This document is scheduled to be published in the
Federal Register on 03/12/2018 and available online at
https://federalregister.gov/d/2018-04943, and on **FDsys.gov**

6712-01

FEDERAL COMMUNICATIONS COMMISSION

Privacy Act of 1974; System of Records.

AGENCY: Federal Communications Commission.

ACTION: Notice of a Modified System of Records.

SUMMARY: The Federal Communications Commission (FCC or Commission or Agency) has modified an existing system of records, FCC/OMD-16, Personnel Security Files, subject to the Privacy Act of 1974 as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of records maintained by the agency. The FCC's Security Operations Center (SOC) in the Office of Managing Director (OMD) uses this system of records to cover the personally identifiable information (PII) that is associated with the administration of the policies and activities that include, but are not limited to determining compliance with Federal regulations, and/or an individual's suitability for access to classified information and/or a security clearance; evaluating an applicant's suitability to perform contractual services for the FCC; evaluating an individual's suitability for Federal internships, including access to Federal systems and information; responding to complaints of threats, harassment, violence, or other inappropriate behavior at the FCC; and documenting security violations and related activities, including insider threats.

DATES: This action will become applicable on **[INSERT DATE OF PUBLICATION IN FEDERAL REGISTER]**. The routine uses in this action will become applicable on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless comments are received that require a contrary determination.

ADDRESSES: Send comments to Leslie F. Smith, Privacy Manager, Information Technology (IT), Room 1-C216, Federal Communications Commission, 445 12th Street, SW, Washington, D.C. 20554, or to Leslie.Smith@fcc.gov.

FOR FURTHER INFORMATION CONTACT: Leslie F. Smith, (202) 418-0217, or Leslie.Smith@fcc.gov (and to obtain a copy of the Narrative Statement and the Supplementary Document).

SUPPLEMENTARY INFORMATION: This notice serves to update and modify FCC/OMD-16, Personnel Security Files, to add insider threats to the list of purposes and to make other miscellaneous but necessary updates and changes since its previous publication. The substantive changes and modifications to the previously published version of the FCC/OMD-16 system of records include:

1. (a) Expansion of the system's purposes to add insider threats to the list of safety and security criteria that the Security Operations Center will use to evaluate and assign employees, contractors, and interns an appropriate security level and to guard against the potential risks posed by insider threats.
   (b) Deletion of the President's Program to Eliminate Waste, Fraud, and Abuse – there is no current information that this program is still in existence.
2. Expansion of the categories of individuals to include security personnel (contractors) to the list of individuals who are authorized to perform, provide, or use FCC facilities.
3. Expansion of the categories of records to add Taxpayer Identification Numbers (TINs), Personal Identity Verification (PIV) data, facial photographs and other biometric data, and office and personal e-mail addresses of FCC employees; personal telephone and e-mail address(es) of relatives who are Federal employees; financial information (in addition to tax data and credit reports) for employee background investigations; insider threat activity data concerning FCC employees; office and home e-mail addresses of witness(es), injured parties, and others as part of an investigation of violence, threats (including insider threats), harassment, and intimidation to the PII that this system will collect, maintain, and use.
4. Replacing two routine uses: (1) Litigation by the Department of Justice and (2) A Court or Adjudicative Body, with (1) Adjudication and Litigation.
5. Updating language and/or renumbering two routine uses: (2) Law Enforcement and Investigation; (3) Congressional Inquiries; (4) Government-wide Program Management and Oversight; (5) Contract Services, Grants, or Cooperative Agreements; (11) Labor Relations; and (13) National Security and

Intelligence Matters.

6. Adding eight new routine uses: (6) Non-FCC Individuals and Organizations to obtain information pertinent to an investigation from these individuals; (7) Complainants and Victims to provide the complainants and victims with information concerning an investigation involving them; (8) Office of Personnel Management (OPM) to OPM et al. to properly administer Federal personnel systems and related agencies' systems; (9) Employment, Clearances, Licensing, Contract, Grants, or other Benefit Decisions by the FCC to allow the Commission to obtain information relevant to a FCC decision concerning an employee; (10) Employment, Clearances, Licensing, Contract, Grants, or other Benefit Decisions by other than the FCC to allow the Commission to provide information relevant to another government agency's decision concerning an employee; (12) Security Officials and Investigators to provide information to the officials for liaison and training purposes on classified materials; and (14) Breach Notification to address the Commission's real or suspected data breach situations; and (15) Assistance to Federal Agencies and Entities for assistance with other Federal agencies' data breach situations. Routine Uses (14) and (15) are required by OMB Memorandum m-17-12.
7. Adding a new section: Reporting to a Consumer Reporting Agency to address valid and overdue debts owed by individuals to the FCC under the Debt Collection Act, as recommended by OMB.

The system of records is also updated to reflect various administrative changes related to the system managers and system addresses; policy and practices for storage, retrieval, and retention and disposal of the records; administrative, technical, and physical safeguards; and updated notification, records access, and contesting records procedures.

SYSTEM NAME AND NUMBER:

FCC/OMD-16, Personnel Security Files.

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:

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

SYSTEM MANAGER(S) AND ADDRESS:

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

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, 13587; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

PURPOSE(S):

The FCC's Security Operations Center (SOC) staff uses this information to document and support decisions that include, but are not limited to:

1. Determining compliance with Federal regulations and/or making 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. Evaluating an applicant's qualifications and suitability to perform contractual services for the U.S. Government and documenting such determinations;
3. Evaluating 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 documenting such determinations;

4. Taking action on, or responding to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees, and counseling employees; and
5. Documenting security violations, including but not limited to insider threats, and the resulting management actions that would be taken.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

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

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 Government or contracts; FCC contractors, experts, instructors, consultants, grantees, and all other individuals who may require regular, on-going access to the FCC's buildings and facilities, information technology (IT) 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, provide, or to use services in FCC facilities (either on an ongoing or occasional basis), including, but not limited to FCC credit union employees, security personnel, custodial staff, maintenance workers, food service workers, contractors, and employee assistance program staff;
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 agreements or other arrangements (both paid and unpaid), including, but not limited to students and interns; and
4. Individuals who have been accused of security violations, including potential insider threat activity.

CATEGORIES OF RECORDS IN THE SYSTEM:

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

1. The information, as applicable, that is needed to identify an individual, including but not limited to the individual's last, first, and middle names, and former name(s), Social Security Number (SSN)/Taxpayer Identification Number (TIN), Personal Identity Verification (PIV) data, date of birth,

birthplace, facial photograph(s) and/or other biometric data, home address, home telephone number(s), residential history, office and personal e-mail address(es), organizational (bureau/office) unit, and position title;

2. Background information that includes but is not limited to the individual's citizenship, types and dates of investigations, agency conducting investigation, investigation dates, security clearance(s)[1] and grant date(s), and position sensitivity level(s), and miscellaneous investigation comments and records;
3. Names of relatives, birth date(s), home address(es), personal telephone number, e-mail address(es), citizenship, and relatives who work for the Federal government;
4. Contact with foreign officials and foreign travel registries, as applicable;
5. Reports that include, but are not limited to information that determines the individual's qualifications for a position, including but not limited to the employee/applicant's employment/work history, summary report of investigation(s), results of suitability decision(s), employment references, and contact information, and educational/training institutions attended, degrees and certifications earned, and educational and training references;
6. Background information that includes but is not limited to what is required to investigate an individual's character, conduct, and behavior in the community where he or she lives or lived; criminal history, including but not limited to arrests and convictions for violations against the law; mental health history; drug use history; financial information that includes but is not limited to income tax return information, credit reports, and related financial information; reports that include but are not limited to information obtained from interviews with present and former supervisors, co-workers, associates, educators, and other related personal references and contact information;
7. Reports that include, but are not limited to inquiries with law enforcement agencies, employers, and reports of action after the Office of Personnel Management (OPM) or FBI Section 8(d) Full Field

[1] A security clearance (i.e., "Certificate of Clearance") is a government document authorizing a specific security status granted to an individual allowing the person access to classified information (state or organizational secrets) or to restricted areas, after completion of a thorough background check).

Investigation; Notices of Security Investigation and other information developed from "Certificates of Clearance,"[2] including. but not limited to date(s) of security clearances, requests for appeals, witness statements, investigator's notes, security violations, circumstances of violations, and agency action(s) taken;

8. Information needed to investigate allegations of FCC employee's misconduct, including but not limited to identifying any insider threats and related activities;
9. Information needed to investigate miscellaneous complaints not covered by the FCC's formal or informal grievance procedure;
10. Information including, but is not limited to what is needed to investigate violence, threats, harassment, intimidation, insider threat activity, or other inappropriate behavior causing an FCC employee, contractor, or visitor to fear for his/her personal safety in the FCC workplace: case number, victim's name, office telephone number, room number, office e-mail address, 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) and e-mail address(es) 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; and
11. Information obtained from sources that include but are not limited to 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.[3]

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

---

[2] Op cite.

[3] This system of records does not duplicate or supersede the Office of Personnel Management (OPM): OPM/Central-9 system of records, which covers the investigations OPM and its contractors conduct on behalf of other agencies at: https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-central-9-personnel-investigations-records.pdf.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FCC as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows. 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.

1. Adjudication and Litigation – To disclose information to the Department of Justice (DOJ), or other administrative body before which the FCC is authorized to appear, 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 DOJ or the FCC has agreed to represent the employee; or (d) the United States is a party to litigation or has an interest in such litigation, and the use of such records by DOJ or the FCC is deemed by the FCC to be relevant and necessary to the litigation.
2. Law Enforcement and Investigation – To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the FCC becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;
3. Congressional Inquiries – To provide information to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of that individual;
4. Government-wide Program Management and Oversight – To the National Archives and Records Administration (NARA) for use in its records management inspections ; to the Government Accountability Office (GAO) for oversight purposes; to the U.S. Department of Justice (DOJ) to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or to the Office of Management and Budget (OMB) to obtain that office's advice regarding obligations under the Privacy Act;
5. Contract Services, Grants, or Cooperative Agreements – 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.

6. Non-FCC Individuals and Organizations – To individuals, including former FCC employees, and organizations in the course of an investigation to the extent necessary to obtain information pertinent to the investigation.
7. Complainants and Victims – To individual complainants and/or victims to the extent necessary to provide such individuals with information and explanations concerning the progress and/or results of the investigation or case arising from the matter of which they complained and/or of which they were a victim.
8. Office of Personnel Management (OPM) – To OPM management, Merit Systems Protection Board, Equal Opportunity Employment Commission, Federal Labor Relations Authority, and the Office of Special Counsel for the purpose of properly administering Federal personnel systems or other agencies' systems in accordance with applicable laws, Executive Orders, and regulations.
9. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the FCC – To a Federal, State, local, foreign, tribal, or other public agency or authority 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 hiring or retention of an employee or other personnel action, the issuance or retention of a security clearance, the classifying of jobs, the letting of a contract, or the issuance or retention 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 decisions on the matter.
10. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by Other than the FCC – To a Federal, State, local, foreign, tribal, or other public agency or authority of the fact that this system of records contains information relevant to the hiring or retention of an employee, the

issuance or retention of a security clearance, the conducting of a suitability or security investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance or retention of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the agency's decision on the matter. 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.

11. Labor Relations – 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.
12. Security Officials and Investigators – To Security Officials and investigators of Federal Government agencies or departments for liaison or training purposes where appropriate during meetings, conferences, or training courses involving access to classified materials.
13. National Security and Intelligence Matters – 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.
14. Breach Notification – To appropriate agencies, entities, and person when (1) the Commission suspects or has confirmed that there has been a breach of the system of records; (2) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and

persons is reasonably necessary to assist in connection with Commission efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

15. Assistance to Federal Agencies and Entities – To another Federal agency or Federal entity, when the Commission determines that information from this system is reasonably necessary to assist the recipient agency or entity in: (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, program, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

REPORTING TO A CONSUMER REPORTING AGENCY

In addition to the routine uses listed above, the Commission may share information from this system of records with a consumer reporting agency regarding an individual who has not paid a valid and overdue debt owed to the Commission, following the procedures set out in the Debt Collection Act, 31 U.S.C. 3711(e).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Information in this system is maintained as follows:

1. Electronic data, records, and files are maintained in a stand-alone computer database hosted on FCC's computer network; and
2. The paper documents, records, and files are stored in file folders in security containers in "non-public" rooms of the SOC office suite. These containers are locked when not in use and/or at the end of the day.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by an individual's name or Social Security Number (SSN).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records in this information system are retained and disposed of in accordance with General Records Schedule (GRS) 18, item 22a, approved by the National Archives and Records Administration (NARA). Both electronic and paper 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. 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.

In accordance with NARA guidelines, the FCC destroys paper records are 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's Records Management Office.

ADMINSTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. The electronic records, data, and files are maintained in the FCC computer network databases, which are protected by the FCC's IT privacy safeguards, a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal IT privacy standards, including those required by the National Institute of Standard and Technology (NIST) and the Federal Information Security Modernization Act of 2014 (FISMA). The protocols cover all electronic records, files, and data, including those that are housed in the FCC's computer network databases, and those information system databases that are housed at the FCC's authorized contractor(s).
2. The paper documents and files are stored in approved security containers, which are locked when not in use and/or at the end of the business day. The security containers are located in a secure "non-public" part of the Security Operations Center (SOC) office suite. All SOC access points are monitored and controlled. Admittance to the SOC office suite is limited to approved SOC and administrative personnel. Access to the IT offices is via a key and card-coded door.
3. Some paper records (limited in number and scope) are also kept in the FCC's regional offices and laboratory facilities. These records are stored in locked metal file cabinets in locked rooms, which

comply with Federal security requirements.

4. Only SOC staff and authorized contractors (including the contractors who maintain the FCC's computer network) may have access to the electronic data and the paper document records and files. As a further measure, access to these electronic records is restricted to the SOC staff and contractors who have a specific role in the Personal Identity Verification (PIV) process that requires their access to background investigation information and related SOC functions. The SOC maintains an audit trail to monitor access.
5. Furthermore, as part of these privacy and security requirements, SOC staff and contractors must complete training specific to their roles to ensure that they are knowledgeable about how to protect PII.

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 procedures for this system of records.

CONTESTING RECORD 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 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.

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 Sections 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.)

HISTORY:

The FCC last gave full notice of this system of records, FCC/OMD-16, Personnel Security Files, by publication in the Federal Register on September 25, 2006 (71 FR 55787, 55790).

Federal Communications Commission.

Marlene H. Dortch,
Secretary.
[FR Doc. 2018-04943 Filed: 3/9/2018 8:45 am; Publication Date: 3/12/2018]