to be used to relocate FCC employees and/or contractors. This information may be shared with the General Services Administration (GSA), National Telecommunications and Information Administration (NTIA), Department of Homeland Security (DHS), and Federal Emergency Management Agency (FEMA), etc.; District of Columbia, Virginia, and Maryland state governments, etc.; and other Federal, state, and local agencies involved in Federal agency evacuation, emergency facilities, space management, and/or relocation policies and plans, etc., as part of the FCC's Reconstitution Plan.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Emergency Response--A record on an individual in this system of records may be disclosed to emergency medical personnel, e.g., doctors, nurses, and/or paramedics, or to law enforcement officials in case of a medical or other

emergency involving the FCC employee without the subsequent notification to the individual identified in 5 U.S.C. 552a(b)(8);

2. First Responders--A record from this system of records may be disclosed to law enforcement officials, Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Department of Defense (DOD), National Telecommunications and Information Administration (NTIA), White House Communications Agency, other federal agencies, and state and local emergency response officials, *e.g.*, fire, safety, and rescue personnel, etc., and medical personnel, *e.g.*, doctors, nurses, and paramedics, etc., in case of an emergency situation at FCC facilities without the subsequent notification to the individual identified in 5 U.S.C. 552a(b)(8);

3. Reconstitution Plan--A record from this system of records may be disclosed to the General Services Administration (GSA), National Telecommunications and Information Administration (NTIA), Department of Homeland Security (DHS), and Federal Emergency Management Agency (FEMA), etc.; District of Columbia, Virginia, and Maryland state governments, etc.; and other Federal, state, and local agencies involved in Federal agency evacuation, emergency facilities, space management, and/or relocation policies and plans, etc.

4. Congressional Inquiries--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

6. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in the Cadapult Space Management System (CSMS) consists of electronic data, files, and records, which are housed in the FCC's computer network databases.

Retrievability:

Information in the CSMS information system is retrieved by the FCC employee or contractor's name, workspace location, and organizational unit, *e.g.*, bureau/office.

Safeguards:

The CSMS information system's electronic records, data, and files are maintained in the FCC's computer network databases. Access to the information in these databases is restricted to authorized CMS supervisors, staff, and contractors and to staff and contractors in the Information Technology Center (ITC), who maintain the FCC's computer network databases. 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 information that is resident on the SMC database is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

The FCC maintains information about the FCC employee and/or contractor only as long as he/she works at the Commission. The records in this system are deleted entirely upon the FCC employee's retirement, voluntary resignation, transfer, or re-assignment outside the Commission, and when the contractor is no longer working at the Commission. The CMS staff uses a sign-out procedure to verify that the FCC employee or contractor is no longer working at the Commission, then the individual's information is deleted from the CSMS system.

System Manager(s) and Address(es):

Space Management Center (SMC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Space Management Center (SMC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Space Management Center (SMC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Space Management Center (SMC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

The sources for the records in the CSMS information system include the FCC employee and/or contractor, his/her workspace requirements, organization, pay type, grade, supervisory status, bargaining unit, workspace location, work telephone number, and IT barcodes on IT equipment assigned to the employee or contractor.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

System Name:

Physical Access Control System (PACS). Note: This system of records was formerly titled "Access Control System."

Security Classification:

None.

System Location(s):

Information in this system is maintained in the following location: Security Operations Center, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554. This location is in a Federal building, where staffed guard stations have been established and which has an installed Personal Identity Verification (PIV) card reader system.

Categories of Individuals Covered by the System:

Any individual who requires regular, on-going access to FCC facilities and information technology systems. This includes but is not limited to:

1. Current FCC employees and current contractors;
2. Frequent visitors, temporary hires, special parking access users, and day contractors;
3. Applicants for Federal employment or contract work;
4. FCC students, interns, volunteers, affiliates, and individuals formerly in these positions, *e.g.*, retired FCC employees; and
5. Non-FCC employees who are authorized to perform or use services in FCC facilities on an on-going basis, *e.g.*, credit union employees, restaurant employees, and building maintenance and cleaning employees.

This system does apply to occasional visitors or short-term guests to whom the FCC will issue temporary identification and credentials, who may include:

1. All visitors to FCC, *e.g.*, non-FCC federal employees and contractors, students, interns, volunteers, and affiliates; and
2. Individuals authorized to perform or use services provided in FCC facilities on an infrequent basis, *e.g.*, and service and maintenance workers performing cleaning, maintenance, and repair duties in the Commission's buildings and facilities.

Categories of Records in the System:

The system consists of a computer database containing records on those individuals to whom the FCC has issued credentials. The records are filed alphabetically by last name, with a corresponding badge number.

1. FCC employee/temporary hire database includes: Full name (first, middle, and last names), Social Security Number (SSN), birth date, signature, image (photograph), fingerprints, hair color, eye color, height, weight, FCC telephone number, FCC Bureau/Office, FCC office/room number, personal identification number (PIN), background investigation form data and results, date the personal identify verification (PIV) card was issued and expiration dates, PIV registrar approval signature, PIV card serial number, emergency responder designation, copies of documents verifying identification or information derived from such documents, *e.g.*, document title, document issuing authority, document

number, document expiration date, other document information), national security level clearance and expiration date, parking permit data, computer system user name, user access and permission rights, authentication certificates, and digital signature information.

2. Contractor database includes: First, middle, and last name, Social Security Number (SSN), birth date, signature, image (photograph), fingerprints, hair color, eye color, height, weight, contractor company name, Federal supervisor, telephone number, FCC point of contact, FCC Bureau/Office, FCC office/room number, FCC telephone number, and FCC contractor badge number, personal identification number (PIN), background investigation form data and results, date the personal identify verification (PIV) card was issued and expiration dates, PIV registrar approval signature, PIV card serial number, emergency responder designation, copies of documents verifying identification or information derived from such documents, *e.g.*, document title, document issuing authority, document number, document expiration date, other document information), national security level clearance and expiration date, parking permit data, computer system user name, user access and permission rights, authentication certificates, and digital signature information.

3. Frequent Visitor's database includes: First and last names, employer's name, address, telephone number, image (photograph), and date of issuance and expiration date.

4. Day contractor database includes: First and last name along with badge number, date of issuance and expiration date.

5. Visitor database includes: First and last name, image (photograph), FCC point of contact and date of issuance.

6. Special Parking Access database includes: First and last name, telephone number, employer, FCC point of contact, and date of issuance.

Note: Records maintained on cardholders entering FCC facilities or using FCC systems, *e.g.*, FCC employees and contractors, include: Individual's first, middle, and last name, PIV card number, date, time, and location of entry and exit, FCC bureau/office, contractor/visitor's employer's name, address, telephone number, level of national security clearance and expiration date, digital signature information, and computer networks/applications/data accessed, and FCC point of contact.

Authority for Maintenance of the System:

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501); Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; Federal Property and Administrative Act of 1949, as amended; and Department of Justice Report, "Vulnerability Assessment of Federal Facilities," June 28, 1995.

Purpose(s):

The purposes of the system are:

1. To ensure the safety and security of FCC facilities, systems, and information, FCC employees, contractors, interns, guests, and frequent visitors;
2. To verify that all people entering the FCC facilities, using FCC and Federal information resources (or accessing classified information), are authorized to do so;
3. To track and control FCC badges (PIV cards) issued to individuals entering and exiting these facilities, using FCC systems, or accessing classified information; and
4. To provide a method by which the FCC may ascertain the times each person was in these facilities.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

1. Litigation by the Department of Justice--when (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the FCC or the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records;
2. Court or Adjudicative Body--in a proceeding when: (a) The FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;
3. Law Enforcement and Investigation--except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, otherwise, responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration or the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act, or when necessary for the review of private relief legislation pursuant to OMB Circular No. A-19;
6. Contract Services, Grants, or Cooperative Agreements--a record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a;
7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, or local government maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;
8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, or tribal government, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel or regulatory action;
9. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5

U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;

10. National Security and Intelligence Matters--disclosure of these records may be disclosed to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign government in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives; and

11. Invalid PIV Card Notification--disclosure may be made to notify another Federal agency, when, or to verify whether, a PIV card is no longer valid.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Note:Disclosures to the FCC of data pertaining to date and time of entry and exit of a Commission employee working in the District of Columbia may not be made to supervisors, managers, or any other individuals (other than the individual to whom the information applies) to verify the employee's time and attendance record for personnel actions because 5 U.S.C. 6106 prohibits Federal Executive Agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless the clock is used as part of a flexible schedule program under 5 U.S.C. 6120 *et seq.*

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information is maintained in a password-protected or logical access controlled electronic media, *e.g.*, computer database(s), and in securely controlled paper files.

Retrievability:

The information can be retrieved by: (1) The name of the individual; (2) Social Security Number (SSN); (3) other ID number, *e.g.*, FCC employee, contractor, or frequent visitor badge number; or (4) PIV card serial number.

Safeguards:

Paper records are kept in locked cabinets in secure facilities and access to them is restricted to individuals, *e.g.*, FCC Security Operations Center staff, whose role requires use of the information. The computer servers in which the information is stored are located in FCC facilities that are secured by limited access card readers. The computer servers themselves are password-protected. Access by individuals working at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A *Privacy Act Warning Notice* appears on the monitor screen when records containing information on individuals are first displayed. The FCC Security Operations Center staff performs a backup operation on these files on a regular basis using a secure medium. The backup data are stored in a locked and controlled room in a secure location.

Retention and Disposal:

Records relating to individuals with FCC access cards, covered by this system, are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). The records disposal is done in accordance with the Commission's disposal policies. Unless retained for specific, on-going security

investigations, records of facility access are maintained for one year and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. The records are disposed of in accordance with FCC Security Operations Center disposal policies, as follows:

1. When an employee/contractor/temporary hire/special parking access leaves the FCC, the file in the database is deleted.
2. Frequent visitor badges are given a two-year valid period, after which the card will automatically deactivate.
3. All returned day contractor cards will be reused on a daily basis.
4. Transaction data for all cards will be stored using a secure medium and retained for one year in the FCC Security Operations Center, which is locked and secured with an alarm system. Otherwise, access records are destroyed upon notification of death, or not later than one year after the employee's retirement or separation from the FCC, or the employee's transfer to another Federal agency, whichever is applicable.

In accordance with HSPD-12, PIV Cards are deactivated within eighteen (18) hours of notification of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by burning in an approved Federal burn-facility.

System Manager(s) and Address(es):

Security Operations Center, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Notification Procedure:

Individuals wishing to inquire whether this system of records contains information about them should contact the system manager indicated above. Individuals must furnish their full name, birth date, Federal agency name, and work location for their records to be located and identified. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the system manager of the records that the requester is entitled to access, *e.g.*, government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at a minimum, their name, date of birth, Social Security Number, and home address to establish identity. *See* 47 CFR 0.554-0.555.

Record Access Procedures:

Individuals wishing to request access to records about them should contact the system manager indicated above. Individuals must furnish their full name (first, middle, and last name), birth date, for their record to be located and identified. An individual requesting access must also follow FCC Privacy Act regulations regarding verification of identity and access to records. *See* 47 CFR 0.554-0.555.

Contesting Record Procedures:

Individuals wishing to request amendment of their records should contact the system manager indicated above. Individuals must furnish their full name (first, middle, and last name), birth date, for their record to be located and identified. An individual requesting amendment must also follow the FCC Privacy Act regulations regarding verification of identity and amendment of records. *See* 47 CFR 0.556-0.557.

Record Source Categories:

The individual FCC employee to whom the information applies, contractor, or applicant for employment; sponsoring

agency; former sponsoring agency; other federal agencies; contract employer; and/or former employee.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-8

System Name:

Time and Attendance Records.

Security Classification:

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

System Location(s):

Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

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

Categories of Records in the System:

The categories of records in this system are used:

1. To administer the pay, leave, and garnishment requirements for FCC employees: FCC employee's name, work and home addresses, Social 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.

Authority for Maintenance of the System:

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.

Purpose(s):

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;
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.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Compliance with Welfare Reform Requirements--Names, Social Security Numbers, home addresses, dates of birth, dates of hire, quarterly earnings, employer identifying information, and state of hire of employees may be disclosed to the Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services for the purposes of locating individuals to establish paternity, establishing and modifying orders of child support, identifying sources of income, and for other child support enforcement actions as required by the Personal Responsibility and Work Opportunity Reconciliation Act;
2. Adjudication and Litigation--Where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute,

regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. Congressional Inquiries--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;

5. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the Agency--Disclosure may be made to a Federal, State, local, foreign, tribal, or other public agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by Other than the Agency--Disclosure may be made to a Federal, State, local, foreign, tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action;

8. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;

9. Financial Obligations under the Debt Collection Act--A record from this system may be disclosed to other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996. A record from this system may be disclosed to any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government. A record from this system may be used to prepare information on items considered income for taxation purposes to be disclosed to Federal, State, and local governments;

10. Financial Obligations Required by the National Finance Center *et al.*--When the National Finance Center (the FCC's designated payroll office), the Department of the Treasury Debt Management Services, and/or a current employer to effect a salary, IRS and/or state tax refund(s), or administrative offset to satisfy an indebtedness; and to Federal agencies to identify and locate former employees for the purposes of collecting such indebtedness, including through administrative, salary, or tax refund offsets. Identifying and locating former employees, and the subsequent referral to such agencies for offset purposes, may be accomplished through authorized computer matching programs. Disclosures will be made only when all procedural steps established by the Debt Collection Act of 1982, as amended by the Debt Collection Improvement Act of 1996 or the Computer Matching and Privacy Protection Act of 1988 as appropriate, have been taken;

11. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records

has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm; and

12. Pay and Leave Disclosures--A record from this system may be disclosed to any source from which additional information is requested relevant to an FCC determination concerning an individual's pay or leave to the extent necessary to identify the individual, inform the source of the purpose(s) of the requests, and to identify the type of information requested.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

Disclosures may be made from this system 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).

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information includes paper document, records, and files that are stored in file cabinets, and electronic records, files and data that are stored on the FCC's network computer database.

Retrievability:

Records are indexed by the FCC's employee's name.

Safeguards:

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 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.

Retention and Disposal:

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>.

System Manager(s) and Address(es):

Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Human Resources Management (HRM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

The sources of the records in this system 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.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OMD-30

System Name:

FCC Visitors Database.

Security Classification:

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

System Location(s):

Office of the Managing Director (OMD), Security Operations Center (SOC), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554;

Categories of Individuals Covered by the System:

The records in this system include all visitors to the FCC. These individuals include, but are not limited to U.S. citizens, permanent residents (*i.e.*, green card holders), and foreign nationals.

Categories of Records in the System:

The categories of records in the FCC Visitors Database include, but are not limited to the individual's first and last name, photographic identification (including but not limited to a driver's license, passport, or other types of photo identification), the authority issuing the photo identification, U.S. visa number, FCC point of contact, visitor signature, professional title, organizational affiliation, contact information for the visitor, including but not limited to wireline and wireless (cell) phone numbers, correspondence related to information required to obtain visitor entry to the FCC, and purpose(s) for visiting the FCC.

Authority for Maintenance of the System:

5 U.S.C. 301; 6 U.S.C. 202; 8 U.S.C. 1103, 1158, 1201, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, 1732; Federal Information Security Act (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, sec. 203); and Federal Property and Administrative Act of 1949, as amended.

Purpose(s):

The purpose of the system is to cover the personally identifiable information (PII) that all visitors to the FCC, including but not limited to U.S. citizens, permanent residents (*i.e.*, green card holders), and foreign nationals, must provide to the FCC's Security Operations Center (SOC) to gain admittance to the FCC headquarters buildings and other FCC facilities.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Litigation by the Department of Justice--When: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the FCC or the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records;
2. Court or Adjudicative Body--In a proceeding when: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;
3. Law Enforcement and Investigation--Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in

conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, State, local, tribal, or foreign, or otherwise responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity;

4. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA), the Government Accountability Office (GAO), and/or the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. §§ 2904 and 2906 (such disclosure(s)) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

5. Congressional Inquiries--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;

6. Contract Services, Grants, or Cooperative Agreements--A record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a;

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the Agency--Disclosure may be made to a Federal, State, local, or tribal government, or other public authority or entity maintaining civil, criminal, intelligence, national security, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the Agency--Disclosure may be made to a Federal, State, local, or tribal government, or other public authority or entity of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel or regulatory action;

9. National Security and Intelligence Matters--Disclosure of these records may be made to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments and international law enforcement organizations and agencies in order to enable a Federal agency or entity charged with, but not limited to national security and/or intelligence activities and related functions, to carry out these duties and responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives;

10. Department of State, Department of Homeland Security, and other Federal Agencies--A record from this system may be disclosed, where appropriate, to the State Department, Department of Homeland Security (DHS), and/or other Federal agencies and entities charged with, but not limited to national security, law enforcement, immigration, intelligence, and related functions, activities, duties, and responsibilities, where there is an indication of a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to enforce,

investigate, or prosecute violations, or to enforce or implement a statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving Federal agency or entity;

11. Foreign Governments--A record from this system may be disclosed through the U.S. Department of State or the Department of Homeland Security (DHS) or other Federal security agencies, entities, or organizations or directly to the representative of such a foreign government or country, to the extent necessary to assist such a government or country in apprehending and/or returning a fugitive to a jurisdiction which seeks the individual's return, or to assist such a country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest; and

12. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when: (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information in the FCC Visitors Database includes paper document, files, and records that are stored in file cabinets in the Security Operations Center (SOC), and electronic records, files, and electronic records, files, and data that are stored in the FCC's computer network databases.

Retrievability:

The information in the FCC Visitors Database may be retrieved by the name of the individual, driver's license number, U.S. passport number, foreign passport number, U.S. visa number, date of birth (DOB), and/or photo ID number.

Safeguards:

The paper documents, records, and files are maintained in file cabinets in the SOC's office suite. The file cabinets where these paper documents, files, and records are stored are controlled by on-site personnel when unlocked and locked when not in use. Access to the SOC office suite is through a card-coded main door. Access to the file cabinets is restricted to authorized SOC supervisors, staff, and contractors, whose duties and responsibilities require use of the information.

The electronic records, files, and data are stored in the FCC computer network databases that are secured by limited access card readers. The computer servers themselves are password-protected. Access to the electronic files is restricted to authorized SOC supervisors, staff, and contractors, and to the Information Technology Center (ITC) staff and contractors, who maintain the FCC's computer network. 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. A *PRIVACY WARNING NOTICE* appears on the monitor screen when records containing information on individuals are first displayed. Information resident on the SOC database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

Records in the FCC Visitors Database are retained in accordance with General Records Schedule (GRS) 18, Item 17 approved by the National Archives and Records Administration (NARA). The records disposal is done in accordance with the Commission's disposal policies. Unless retained for specific, on-going security investigations, records of facility access are maintained for one year and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with GRS 18, item 22a, approved by NARA. The records are disposed of in accordance with SOC disposal policies, as follows:

1. All returned day contractor cards will be reused on a daily basis.
2. Transaction data for all FCC Visitors Database cards will be stored using a secure medium and retained for one year in the SOC, which is locked and secured with an alarm system.

In accordance with Homeland Security Presidential Directive (HSPD-12), Personal Identity Verification (PIV) Cards are deactivated within eighteen (18) hours of notification of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with GRS 11, Item 4. PIV Cards are destroyed by burning in an approved Federal burn-facility.

System Manager(s) and Address(es):

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Notification Procedure:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Access Procedures:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Contesting Record Procedures:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Source Categories:

The sources for information in this system are the visitors themselves and/or their agency or organizational sponsor(s) who have been invited to or have requested admittance to the FCC headquarters buildings and other FCC facilities for the visitors.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /PSHSB-1

System Name:

FCC Emergency and Continuity Contacts System (ECCS).

Security Classification:

The Security Operations Center (SOC) has not assigned a security classification to the FCC EPS; however, information in this system may be designated as "Non Public," or "For Internal Use Only," Or "For Official Use Only."

System Location(s):

Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in the FCC EPS include:

1. Emergency Contacts: FCC employees, Federal Government contacts, State, Tribal, Territorial, Local Government and private sector contacts along with institutions, organizations, and individuals with crisis management and emergency preparedness functions, *etc.*
2. Continuity of Operations (COOP) Contacts: Bureau and Office Emergency Response Group (ERG) and Devolution Emergency Response Group (DERG) members (employees and contractors) and FCC and Bureau and Office lines of succession.

Categories of Records in the System:

The records in the FCC EPS include:

1. Emergency Contacts: Individual and/or business name(s), position title, business telephone number(s), business cell phone number(s), business satellite phone number(s), business pager number(s), business facsimile number(s), business address(es), business e-mail address(es), home telephone number(s), personal cell phone number(s), personal pager number (s), personal facsimile number(s), and personal e-mail address(es), *etc.*; and
2. COOP Contacts: FCC members, FCC employee's and contractor's name(s), position title, security clearance information, line of succession information, work and personal telephone number(s), work and personal facsimile number(s), work and personal cell phone number(s), satellite telephone number(s), FCC Government Emergency Telecommunications System (GETS) and Wireless Priority System (WPS) information, satellite telephone number(s), Government passport numbers, work and personal pager number(s), and work and personal e-mail address(es), *etc.*

Authority for Maintenance of the System:

Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984, *as amended* February 28, 2003 and June 26, 2006; Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 21, 1998; Homeland Security Act of 2002 (6 U.S.C. § 101 *et seq.*), November 25, 2002; National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*, May 9, 2007; National Communications System Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, July 25, 2007; *National Continuity Policy*

Implementation Plan, Homeland Security Council, August 2007; Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, February 2008; Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, February 2008.

Purpose(s):

The FCC uses the records in the FCC ECCS:

1. Emergency Contacts: To allow the FCC to coordinate crisis response activities, *etc.*;
2. COOP Contacts: To allow the FCC to contact FCC employees and contractors regarding COOP matters, *etc.*; and
3. To allow the FCC to use an automated telephone and e-mail system to contact its Emergency Contacts and COOP Contacts, *etc.*

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Emergency Response--A record of an individual in this system of records may be disclosed to emergency medical personnel, *i.e.*, doctors, nurses, and/or paramedics, to law enforcement officials or other first responders and emergency officials in case of a medical or other emergency involving the FCC employee or contractor without the subsequent notification to the individual identified in 5 U.S.C. 552a(b)(8);
2. Adjudication and Litigation--Where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in her or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
3. Law enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--When requested by a Congressional office in response to a written inquiry by an individual made to the Congressional office for the individual's own records;
5. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA) and/or the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
6. Employment, Clearances, Licensing, Contract, Grant or other Benefits Decisions by the agency--A disclosure may be made to Federal, State, local or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit;
7. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5

U.S.C. chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

8. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

9. First Responders--A record from this system of records may be disclosed to law enforcement officials, Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Department of Defense (DOD), National Telecommunications and Information Administration (NTIA), White House Communications Agency, other Federal agencies, and state and local emergency response officials, *e.g.*, fire, safety, and rescue personnel, *etc.*, and medical personnel, *e.g.*, doctors, nurses, and paramedics, *etc.*, in case of an emergency situation at FCC facilities, without the subsequent notification to the individual identified in 5 U.S.C. 552a(b)(8); and

10. Contracted Third Parties--A record of this system may be disclosed to external contracted parties throughout the United States for required maintenance, data input, and/or extraction requirements, testing, and activation of an automated telephone and e-mail system.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in the FCC ECCS consists of electronic data, files, and records, which are housed in the FCC's computer network databases, and paper documents, files, and records, which are stored in file cabinets in the PSHSB office suite.

Retrievability:

Information in the Emergency Contacts and the COOP Contacts databases is retrieved by searching any field in the respective database;

Safeguards:

1. Emergency Contacts: The paper records, documents, and files are stored in filing cabinets in the PSHSB office suite, which are locked when not in use. The electronic records, files, and data are maintained in the FCC's network computer databases and by a third-party vendor.

2. COOP Contacts: The paper records, documents, and files are stored in filing cabinets in the PSHSB office suite, which are locked when not in use. The electronic records, files, and data are maintained in the FCC's network computer databases.

The FCC's computer networks that house the Emergency Contacts database and the COOP Contact database are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. Information resident on the Emergency Contacts and COOP Contacts database servers is backed-up per FCC Office of Managing Director protocols.

The information in the Emergency Contacts database and COOP Contacts database is only available for review and updating by the employees and contractors (whose information is maintained in the databases), Bureau/Office administrative personnel, and FCC management on a need-to-know basis. Authorized PSHSB supervisors and staff also have access to the paper documents, files, and records that are stored in the filing cabinets located in the PSHSB office suite and to the electronic records, files, and data that are housed in the FCC's computer network databases and in those of a third-party vendor. The supervisors, staff, and contractors in the FCC's Information Technology Center's (ITC), who manage the FCC's computer network databases have access to the electronic information. Other employees and contractors are only granted access to the information in the filing cabinets and electronic databases on a "need-to-know" basis.

Retention and Disposal:

1. Emergency Contacts: The paper files and electronic data in this system are retained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule 1, which may be viewed at <http://www.archives.gov/records-mgmt/ardor/grs01.html>.

2. COOP Contacts: The retention schedule for this system's electronic records has not yet been determined. No records will be destroyed until a disposal schedule has been approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Address inquiries to Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

1. Emergency Contacts: The sources for the information in this system include FCC employees, Federal Government contacts, State, Tribal, Territorial, Local Government and private sector contacts along with institutions, organizations, and individuals with crisis management and emergency preparedness functions, *etc.*; and

2. COOP Contacts: The sources for information in this system include FCC employees and contractors.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /PSHSB-2

System Name:

PSHSB Contact Database.

Security Classification:

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

System Location(s):

Public Service and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

Individuals from the public-at-large and the public safety community.

Categories of Records in the System:

The categories of records in this information system include the contact information in the PSHSB Contact Database that individuals have provided with their comments or messages, which includes one or more of the following, depending upon PSHSB requirements:

1. Personal contact information, including but not limited to, individual's name, personal cell phone number(s), home telephone number(s), business telephone number(s), personal and professional email address(es), personal and professional fax number(s), IP address, business and home mailing address, etc.; and

2. Job-related data, including but not limited to:

(a) Type(s) of organization(s): Title, academia, association/institution, authorities, college/university, boards, commissions, councils, legislative, military, non-for-profit organization(s), private sector, business(es), research and development (R&D), training facilities; and

(b) Government(s): City, county, federal, foreign, state, tribal; and organization affiliation, *i.e.*, such as 9-1-1 Services, Public Safety Answering Points (PSAPs), Emergency Alert System (EAS), first responders, health care sector, persons with disabilities, and spectrum. *e.g.*, spectrum authorizations, spectrum management, spectrum enforcement.

Authority for Maintenance of the System:

Sec. 151, 152, 155, 257, 303 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 155.

Purpose(s):

The FCC's PSHSB Contact Database information system stores the personally identifiable information (PII) that individuals may submit voluntarily via one or more of these customer comment formats:

(a) PSHSB's (electronic) Web page Comment Card (Contact Us) at: <http://www.fcc.gov/pshs/contactus.html> for those who wish to submit comments to PSHSB;

(b) PSHSB's (electronic) Summit Comment Card (Feedback): <http://volta.fcc.gov:9090/pshs/summits/> and <http://www.fcc.gov/pshs/event-registration2.html> for those who participate in PSHSB's public events, such as summits, conferences, forums, expos, lectures, etc., and wish to submit comments;

(c) PSHSB's (electronic) Event Registration Form (Event Registration): <http://www.fcc.gov/pshs/event-registration.html> for those who wish to register for PSHSB events online;

(d) PSHSB's (electronic) Photo Safety Contest: <http://www.fcc.gov/pshs/photo-project-and-contest.html> for those who wish to submit a photo entry for PSHSB's monthly contest;

(e) PSHSB's (electronic) Network Outage Reporting System (NORS): <http://www.fcc.gov/pshs/services/cip/nors/nors.html> for those who submit questions to PSHSB regarding NORS content; and/or

(f) PSHSB's (paper) business card collections, whose information is transferred into PSHSB's (electronic) Contact Database, and the business card is then destroyed.

These formats provide a means by which PSHSB receives feed-back as part of PSHSB's public relations and outreach activities.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Congressional Inquiries--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;

2. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA), the General Services Administration (GSA), and/or the Government Accountability Office (GAO) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

3. Program Partners (public safety community)--A record from this system may be used as part of the PSHSB's statistical reporting and/or summaries of the comments that the Bureau provides to first responders such as the Red Cross, Association of Public Communications Officials (APCO), National Emergency Number Association (NENA), Department of Homeland Security (DHS), and other federal partners, law enforcement agencies, and medical organizations, etc., which have participated in PSHSB summit conferences, and who may have expressed interest in such reports and/or comment summaries.

4. Adjudication and Litigation--Where after careful review, the Agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

5. Law Enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate federal, state, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency; and

6. Breach Notification--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm; and

7. Public Access--Information pertaining to these PSHSB outreach activities is available for public inspection via the Internet at <http://www.fcc.gov/psheb/>. PSHSB may redact any personally identifiable information (PII) or other sensitive information at the request of the individual whose information is being posted.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose(s) for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

STORAGE:

The information in this system includes electronic comment records, files, and data that are maintained in the FCC's computer network databases; and paper business cards are immediately destroyed after the information is transferred into the PSHSB's (electronic) Contact Database.

Retrievability:

The information in the paper business cards is immediately transferred to the PSHSB (electronic) Contact Database, and any information can then be retrieved by the individual's personal contact information, and the individual's job-related data.

Information in the PSHSB Contact Database information system's electronic databases can be retrieved by the individual's personal contact information, and the individual's job-related data.

Safeguards:

The information on paper business cards, which are collected by PSHSB personnel, is immediately transferred to the PSHSB (electronic) Contact Database and the paper cards are then destroyed soon after.

The electronic records, data, and files are maintained in the FCC computer network databases. Access to the information in the electronic files is restricted to authorized PSHSB supervisors and staff. Authorized staff and contractors in the FCC's Information Technology Center (ITC), who maintain these computer 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. Information resident on the database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

The information on the paper business cards, which are collected by PSHSB personnel, is immediately transferred to the PSHSB (electronic) Contact Database, and the paper cards are then destroyed soon after.

All information that is collected via the electronic Web sites and/or transferred (from paper business cards) to these PSHSB electronic databases will be kept by the FCC until a records schedule has been approved by the National Archives and Records Administration (NARA).

System Manager(s) and Address(es):

Public Safety and Homeland Security (PSHSB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Public Service and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Public Service and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Public Service and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Source Categories:

Information in the Contact Database system is provided by individuals (general public and public safety community) who submit their comments and messages to PSHSB via PSHSB's (electronic) Web page Comment Card (Contact Us); PSHSB's (electronic) Summit Comment Card (Feedback); PSHSB's (electronic) Event Registration Form (Event Registration); PSHSB (electronic) Photo Safety Contest; PSHSB (electronic) Network Outage Reporting System (NORS); and PSHSB's (paper) business card collections; which provide the means by which PSHSB receives input and feed-back as part of the Bureau's customer relations activities.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OSP-1

System Name:

Broadband Dead Zone Report and Consumer Broadband Test.

Security Classification:

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

System Location(s):

Office of Strategic Planning (OSP), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in this system include individuals who participate in the Broadband Dead Zone Report voluntary survey and individuals who participate in both the fixed and mobile versions of the voluntary Consumer Broadband Test.

Categories of Records in the System:

The categories of records in this system include the street address, city, state, zip code, of each individual who selects to participate in the Broadband Dead Zone Report voluntary survey and each individual who participates in both the fixed and mobile versions of the voluntary Consumer Broadband Test. The voluntary fixed and mobile Consumer Broadband Test also collects the "Internet Protocol (IP) address" of each user who selects to participate. The voluntary fixed and mobile consumer broadband tests collect the "unique handset identification number" of each individual's smartphone used to access the test, and collect the location reported by each user's handset (reported as a latitude and longitude point) at the moment the user initiates the test.

Authority for Maintenance of the System:

Broadband Data Improvement Act of 2008, Public Law 110-385, Stat 4096 § 103(c)(1); American Reinvestment and Recovery Act of 2009 (ARRA), Public Law 111-5, 123 Stat 115 (2009); and Communications Act, 47 U.S.C. 154(i).

Purpose(s):

The Commission uses the records in this system collected from the Broadband Dead Zone Report and the voluntary fixed and mobile Consumer Broadband Test to determine the access of U.S. residents to broadband--cable, DSL, fiber, mobile wireless, and other broadband services, and to gather data on the quality of the broadband services being provided. The Consumer Broadband Test permits users to measure the quality of their fixed or mobile Internet broadband connection. Individual street addresses, IP addresses, mobile handset location, and unique handset identification numbers are not made public by the FCC, but aggregated or anonymized data from the database may be made public. Additionally, IP addresses, mobile handset location, and unique handset identification numbers may be shared with FCC software partners as part of the Consumer Broadband Test application. These partners may publish the IP address, mobile handset location, unique handset identification numbers, and broadband performance data, or otherwise make this information available to the public (but the IP address is not associated with a street address). These data may be used to inform implementation of the National Broadband Plan, the National Broadband Map, and other proceedings related to the provisioning of broadband services.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Law Enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be referred to the appropriate Federal, state, or local agency responsible for investigating or prosecuting a violation or for implementing or enforcing the statute, rule, regulation, or order.

2. Department of Justice, Courts, and Adjudicative Bodies--A record from this system of records may be disclosed to the Department of Justice (DOJ) or in a proceeding before a court or adjudicative body when:

(a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Commission determines that the disclosure is relevant or necessary to the litigation.

3. Congressional Inquiries--A record on an individual in this system of records may be disclosed to a Congressional office in response to an inquiry the individual has made to the Congressional office.

4. Government-wide Program Management and Oversight--A record from this system of records may be disclosed to General Services Administration (GSA) and to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; to the U.S. Department of Justice (DOJ) in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or to the Office of Management and Budget (OMB) in order to obtain that office's advice regarding obligations under the Privacy Act. Such disclosure shall not be used to make a determination about individuals.

5. Data Breach--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

6. Public-Private Partnerships and the USDA Rural Development Agency's Telecommunications Program--The information collected through the Broadband Dead Zone Report and voluntary fixed and mobile Consumer Broadband Test, with the exception of any personally identifiable information (PII), may be shared with public-private partnerships and with the Telecommunications Program of the United States Department of Agriculture (USDA) Rural Development Agency. This sharing regime is described in the Commission's Broadband Data Order of 2008 (FCC 08-89).

7. NTIA and State Designated Entities--The information collected through the Broadband Dead Zone Report and voluntary fixed and mobile Consumer Broadband Test, including the personally identifiable information (PII), may be shared with the National Telecommunications and Information Administration (NTIA) and the 56 State Designated Entities for the State Broadband Data & Development Grant Program, who are tasked with gathering broadband availability information that is delivered to the FCC and NTIA for compilation into the National Broadband Map. Any PII shared with these entities is disclosed under the rules of the agreement between NTIA and the state grantees governing the protection of sensitive, protected, or classified data collected pursuant to the grant program. The NTIA and the state grantees do not make any PII publicly available.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information includes the electronic data and records that are stored in the FCC's computer network databases.

Retrievability:

Information in the Broadband Dead Zone Report and voluntary fixed and mobile Consumer Broadband Test system may be retrieved by the responses to the broadband Internet access questions: (1) Broadband access (yes/no); (2) broadband service availability (check boxes for types of broadband services available at an individual's home); (3) the individual's home address: street address, city, state, and zip code; (4) the individual's IP address; (5) the individual's reported handset location; and (6) the individual's unique handset identification number. Furthermore, the information may be retrieved and/or aggregated based upon other voluntary fixed and mobile Consumer Broadband Test variables, such as broadband speed, latency, jitter, and packet loss, among other broadband quality variables.

Safeguards:

Access to the information in the Broadband Dead Zone Report or the voluntary fixed and mobile Consumer Broadband Test database, which is housed in the FCC's computer network databases, is restricted to authorized supervisors and staff in the Office of Strategic Planning (OSP) and the Information Technology Center's (ITC) Planning and Support Group, who maintain these computer databases. Additionally, staff of the National Broadband Map may be granted access to this data. 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. Information resident on the database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

The information in this system is limited to electronic files, records, and data, which pertains to the Dead Zone Report, which includes:

- (1) The information obtained from individuals who participated in the Consumer Information survey; and
- (2) The information obtained from individuals who participated in the voluntary fixed and mobile Consumer Broadband Test.

Until the National Archives and Records Administration (NARA) approves the retention and disposal schedule, these records will be treated as permanent.

System Manager(s) and Address(es):

Address inquiries to the Office of Strategic Planning (OSP), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Office of Strategic Planning (OSP), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Office of Strategic Planning (OSP), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Office of Strategic Planning (OSP), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in this system are the Broadband Dead Zone Report survey respondents and voluntary fixed and mobile Consumer Broadband Test participants.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /OWD-1

System Name:

Reasonable Accommodation Requests under the Rehabilitation Act of 1973.

Security Classification:

None.

System Location(s):

Office of Workplace Diversity (OWD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 5-C750, Washington, DC 20554.

Categories of Individuals Covered by the System:

Federal Communications Commission (FCC) employees or contractors with disabilities.

Categories of Records in the System:

Electronic databases with all records containing the last and first name, filed alphabetically by last name, and a corresponding identification number, which includes:

1. FCC employee/temporary hire database contains: first and last name, telephone number, organizational unit, room number, date of issuance, and property pass privileges, if applicable.
2. Contractor database contains: first and last name, contractor company name, telephone number, FCC point of contact, telephone number, and date of issuance.

Authority for Maintenance of the System:

Executive Order (EO) 13164, Establishing Procedures to Facilitate the Provision of Reasonable Accommodation; EEOC, Enforcement Guidance on Reasonable Accommodation and Undue Hardship Under the Americans with Disabilities Act, 29 CFR Part 1615; Rehabilitation Act of 1973, 29 U.S.C. 12101 *et seq.*; 29 CFR 1630.

Purpose(s):

The system provides a method by which the FCC can identify Commission employees who have requested "reasonable accommodations" in their office, work stations, or to use other FCC facilities. Information on the disposition of each request is also maintained in this system.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act; and
5. Labor Relations--A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are maintained in a password protected computer database.

Retrievability:

Records are retrieved by the name of the individual or accommodation identity number.

Safeguards:

The computer terminals are stored within a secured area. The Security Office staff performs a backup operation on these files on a weekly and monthly basis on 1/4" data cartridges, which are stored/safeguarded in the Security Office.

Retention and Disposal:

Records kept by the FCC are retained until an employee or contractor leaves the FCC and then shredded. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Director of Workplace Diversity (OWD), 445 12th Street, SW., Room 5-C750, Washington, DC 20554; or Security Operations Center, Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Individuals requesting accommodation.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /WTB-1

System Name:

Wireless Services Licensing Records.

System Location(s):

Wireless Telecommunications Bureau (WTB), Room 3-C122, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

1. Licensees and applicants (including persons or entities with attributable interests therein as described below);
2. Tower owners; and
3. Contact persons relating to radio systems licensed or processed by the Wireless Telecommunications Bureau under parts 13, 22, 24, 27, 74, 80, 87, 90, 95, 97, and 101 of the Commission's Rules (Wireless Services).

Categories of Records in the System:

The information includes:

1. Applications, licenses, and pleadings relating to such applications--including Individual Taxpayer Identification Numbers;
2. Correspondence relating to authorizations, and
3. Requests for authorizations in the Wireless Services.
4. FCC Forms 175, 601, 602, 603, 603T, and 605 and any supporting exhibits submitted by the applicant(s), and related documentation associated with the FCC's processing of these forms.

Authority for Maintenance of the System:

31 U.S.C. 7701; and 47 U.S.C. 301, 303, 309, 312, 362, 364, 386, 507, and 510.

Purpose(s):

Records are kept to administer the Federal Communications Commission's (FCC) regulatory responsibilities including licensing, enforcement, rulemaking, and other actions necessary to perform spectrum management duties, as follows:

1. To provide public access to pending requests for authorizations and information regarding current licensees;
2. To determine the availability of spectrum for licensing;
3. To determine when compliance filings, renewal applications, and fees are due from licensees;
4. To resolve disputes between radio operators regarding who has certain rights to use particular frequency bands in particular geographic areas;
5. To resolve cross border disputes, on occasion, *e.g.*, dispute(s) with entities operating in Canada and Mexico.
6. To allow licensees to transfer or assign their interests in particular licenses or portions of licenses as the rules permit (after agency approval);
7. To evaluate the completeness and sufficiency of requests for new or modified authorizations;

8. To provide reports to a variety of Federal officials on the current uses and utilization of the spectrum the FCC is charged with regulating; and

9. To provide public access to license data (except ITIN numbers), which promotes the economically efficient allocation of spectrum and the resolution of radio interference problems.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--the licensee records will be publicly available and routinely used in accordance with Subsection b. of the Privacy Act; ITIN Numbers and material which is afforded confidential treatment pursuant to a request made under 47 CFR 0.459 will not be available for public inspection;
2. Financial obligations under the Debt Collection Acts--a record from this system may be disclosed to other Federal agencies for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982, the Debt Collection Improvement Act of 1996, or the Federal Claims Collection Standard. A record from this system may be disclosed to any Federal, state, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals who are delinquent in their repayment of certain debts owed to the U.S. Government. A record from this system may be used to prepare information on items considered income for taxation purposes to be disclosed to Federal, state, and local governments;
3. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
4. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
5. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
6. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

Pursuant to 5 U.S.C. 552a (b) (12), the Department of Treasury may disclose to a consumer reporting agency information regarding a claim by the FCC that is determined to be valid and overdue as follows:

1. The name, address, SSN or ITIN, and other information necessary to establish the identity of the individual or organization responsible for the claim;
2. The amount, status, and history of the claim; and

3. The program under which the claim arose.

The Commission may disclose the information specified in this paragraph under 5 U.S.C. 552a (b)(12) and the procedures contained in subsection 31 U.S.C. 3711(e). A consumer reporting agency to which these disclosures may be made is defined at 31 U.S.C. 3701(a) (3).

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

All records are stored and accessed electronically:

1. Records that are submitted on paper are scanned or keyed into the computer system as appropriate; and
2. Paper records are archived after being entered electronically.

Tape backups of records are periodically created. Records of prior licensees are archived.

Retrievability:

Records may be retrieved by searching electronically using a variety of parameters including name, a licensee's unique identifier, call sign, file number, *etc.* However, paper records which contain ITIN's are not available for public inspection.

Safeguards:

Records are protected by passwords and other computer security measures including the issuance of unique identifiers after such applicant or licensee completes the initial registration of such protected data as ITIN's. Access to privacy protected data is available only to those persons whose jobs require such access. Data resident on network servers are backed-up on to magnetic media. Back-up tapes are stored on-site and at an off-site storage location.

Retention and Disposal:

Records are maintained for eleven years after an individual ceases to be a licensee. Electronic records are destroyed physically (electronic storage media) or by electronic erasure.

System Manager(s) and Address(es):

Chief, Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Room 3-C122, Washington, DC 20554.

Notification Procedure:

Address inquiries to the system manager.

Record Access Procedures:

Address inquiries to the system manager.

Contesting Record Procedures:

Address inquiries to the system manager.

Record Source Categories:

Individual conducting business with the FCC.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /WTB-5

System Name:

Application Review List for Present or Former Licensees, Operators, or Unlicensed Persons Operating Radio Equipment Improperly.

Security Classification:

None.

System Location(s):

Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Room 3-C122, Washington, DC 20554.

Categories of Individuals Covered by the System:

1. Individuals who are or have been licensed under parts 13, 22, 24, 27, 74, 80, 87, 90, 95, 97, and 101 of FCC Rules, and who have operated in violation of the Federal Communications Commission's (FCC) rules or the Communications Act of 1934, as amended;
2. Unlicensed persons who have operated radio transmitting equipment; and
3. Persons who have had a license revoked or have had an application dismissed or denied, and are prohibited from filing another application within one year.

Categories of Records in the System:

Information in this system includes: name, address, date of birth (if known), authorization code of staff member who placed name in the file, and date the name was placed in the file.

Authority for Maintenance of the System:

47 U.S.C. 301, 303, 309(e), and 312.

Purpose(s):

The records are used by selected staff and field employees to determine whether the application of these individuals should be granted, dismissed, or set for hearing.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;
2. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
3. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and
4. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are stored on magnetic tape and computer printout(s).

Retrievability:

Information is filed alphabetically by name of individual in a computer and is retrieved periodically through computer printout.

Safeguards:

Access to the computer database(s) is controlled by passwords; the computer(s) is located in a secured office; and the printouts are available only to selected staff personnel.

Retention and Disposal:

The printouts are destroyed by machine shredding when a new list is distributed. The computer tapes are retained for four back-up cycles, and on the fifth update, the oldest tape is destroyed by burning.

System Manager(s) and Address(es):

Chief, Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Room 3-C122, Washington, DC 20554.

Notification Procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its notification procedure for this system of records.

Record Access Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record access procedures for this system of records.

Contesting Record Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its contesting record procedure for this system of records.

Record Source Categories:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

Exemptions Claimed for the System:

This system of records is exempt from sections (c)(3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;
2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act; and
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

[\[Return to TOP\]](#)

FCC /WTB-6

System Name:

Archival Radio Operator Records.

Security Classification:

None.

System Location(s):

Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 1270 Fairfield Road, Gettysburg, Pennsylvania 17325.

Categories of Individuals Covered by the System:

Individuals who applied for and/or received a radiotelephone (wireless) operator license or permit prior to the implementation of the Federal Communications Commission's Universal Licensing System (ULS) in 2001.

Categories of Records in the System:

Information includes: applications for radiotelephone (wireless) operator's license or permit prior to the implementation of the Federal Communications Commission's Universal Licensing System in 2001, and documents associated with these applications.

Authority for Maintenance of the System:

47 U.S.C. 303(l), 303(m), and 318.

Purpose(s):

These archival records are used to:

1. Administer the Commission's radio operator program including applications and determinations of license applicant qualifications. Limited file materials concerning licensed radio operators are maintained in the FCC's computer database. The information in the license database will be available for public inspection.
2. Refer possible violations of law to the Federal Communication Commission's (FCC) Enforcement Bureau, Office of General Counsel (OGC), and to the appropriate agency charged with the responsibility of investigating or prosecuting such violation(s).

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Public access--the licensee records will be publicly available and routinely used in accordance with Subsection b. of the Privacy Act; ITIN Numbers and material which is afforded confidential treatment pursuant to a request made under 47 CFR 0.459 will not be available for public inspection;
2. Adjudication and Litigation--where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. Law Enforcement and Investigation--where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;
4. Congressional Inquiries--when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;
5. Government-wide Program Management and Oversight--when requested by the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency--disclosure may be made to a Federal, State, local, or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit; and
7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency--disclosure may be made to a Federal, State, local, foreign, tribal, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel or regulatory action.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information is stored on microfilm and in a computer database.

Retrievability:

All records are retrievable by applicant name.

Safeguards:

The microfilm is stored in file cabinets that are secured at the close of the business day. Access to the database is secured by passwords. Data resident on network servers are backed-up onto magnetic media. Back-up tapes are stored on-site and at an off-site storage location.

Retention and Disposal:

Commercial applications are destroyed when eleven years old. Electronic records are destroyed physically (electronic storage media) or by electronic erasure. Both General and Restricted Permit applications are retained for 75 years.

System Manager(s) and Address(es):

Chief, Database Management Division, Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 1270 Fairfield Road, Gettysburg, PA 17325.

Notification Procedure:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its notification procedure for this system of records.

Record Access Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record access procedures for this system of records.

Contesting Record Procedures:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its contesting record procedure for this system of records.

Record Source Categories:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

Exemptions Claimed for the System:

This system of records is exempt from sections (c)(3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554-0.557 of the Commission's rules. These provisions concern the notification, record access, and contesting procedures described above, and also the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;
2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act; and
3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended.

[\[Return to TOP\]](#)

FCC /WTB-7

System Name:

Remedy Action Request System (RARS).

Security Classification:

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

System Location(s):

Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in the RARS system include individuals who request help using the FCC's licensing systems and related Commission research tools, information systems, and electronic databases, *i.e.*, Integrated Spectrum Auctions System (ISAS), Antenna Registration System (ARS), and Commission Registration System (CORES), *etc.*, and other subsystems included in, or as part of, these systems, *etc.*

Categories of Records in the System:

The categories of records in the RARS system include:

1. Requests for assistance by the requester's first name, last name, telephone number and extension, alternative telephone number and extension, fax number, e-mail address(es), computer operating system, Web browser, FCC Registration Number (FRN), and/or Individual Taxpayer Identification Number (ITIN), and personal security question and answer.
2. Records verifying identity information by the individual's first name, last name, contact telephone number, FRN and/or ITIN, and personal security question and answer.

Authority for Maintenance of the System:

Sec. 151, 154, 258, 301, 303, 309(e), 312, 362, 364, 386, 507 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154, 226, 258, 301, 303, 309(e), 312, 362, 364, 386, 507; and 29 U.S.C. 794, 794(d).

Purpose(s):

1. The FCC staff uses the records in the RARS information system to record and process requests from individuals or groups for technical help, *i.e.*, technical questions, password requests, *etc.*, using the FCC's licensing systems and related Commission research tools, information systems and electronic databases; and
2. The FCC management uses the RARS information system software to ensure good customer service and problem resolution.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. *Public Access*--Records in this system will be made available upon request for public inspection after redaction of information that could identify the correspondent, *i.e.*, name, telephone number, ITIN, and e-mail address. Limited public access to certain records may be available via the Internet at: <https://esupport.fcc.gov/request.htm>. This information includes the status of request, request ID number, and the agent's number who took the call or electronic

request for support. Public users who have contacted FCC personnel via telephone, e-mail, or electronic submission may access the system to retrieve a status on the ticket assigned to their request. They will be given this ticket/request number generated by the Remedy Action Request System (RARS) upon submission of a request. This number may be entered into the appropriate field on the FCC Web site to check the status of the ticket. Only the status of that ticket will be released to the public by entering the ticket number--no personal or confidential information is available to the public;

2. *Adjudication and Litigation*--Where by careful review, the agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

3. *Law Enforcement and Investigation*--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate Federal, State, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency;

4. *Congressional Inquiries*--When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records; and

5. *Government-wide Program Management and Oversight*--When requested by the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

6. *Breach Notification*--A record from this system may be disclosed to appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Information in the RARS information system consists of electronic data, files, and records, which are housed in the FCC's computer network databases. Any paper documents that WTB receives are scanned into the electronic database upon receipt, and then the paper documents are destroyed.

Retrievability:

The electronic data, files, and records may be retrieved by searching electronically using a variety of parameters including the requester's name, entity name, licensee, applicant or unlicensed individual, call sign, file number, problem type, FRN, ITIN, e-mail address, and/or subject matter.

Safeguards:

The information in the RARS information system's electronic documents, files, and records is housed in the FCC's computer network databases. Access to the information in these databases is restricted to authorized WTB supervisors, staff, and contractors in WTB and to staff and contractors in the Information Technology Center (ITC), who maintain the FCC's computer network databases. Those who have access to the computer networks are assigned a secured log-in ID and password maintained in the RARS information system. Other employees and contractors may be granted access on a "need-to-know" basis.

The network computers are located in secured areas, and they are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. Information resident on the database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

Retention and Disposal:

The information in the RARS information system is maintained for 11 years after an individual ceases to be a user of the system. The electronic records, files, and data are destroyed physically (electronic storage media) or by electronic erasure.

Paper documents are destroyed by shredding after they are scanned into the RARS information system's electronic databases.

System Manager(s) and Address(es):

Address inquiries to the Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Notification Procedure:

Address inquiries to the Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Access Procedures:

Address inquiries to the Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Contesting Record Procedures:

Address inquiries to the Wireless Telecommunications Bureau (WTB), Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554.

Record Source Categories:

Information in the RARS information system is provided by RARS user customers who request assistance with the FCC's licensing systems and related Commission research tools, information systems, and electronic databases, *i.e.*, Integrated Spectrum Auctions System (ISAS), Antenna Registration System (ARS), and Commission Registration

System (CORES), etc., and other subsystems included in, or as part of, these systems, *etc.*

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

FCC /WCG-1

System Name:

Lifeline Program

Security Classification:

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

System Location(s):

Universal Service Administrative Company (USAC)/Contractor Server Address:

Universal Service Administrative Company (USAC), 2000 L St. NW., Suite 200, Washington, DC 20036; and Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Categories of Individuals Covered by the System:

The categories of individuals in this system include those individuals (residing in a single household) who have applied for benefits; are currently receiving benefits; are minors whose status qualifies a parent or guardian for benefits; or who have received benefits under the Lifeline Program, which serves low-income individuals by providing these qualifying individuals with discounts on telephone service for their household.

Categories of Records in the System:

The categories of records in the system include, but are not limited to: The individual's name, residential address, date of birth, last four digits of social security number, tribal identification number, telephone number, means of qualification for Lifeline (*i.e.*, income or relevant program participation), Lifeline service initiation date and termination date, amount of Lifeline support received per month, date of the provision of Link-Up support (if applicable).

Authority for Maintenance of the System:

47 U.S.C. 151-154, 201-205, 214, 254, 403. 47 CFR 54.404-54.410.

Purpose(s):

The Lifeline Program provides discounts for voice telephony service, and the initial connection charge in tribal areas to support such service, to qualifying low-income individuals (*i.e.*, one Lifeline telephone service per household). Individuals may qualify for Lifeline through proof of income or proof of participation in another qualifying program. The Lifeline Program system of records covers the PII that the Eligible Telecommunications Carriers (ETCs) must provide to prevent the individuals in a single household from receiving more than one Lifeline Program benefit, as

required by 47 CFR 54.404 and 54.410. The Lifeline Program system of records also covers the PII that enables USAC to recertify the eligibility of current Lifeline Program subscribers of ETCs who have elected this option, as required by 47 CFR 54.410. The PII in WCB-1 will include:

1. The information that is used to determine whether an individual in a household, who is applying for a Lifeline Program benefit, is already receiving a Lifeline Program benefit from one or more providers. In order to determine if this information is in fact accurate, the information is confirmed with a third-party verification service not in the control of USAC or the Commission;
2. The information that ETCs that elect to have USAC recertify their Lifeline subscribers. These ETCs must provide USAC with a subscriber list containing PII that includes the first name, last name, address, Lifeline telephone number, date of birth, and last four digits of social security number for each subscriber; and
3. The information that is contained in the records of the inquiries that the ETCs will make to the Lifeline Program contractor's call center to verify that an individual is eligible to participate in the Lifeline Program. USAC will designate a third party contractor to establish this call center as part of USAC's "exception management practices." The contractor will operate this call center, which individuals may use who are seeking to participate in or are already participating in the Lifeline Program. These individuals may call the center to ensure that they have not been improperly denied access to Lifeline Program benefits through the verification process. Any information generated by these inquiries will constitute a separate, distinct database, which will include, but is not limited to, recordings of live agent calls to be stored for 30 days from the date of the call, identity of the user initiating the request, brief description of the request, type of request, identification of the USAC-approved script used in responding to the request, resolution status, and whether the request was escalated (*i.e.*, if the agents escalates the issue to the agent's manager or USAC program personnel). This information will be used, among other things, to verify the accuracy of the information stored in the Lifeline system (*i.e.*, to determine the accuracy of the PII provided by the ETC.) Records in the Lifeline system are available for public inspection after redaction of information that could identify the individual participant, such as the individual's name(s), date of birth, last four digits of social security number, tribal ID number, telephone number, or other PII.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

Information about individuals in this system of records may routinely be disclosed under the following conditions. The FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected in each of these cases.

1. FCC Program Management--A record from this system may be accessed and used by the FCC and USAC employees to conduct official duties associated with the management and operation of the Lifeline Program and the National Lifeline Accountability Database (NLAD), as directed by the Commission. While the FCC will not routinely access the information in this system, information which includes, but is not limited to USAC audits and/or investigations of the ETCs (for the purposes of eliminating waste, fraud, and abuse in this program) may be shared with the FCC's Enforcement Bureau (EB), Wireline Competition Bureau (WCB), Office of Managing Director (OMD), and/or Office of Inspector General (OIG), as necessary;
2. Third Party Contractors--A record from this system may be disclosed to an employee of a third-party contractor to conduct the verification process that allows the ETC to determine the accuracy of the PII provided by the ETC to the system of records. When an employee of a third-party contractor, responsible for exception management, verifies the eligibility of the consumer subject to an exception;
3. State Agencies and Authorized Entities--A record from this system may be disclosed to designated state agencies and other authorized entities, which include, but are not limited to, state public utility commissions, and their agents, as is consistent with applicable Federal and State laws, to administer the Lifeline Program on behalf of an ETC in that state and to perform other management and oversight duties and responsibilities, as necessary;
4. FCC Enforcement Actions--When a record in this system involves an informal complaint filed alleging a violation of

FCC Rules and Regulations by an applicant, licensee, certified or regulated entity or an unlicensed person or entity, the complaint may be provided to the alleged violator for a response. When an order or other Commission-issued document that includes consideration of an informal complaint or complaints is issued by the FCC to implement or to enforce FCC Rules and Regulations, the complainant's name may be made public in that order or document. Where a complainant in filing his or her complaint explicitly requests that confidentiality of his or her name from public disclosure, the Commission will endeavor to protect such information from public disclosure. Complaints that contain requests for confidentiality may be dismissed if the Commission determines that the request impedes the Commission's ability to investigate and/or resolve the complaint;

5. Congressional Inquiries--When requested by a Congressional office in response to an inquiry that an individual made to the Congressional office for the individual's own records;

6. Congressional Investigations and Inquiries--A record from this system may be disclosed to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, for the purposes of an official Congressional investigation;

7. Government-wide Program Management and Oversight--When requested by the National Archives and Records Administration (NARA), the Office of Personnel Management, the General Services Administration (GSA), and/or the Government Accountability Office (GAO) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906 (such disclosure(s) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

8. Income and Program Eligibility Records--A record from this system may be disclosed to the appropriate Federal and/or State authorities for the purposes of determining whether a household may participate in the Lifeline Program;

9. Law enforcement and Investigation--Where there is an indication of a violation or potential violation of a statute, regulation, rule, or order, records from this system may be shared with appropriate federal, state, or local authorities either for purposes of obtaining additional information relevant to a FCC decision or for referring the record for investigation, enforcement, or prosecution by another agency, *e.g.*, Internal Revenue Service (IRS) to investigate income eligibility verification;

10. Adjudication and Litigation--Where by careful review, the Agency determines that the records are both relevant and necessary to litigation and the use of such records is deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records, these records may be used by a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation;

11. Department of Justice--A record from this system of records may be disclosed to the Department of Justice (DOJ) or in a proceeding before a court or adjudicative body when:

(a) The United States, the Commission, a component of the Commission, or, when represented by the government, an employee of the Commission is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Commission determines that the disclosure is relevant or necessary to the litigation; and

12. Breach of Federal Data--A record from this system may be disclosed to appropriate agencies, entities (including USAC), and persons when: (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity (including USAC)) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to

respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

None.

Policies and Practice for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

The information pertaining to the Lifeline Program includes electronic records, files and data and paper documents, records, and files. Both USAC and the contractor will jointly manage and the electronic data, which will be stored in the computer network databases housed at USAC and at the contractor, and the paper documents, which will be stored in filing cabinets in their respective offices at USAC and the contractor.

Retrievability:

Information in the Lifeline Program may be retrieved by various identifiers, including, but not limited to the individual's name, last four digits of the Social Security Number (SSN), tribal identification number, date of birth, phone number, and residential address.

Safeguards:

Access to the electronic files is restricted to authorized USAC and the contractor's supervisors and staff. The FCC requires that these computer network databases be protected by various security protocols, which include, but are not limited to, controlled access, passwords, and other security features. In addition, data in the network servers for both USAC and the contractor will be routinely backed-up. The servers will be stored in secured environments to protect the data.

The paper documents are maintained in file cabinets that are located in the USAC and the contractor's office suites. The file cabinets are locked when not in use and at the end of the business day. Access to these files is restricted to authorized USAC and the contractor's staffs.

Retention and Disposal:

The National Archives and Records Administration (NARA) has not established a records schedule for the information in the Lifeline Program. Consequently, until NARA has approved a records schedule, USAC will maintain the information in the Lifeline Program in accordance with the requirements of the *Lifeline Reform Order*. The *Lifeline Reform Order* states that information in the Lifeline Program is maintained for ten years after the consumer de-enrolls from the Lifeline Program. *See Lifeline and Link Up Reform and Modernization et al.*, WC Docket No. 11-42 *et al.*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6740, para. 195 (2012). Disposal of obsolete or out-of-date paper documents and files is by shredding. Electronic data, files, and records are destroyed by electronic erasure.

System Manager(s) and Address(es):

USAC maintains the Lifeline Program for the FCC.

Address inquiries to the Universal Service Administrative Company (USAC), 2000 L Street NW., Suite 200, Washington, DC 20036; or

Wireline Competition Bureau (WCB), 445 12th Street SW., Washington, DC 20554.

Notification Procedure:

Universal Service Administrative Company (USAC), 2000 L Street NW., Suite 200, Washington, DC 20036;

Wireline Competition Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or

Privacy Analyst, Performance Evaluation and Records Management (PERM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Access Procedures:

Universal Service Administrative Company (USAC), 2000 L Street NW., Suite 200, Washington, DC 20036;

Wireline Communications Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or

Privacy Analyst, Performance Evaluation and Records Management (PERM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Contesting Record Procedures:

Universal Service Administrative Company (USAC), 2000 L Street NW., Suite 200, Washington, DC 20036;

Wireline Competition Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or

Privacy Analyst, Performance Evaluation and Records Management (PERM), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

Record Source Categories:

The sources for the information in the Lifeline Program include, but are not limited to:

1. The information that the ETCs must provide prior to enrolling subscribers and/or to re-certifying subscribers (in qualifying households) for participation in the Lifeline Program; and
2. The information that individuals (in qualifying households) must provide to determine their households' eligibility for participation in the Lifeline Program, *e.g.*, participating in other qualifying programs and/or services.

Exemptions Claimed for the System:

None.

[\[Return to TOP\]](#)

Privacy Act Regulations

Chapter I — Federal Communications Commission

Part 0 — COMMISSION ORGANIZATION

Subpart E--Privacy Act Regulations

0.551 Purpose and scope; definitions.

0.552 Notice identifying Commission systems of records.

0.553 New uses of information.

0.554 Procedures for requests pertaining to individual records in a system of records.

0.555 Disclosure of record information to individuals.

0.556 Request to correct or amend records.

0.557 Administrative review of an initial decision not to amend a record.

0.558 Advice and assistance.

0.559 Disclosure of disputed information to persons other than the individual to whom it pertains.

0.560 Penalty for false representation of identity.

0.561 Exemptions.

Authority: Secs. 4, 303, 49 Stat. as amended, 1066, 1082 (47 U.S.C. 154, 303).

Source: 40 FR 44512, Sept. 26, 1975, unless otherwise noted.

Subpart E--Privacy Act Regulations

§ 0.551 Purpose and scope; definitions.

(a) The purpose of this subpart is to implement the Privacy Act of 1974, 5 U.S.C. 552(a), and to protect the rights of the individual in the accuracy and privacy of information concerning him which is contained in Commission records. The regulations contained herein cover any group of records under the Commission's control from which information about individuals is retrievable by the name of an individual or by some other personal identifier.

(b) In this subpart:

(1) *Individual* means a citizen of the United States or an alien lawfully admitted for permanent residence;

(2) *Record* means any item, collection or grouping of information about an individual that is maintained by the Commission, including but not limited to, such individual's education, financial transactions, medical history, and criminal or employment history, and that contains such individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(3) *System of Records* means a group of records under the control of the Commission from which information is retrievable by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(4) *Routine Use* means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

(5) *System Manager* means the Commission official responsible for the storage, maintenance, safekeeping, and disposal of a system of records.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 49 FR 13368, Apr. 4, 1984]

§ 0.552 Notice identifying Commission systems of records.

The Commission publishes in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, including for each system of records:

(a) The name and location of the system;

(b) The categories of individuals on whom records are maintained in the system;

(c) The categories of records maintained in the system;

(d) Each routine use of the records contained in the system, including the categories of users and the purposes of such use;

(e) The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(f) The title and business address of the system manager;

(g) The address of the agency office to which inquiries should be addressed and the addresses of locations at which the individual may inquire whether a system contains records pertaining to himself;

(h) The agency procedures whereby an individual can be notified how access can be gained to any record pertaining to that individual contained in a system of records, and the procedure for correcting or contesting its contents; and

(i) The categories of sources of records in the system.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 49 FR 13368, Apr. 4, 1984]

§ 0.553 New uses of information.

Before establishing a new routine use of a system of records, the Commission will publish a notice in the *Federal Register* of its intention to do so, and will provide at least 30 days for public comment on such use. The notice will contain:

(a) The name of the system of records for which the new routine use is to be established;

(b) The authority for the system;

(c) The categories of records maintained;

(d) The proposed routine use(s); and

(e) The categories of recipients for each proposed routine use.

§ 0.554 Procedures for requests pertaining to individual records in a system of records.

(a) Upon request, the Commission will notify individuals as to whether it maintains information about them in a system of records and, subject to the provisions of § 0.555(b), will disclose the substance of such information to that individual. In order to properly request notification or access to record information, reference must be made to the Notice described in § 0.552. A table of contents, which is alphabetized by bureau or office, precedes the system descriptions and allows members of the public to easily identify record systems of interest to them. An individual may inquire into information contained in any or all systems of records described in the Notice. However, each inquiry shall be limited to information from systems located within a single bureau or office and shall be addressed to that bureau or office.

(b) Reasonable identification is required of all individuals making requests pursuant to paragraph (a) of this section in order to assure that disclosure of any information is made to the proper person.

(1) Individuals who choose to register a request for information in person may verify their identity by showing any two of the following: social security card; drivers license; employee identification card; medicare card; birth certificate; bank credit card; or other positive means of identification. Documents incorporating a picture and/or signature of the individual shall be produced if possible. If an individual cannot provide suitable documentation for identification, that individual will be required to sign an identity statement stipulating that knowingly or willfully seeking or obtaining access to records about another person under false pretenses is punishable by a fine of up to \$5,000.

Note:

An individual's refusal to disclose his social security number shall not constitute cause in and of itself, for denial of a request.

(2) All requests for record information sent by mail shall be signed by the requestor and shall include his printed name, current address and telephone number (if any). Commission officials receiving such requests will attempt to verify the identity of the requestor by comparing his or her signature to those in the record. If the record contains no signatures and if positive identification cannot be made on the basis of other information submitted, the requestor will be required to sign an identity statement and stipulate that knowingly or willfully seeking or obtaining access to records about another person under false pretense is punishable by a fine of up to \$5,000.

(3) If positive identification cannot be made on the basis of the information submitted, and if data in the record is so sensitive that unauthorized access could cause harm or embarrassment to the individual to whom the record pertains, the Commission reserves the right to deny access to the record pending the production of additional more satisfactory evidence of identity.

Note:

The Commission will require verification of identity only where it has determined that knowledge of the existence of record information or its substance is not subject to the public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, as amended.

(c) All requests for notification of the existence of record information or for access to such information shall be delivered to the business address of the system manager responsible for the system of records in question, except that requests relating to official personnel records shall be addressed to the Associate Managing Director--Personnel Management. Such addresses can be found in the *Federal Register* Notice described in § 0.552.

(d) A written acknowledgement of receipt of a request for notification and/or access will be provided within 10 days (excluding Saturdays, Sundays, and legal public holidays) to the individual making the request. Such an acknowledgement may, if necessary, request any additional information needed to locate a record. A search of all systems of records identified in the individual's request will be made to determine if any records pertaining to the individual are contained therein, and the individual will be notified of the search results as soon as the search has been completed. Normally, a request will be processed and the individual notified of the search results within 30 days (excluding Saturdays, Sundays, and legal holidays) from the date the inquiry is received. However, in some cases, as

where records have to be recalled from Federal Record Centers, notification may be delayed. If it is determined that a record pertaining to the individual making the request does exist, the notification will state approximately when the record will be available for personal review. No separate acknowledgement is required if the request can be processed and the individual notified of the search results within the ten-day period.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 49 FR 13368, Apr. 4, 1984]

§ 0.555 Disclosure of record information to individuals.

(a) Individuals having been notified that the Commission maintains a record pertaining to them in a system of records may request access to such record in one of three ways: by in person inspection at the system location; by transfer of the record to a nearer location; or by mail.

(1) Individuals who wish to review their records at the system location must do so during regular Commission business hours (8:00 a.m.-4:30 p.m., Monday through Friday). For personal and administrative convenience, individuals are urged to arrange to review a record by appointment. Preferences as to specific dates and times can be made by writing or calling the system manager responsible for the system of records in question at least two days in advance of the desired appointment date, and by providing a telephone number where the individual can be reached during the day in case the appointment must be changed. Verification of identity is required as in § 0.554(b)(1) before access will be granted an individual appearing in person. Individuals may be accompanied by a person of his or her own choosing when reviewing a record. However, in such cases, a written statement authorizing discussion of their record in the presence of a Commission representative having physical custody of the records.

(2) Individuals may request that a record be transferred to a Commission field office or installation in the vicinity of his or her home and that access be granted at that location. The addresses of Commission field offices are listed in § 0.121. A request to transfer records must specify the exact location where the records should be sent and a telephone number to call when the information is available for review at the field location. Paragraph (a)(1) of this section regarding personal appointments, verification of identity accompanying persons, and disclosure of original records applies equally to this paragraph.

(3) Individuals may request that copies of records be sent directly to them. In such cases, individuals must verify their identity as § 0.554(b)(2) and provide an accurate return address. Records shall be sent only to that address.

(b) The disclosure of record information under this section is subject to the following limitations:

(1) Records containing medical information pertaining to an individual are subject to individual access under this section unless, in the judgment of the system manager having custody of the records after consultation with a medical doctor, access to such record information could have an adverse impact on the individual. In such cases, a copy of the record will be delivered to a medical doctor named by the individual.

(2) Classified material, investigative material compiled for law enforcement purposes, investigatory material compiled solely for determining suitability for Federal employment or access to classified information, and certain testing or examination material shall be removed from the records to the extent permitted in the Privacy Act of 1974, 5 U.S.C. 552(a). Section 0.561 of this subpart sets forth the systems of records maintained by the Commission which are either totally or partially exempt from disclosure under this subparagraph.

(c) No fee will be imposed if the number of pages of records requested is 25 or less. Requests involving more than 25 pages shall be submitted to the duplicating contractor (see § 0.456(a)).

(d) The provisions of this section in no way give an individual the right to access any information compiled in reasonable anticipation of a civil action or proceeding.

(e) In the event that a determination is made denying an individual access to records pertaining to that individual for any

reason, such individual may either:

(1) Seek administrative review of the adverse determination. Such a request shall be in writing and should be addressed to the system manager who made the initial decision. In addition, the request for review shall state specifically why the initial decision should be reversed.

(2) Seek judicial relief in the district courts of the United States pursuant to paragraph (g)(1)(B) of the Act.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 40 FR 58858, Dec. 19, 1975; 49 FR 13369, Apr. 4, 1984]

§ 0.556 Request to correct or amend records.

(a) An individual may request the amendment of information contained in their record. Except as otherwise provided in this paragraph, the request to amend should be submitted in writing to the system manager responsible for the records. Requests to amend the official personnel records of active FCC employees should be submitted to the Associate Managing Director--Human Resources Management, 445 12th Street, SW., Washington, D.C. 20554. Requests to amend official personnel records of former FCC employees should be sent to the Assistant Director for Work Force Information, Compliance and Investigations Group, Office of Personnel Management, 1900 E Street, NW., Washington, D.C. 20415. Any request to amend should contain as a minimum:

(1) The identity verification information required by § 0.554(b)(2) and the information needed to locate the record as required by § 0.554(a).

(2) A brief description of the item or items of information to be amended; and

(3) The reason for the requested change.

(b) A written acknowledgement of the receipt of a request to amend a record will be provided within 10 days (excluding Saturdays, Sundays, and legal public holidays) to the individual requesting the amendment. Such an acknowledgement may, if necessary, request any additional information needed to make a determination. There will be no acknowledgement if the request can be reviewed, processed, and the individual notified of compliance or denial within the 10 day period.

(c) The responsible system manager, or in the case of official personnel records of active FCC employees, the Associate Managing Director--Personnel Management, shall (normally within 30 days) take one of the following actions regarding a request to amend:

(1) If the system manager agrees that an amendment to the record is warranted, the system manager shall:

(i) So advise the individual in writing;

(ii) Correct the record in compliance with the individual's request; and

(iii) If an accounting of disclosures has been made, advise all previous recipients of the fact that the record has been corrected and of the substance of the correction.

(2) If the system manager, after an initial review, does not agree that all or any portion of the record merits amendment, the system manager shall:

(i) Notify the individual in writing of such refusal to amend and the reasons therefore;

(ii) Advise the individual that further administrative review of the initial decision by the full Commission may be sought pursuant to the procedures set forth in § 0.557. (In cases where the request to amend involves official personnel records, review is available exclusively from the Assistant Director for Work Force Information, Compliance and Investigations

Group, Office of Personnel Management, Washington, DC 20415; and

(iii) Inform the individual of the procedures for requesting Commission review pursuant to § 0.557.

(d) In reviewing a record in response to a request to amend, the system manager shall assess the accuracy, relevance, timeliness, or completeness of the record in light of each data element placed into controversy and the use of the record in making decisions that could possibly affect the individual. Moreover, the system manager shall adjudicate the merits of any request to delete information based on whether or not the information in controversy is both relevant and necessary to accomplish a statutory purpose required of the Commission by law or executive order of the President.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 45 FR 39850, June 12, 1980; 49 FR 13369, Apr. 4, 1984; 65 FR 58466, Sept. 29, 2000]

§ 0.557 Administrative review of an initial decision not to amend a record.

(a) Individuals have 30 days from the date of the determination not to amend a record consistent with their request to seek further administrative review by the full Commission. Such a request shall be in writing and should be addressed to either the system manager who made the initial adverse decision, or, in the case of official personnel records of active FCC employees, to the Assistant Director for Work Force Information, Compliance and Investigations Group, Office of Personnel Management, Washington, DC 20415. Any request for administrative review must:

(1) Clearly identify the questions presented for review (e.g., whether the record information in question is, in fact, accurate; whether information subject to a request to delete is relevant and necessary to the purpose for which it is maintained);

(2) Specify with particularity why the decision reached by the system manager is erroneous or inequitable; and

(3) Clearly state how the record should be amended or corrected.

(b) The Commission shall conduct an independent review of the record in controversy using the standards of review set out in § 0.556(d). It may seek such additional information as is necessary to make its determination. Final administrative review shall be completed not later than 30 days (excluding Saturdays, Sundays and legal public holidays) from the date on which the individual requests such review unless the Chairman determines that a fair and equitable review cannot be made within the 30 day period. In such event, the individual will be informed in writing of the reasons for the delay and the approximate date on which the review is expected to be completed.

(c) If upon review of the record in controversy the Commission agrees with the individual that the requested amendment is warranted, the Commission will proceed in accordance with § 0.556(c)(1) (i) through (iii).

(d) If after the review, the Commission also refuses to amend the record as requested, it shall:

(1) Notify the individual in writing of its refusal and the reasons therefore;

(2) Advise the individual that a concise statement of the reasons for disagreeing with the decision of the Commission may be filed;

(3) Inform the individual:

(i) That such a statement should be signed and addressed to the system manager having custody of the record in question;

(ii) That the statement will be made available to any one to whom the record is subsequently disclosed together with, at the Commission's discretion, a summary of its reasons for refusing to amend the record; and

(iii) That prior recipients of the record will be provided a copy of the statement of dispute to the extent that an accounting of such disclosures is maintained; and

(4) Advise the individual that judicial review of the Commission's decision not to amend the record in any district court of the United States is available.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 45 FR 39850, June 12, 1980; 49 FR 13369, Apr. 4, 1984]

§ 0.558 Advice and assistance.

Individuals who have questions regarding the procedures contained in this subpart for gaining access to a particular system of records or for contesting the contents of a record, either administratively or judicially, should write or call the Privacy Liaison Officer at the following address:

Federal Communications Commission, Office of General Counsel, 445 12th Street, SW., Washington, DC 20554.

Individuals who request clarification of the Notice described in § 0.552 or who have questions concerning the characterization of specific systems of records as set forth therein, should write or call the Privacy Liaison Officer at the following address:

Federal Communications Commission, Performance Evaluation and Records Management, Office of the Managing Director, 445 12th Street, SW., Washington, DC 20554

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 49 FR 13369, Apr. 4, 1984; 65 FR 58466, Sept. 29, 2000]

§ 0.559 Disclosure of disputed information to persons other than the individual to whom it pertains.

If the Commission determines not to amend a record consistent with an individual's request, and if the individual files a statement of disagreement pursuant to § 0.557(d)(2), the Commission shall clearly annotate the record so that the disputed portion becomes apparent to anyone who may subsequently have access to, use or disclose the record. A copy of the individual's statement of disagreement shall accompany any subsequent disclosure of the record. In addition, the Commission may include a brief summary of its reasons for not amending the record when disclosing the record. Such statements become part of the individual's record for granting access, but are not subject to the amendment procedures of § 0.556.

§ 0.560 Penalty for false representation of identity.

Any individual who knowingly and willfully requests or obtains under false pretenses any record concerning an individual from any system of records maintained by the Commission shall be guilty of a misdemeanor and subject to a fine of not more than \$5,000.

§ 0.561 Exemptions.

The following systems of records are totally or partially exempt from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552(a), and from §§ 0.554 through 0.557 of this subpart:

(a) *System name.* Radio Operator Records--FCC/FOB-1. Parts of this system of records are exempt pursuant to Section (k)(2) of the Act because they contain investigatory material compiled solely for law enforcement purposes.

(b) *System name.* Violators File (records kept on individuals who have been subjects of FCC field enforcement actions)--FCC/FOB-2. Parts of this system of records are EXEMPT because they are maintained as a protective service for individuals described in section 3056 of title 18, and because they are necessary for Commission employees to perform

their duties, pursuant to sections (k) (1), (2), and (3) of the Act.

(c) *System name.* Attorney Misconduct Files--FCC/OGC-2. This system of records is exempt pursuant to section 3(k)(2) of the Act because it is maintained for law enforcement purposes.

(d) *System name.* Licensees or Unlicensed Persons Operating Radio Equipment Improperly--FCC. Parts of this system of records are exempt pursuant to section 3(k)(2) of the Act because they embody investigatory material compiled solely for law enforcement purposes.

(e) *System name.* Personnel Investigation Records--FCC/Central-6. Parts of these systems of records are exempt because they embody investigatory material pursuant to sections 3(k)(2) and 3(k)(5) of the Act as applicable.

(f) *System name.* Criminal Investigative Files--FCC/OIG-1. Compiled for the purpose of criminal investigations. This system of records is exempt pursuant to section (j)(2) of the Act because the records contain investigatory material compiled for criminal law enforcement purposes.

(g) *System name.* General Investigative Files--FCC/OIG-2. Compiled for law enforcement purposes. This system of records is exempt pursuant to section (k)(2) of the Act because the records contain investigatory material compiled for law enforcement purposes.

(Secs. 4(i) and 303(n), Communications Act of 1934, as amended, 47 U.S.C. 154(i) and 303(n); 47 CFR 0.231(d))

[40 FR 44512, Sept. 26, 1975, as amended at 49 FR 13369, Apr. 4, 1984; 58 FR 11549, Feb. 26, 1993]

[\[Return to TOP\]](#)