FEDERAL COMMUNICATIONS COMMISSION

[FR ID: **211947]**

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, Commission, or Agency) has modified an existing system of records, FCC/OMD-30, FCC Visitors Database, 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 to maintain 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 SOC to gain admittance to the FCC headquarters buildings and other FCC facilities.

DATES: This modified system of records will become effective on **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written comments on the routine uses are due by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The routine uses in this action will become effective 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 Brendan McTaggart, Attorney-Advisor, Office of General Counsel, Federal Communications Commission, 45 L Street, NE, Washington, DC 20554, or to privacy@fcc.gov.

FOR FURTHER INFORMATION CONTACT: Brendan McTaggart, (202) 418-1738, or privacy@fcc.gov.

SUPPLEMENTARY INFORMATION: This notice serves to update and modify FCC/OMD-30 as a result of the various necessary changes and updates. The substantive changes and modifications to the previously published version of the FCC/OMD-30 system of records include:

1. Adding one new routine use: (8) Assistance to Federal Agencies and Entities Related to Breaches, the addition of which is required by OMB M-17-12;

2. Updating and/or revising language in six routine uses (listed by current routine use number): (1) Litigation (formerly "Litigation by the Department of Justice"); (2) Adjudication (formerly "Court or Adjudicative Body"); (3) Law Enforcement and Investigation (formerly "Department of State, Department of Homeland Security, and other Federal Agencies"; (4) Government-wide Program Management and Oversight; (5) Congressional Inquiries; (6) Nonfederal Personnel (formerly "Contract Services, Grants, or Cooperative Agreements"); and (7) Breach Notification, the modification of which is required by OMB M-17-12.

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, retention, disposal and retrieval of the information; administrative, technical, and physical safeguards; and updated notification, records access, and contesting records procedures.

SYSTEM NAME AND NUMBER: FCC/OMD-30, FCC Visitors Database.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Security Operations Center (SOC), Office of the Managing Director (OMD), Federal Communications Commission (FCC), 45 L St NE, Washington, DC 20554.

SYSTEM MANAGER(S): SOC, OMD, FCC, 45 L St NE, Washington, DC 20554.

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; National Defense

Authorization Act for FY 1996 (Pub. L. No. 104-106, sec. 5113); E- Government Act of 2002 (Pub. L. No. 107-347, sec. 203); and Federal Property and Administrative Act of 1949, as amended (Pub. L. No. 81-152).

PURPOSE(S) OF THE SYSTEM: 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 SOC to gain admittance to the FCC headquarters buildings and other FCC facilities.

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 may 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 or wireless (cell) phone numbers, correspondence related to information required to obtain visitor entry to the FCC, and purpose(s) for visiting the FCC.

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.

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—To disclose records to the Department of Justice (DOJ) when: (a) the FCC or any component thereof; (b) any employee of the FCC in their official capacity; (c) any employee of the FCC in their individual capacity where the DOJ or the FCC 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.

2. Adjudication—To disclose records in a proceeding before a court or adjudicative body, when: (a) the FCC or any component thereof; or (b) any employee of the FCC in their official capacity; or (c) any employee of the FCC in their individual capacity; 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.

3. Law Enforcement and Investigation—When the FCC investigates any violation or potential violation of a civil or criminal law, regulation, policy, executed consent decree, order, or any other type of compulsory obligation and determines that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law, regulation, policy, consent decree, order, or other compulsory obligation, the FCC may disclose pertinent information as it deems necessary to the target of an investigation, as well as with the appropriate Federal, State, local, Tribal, international, or multinational agencies, or a component of such an agency, responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, order, or other compulsory obligation.

4. Government-wide Program Management and Oversight—To disclose information to the 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. Congressional Inquiries—To provide information to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the written request of that individual.

6. Non-Federal Personnel—To disclose information to non-Federal personnel, including contractors, other vendors (*e.g.*, identity verification services), grantees, and 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.

7. Breach Notification—To appropriate agencies, entities, and persons when (a) the Commission suspects or has confirmed that there has been a breach of the system of records; (b) 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 (c) 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 breach or to prevent, minimize, or remedy such harm.

8. Assistance to Federal Agencies and Entities Related to Breaches—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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: The information in the FCC Visitors Database includes electronic records, files, and electronic records, files, and data that are stored in the FCC's computer network databases.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: 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.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in the FCC Visitors Database are retained and disposed of in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.6, Security Management Records, DAA-GRS-2021-0001.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The electronic records, files, and data are stored within FCC or a vendor's accreditation boundaries and maintained in a database housed in the FCC's or vendor's computer network databases. Access to the files is restricted to authorized employees and contractors, including IT staff, contractors, and vendors who maintain the IT networks and services. Other employees and contractors may be granted access on a need-to-know basis. The files and records are protected by the FCC and third-party privacy safeguards, a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal privacy standards, including those required by the Federal Information Security Modernization Act of 2014 (FISMA), OMB, and the National Institute of Standards and Technology (NIST).

RECORD ACCESS PROCEDURES: Individuals wishing to request access to and/or amendment of records about themselves should follow the Notification Procedures below.

CONTESTING RECORD PROCEDURES: Individuals wishing to contest information pertaining to him or her in the system of records should follow the Notification Procedures below.

NOTIFICATION PROCEDURES: Individuals wishing to determine whether this system of records contains information about themselves may do so by writing to privacy@fcc.gov.

Individuals requesting record access or amendment must also comply with the FCC's Privacy Act regulations regarding verification of identity as required under 47 CFR part 0, subpart E.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 77 FR 31851 (May 30, 2012)

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2024-06959 Filed: 4/1/2024 8:45 am; Publication Date: 4/2/2024]