

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 PRACTICES 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:

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

NOTIFICATION, RECORD ACCESS AND CONTESTING RECORD 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.

EXEMPTION FROM CERTAIN PROVISIONS OF THE ACT:

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.

Federal Communications Commission.

Marlene H. Dortch,
Secretary.

[FR Doc. 03–1195 Filed 1–17–03; 8:45 am]

BILLING CODE 6712–01–P