network computer databases. Other FCC staff and contractors may be granted access to this information, only on a ''need-to-know'' basis. The COALS, CDBS, and LMS databases are part of the FCC's computer network databases. The records 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. The electronic 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), the Office of Management and Budget (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 request access to and/or amendment of records about themselves 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 access must also comply with the FCC's Privacy Act regulations regarding verification of identity to gain access to records as required under 47 CFR part 0, subpart E.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

81 FR 72047 (October 19, 2016)

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2024–20847 Filed 9–12–24; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 243635]

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) proposes to modify an existing system of records, FCC/MB–2, Broadcast Station Public Inspection Files, which has been renamed FCC/MB–2, Online Public Inspection File. The Commission requires television broadcasters to submit their public filing information to the FCC to be posted in an online public inspection file. In 2016, the Commission expanded its Online Public Inspection File (OPIF) requirements to cable operators, satellite TV (also referred to as ''Direct Broadcast Satellite'' or ''DBS'') providers, broadcast radio licensees, and satellite radio (also referred to as ''Satellite Digital Audio Radio Services'' or ''SDARS'') licensees. This system of records covers the personally identifiable information (PII) that may be contained in an OPIF.

DATES: This modified system of records will become effective on September 13, 2024. Written comments on the routine uses are due by October 15, 2024. The routine uses in this action will become effective on October 15, 2024 unless comments are received that require a contrary determination.

ADDRESSES: Send comments to Brendan McTaggart, Federal Communications Commission, 45 L Street NE, Washington, DC 20554, or *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/MB–2 as a result of various necessary changes and updates. The substantive changes and modifications to the previously published version of the FCC/MB–2 system of records include:

1. Updating the SORN to reflect the addition of cable operators, DBS providers, broadcast radio licensees, and SDARS licensees, and changing the name of the system to ''Online Public Inspection File;''

2. Updating the Purposes, Categories of Records, Categories of Individuals, and Record Source Categories to reflect the collection of Equal Employment Opportunity (EEO) and related data through FCC Form 2100 Schedule 396 Broadcast Equal Employment Opportunity Program Report (Form 396–B), annual EEO Public File Reports (certain years of which can also be attached to Form 396–B, attached to the Multichannel Video Program Distributor EEO Program Report (Form 396–C), or submitted in response to an EEO audit), and audit responses related to the administration of the Commission's responsibilities under 47 CFR 73.2080; and adding the Enforcement Bureau to System Location and System Manager, to reflect the Bureau's role in enforcing the Commission's EEO requirements;

3. Updating the language in the Security Classification to follow OMB guidance;

4. Otherwise modifying the language in the Categories of Individuals and Categories of Records to be consistent with the language and phrasing now used in FCC SORNs;

5. Deleting three former routine uses (listed by the routine use number in the previous iteration of this SORN: (9) FCC Enforcement Actions, which is duplicative of the expanded Law Enforcement and Investigation routine use in this notice; and (10) Due Diligence Inquiries and (11) Financial Obligations under the Debt Collection Acts, both of which are no longer applicable.

6. Adding one new routine use (listed by the routine use number provided in this SORN): (8) Assistance to Federal Agencies and Entities Related to Breaches, the addition of which is required by OMB M–17–12;

7. Updating and/or revising language in seven routine uses (listed by the routine use number provided in this SORN): (2) Law Enforcement and Investigation; (3) Litigation and (4) Adjudication (now two separate routine uses); (5) Congressional Inquiries; (6) Government-wide Program Management and Oversight; (7) Breach Notification, the modification of which is required by OMB M–17–12; and (9) Nonfederal Personnel.

8. Updating the SORN to include the National Archives and Records Administration (NARA) records schedule DAA–0173–2020–0003, EEO Audits.

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/MB–2, Online Public Inspection File.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Media Bureau (MB) and Enforcement Bureau (EB), Federal Communications Commission (FCC), 45 L Street NE, Washington, DC 20554.

SYSTEM MANAGER(S):

MB and EB, FCC, 45 L Street NE, Washington, DC 20554.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

47 U.S.C. 151, 152, 154(i), 154(j), 303, 307, 315, and 335.

PURPOSE(S) OF THE SYSTEM:

The Commission requires television broadcasters to submit their public filing information to the FCC to be posted in an online public inspection file. In 2016, the Commission expanded its OPIF requirements to cable operators, DBS providers, broadcast radio licensees, and SDARS licensees. This system of records covers the PII that may be contained in an OPIF. This includes information related to individuals associated with broadcast entities and SDARS licensees as well as individuals identified in EEO data (including the name of any EEO complainants) collected through Form 396–B pursuant to 47 CFR 73.2080 as well as in audit responses. EEO data are also provided in EEO Public File Reports (including PII related to recruitment and referral sources), which are uploaded to OPIF annually and, in certain years, are attached to Form 396–B and/or an EEO audit response. Further, this system of records also includes information related to individuals associated with cable operators and DBS providers identified in EEO data provided in annual EEO Public File Reports (including PII related to recruitment and referral sources), which are required to be uploaded to OPIF annually, and, every fifth year, the most recent report must be attached by cable operators and DBS providers to the Supplemental Investigation Sheet (SIS) of the Form 396–C, under 47 CFR 76.77. The Commission hosts OPIF in an online, publicly available database for the purpose of making the files more accessible to the public.

This system also includes information about individuals who are required to file personal information pertaining to their political campaigns, including requests for broadcast time made by or on behalf of a candidate and the disposition of those requests, information regarding other appearances by candidates (excluding those in certain news programming exempt from the equal opportunities provision), and information about issue advertising that communicates a message relating to any political matter of national importance. Requiring these entities to maintain complete and up to date political files is critical because the information in these files directly affects, among other things, the statutory rights of opposing candidates to request equal opportunities under Section 315(a) of the Communications Act and present their positions to the public prior to an election. In addition, the political files allow the public to verify that Commission licensees and regulatees have complied with their obligations relating to use of their facilities by candidates for political office and to obtain information about entities sponsoring candidate and issue advertisements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals in this system include: (1) Individuals who are required to file personal information pertaining to their political campaigns, as described above; (2) Individuals who are associated with a television or radio broadcast station licensee, cable operator, DBS provider, or SDARs licensee and are required to submit information under 47 CFR 73.3526, 73.3527, 25.701, 25.702, and 76.1700; and (3) Individuals filing Form 396–B on behalf of broadcast stations and SDARS licensees and individuals who have filed discrimination complaints involving those licensees and are named in attachments to Form 396–B, which is required under 47 CFR 73.2080, and individuals identified in audit responses and EEO Public File Reports; (4) Individuals associated with EEO data provided by cable operators and DBS providers in annual EEO Public File Reports, including the year subject to SIS which is attached to the Form 396–C.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records in this system may include an individual's name, home address, home telephone number, personal cell phone number, personal email address(es), personal fax number, and other personal information that stations may include in their public files, and which may be included in the documents, files, and records (including Form 396) that television and radio broadcast stations, cable operators, DBS providers, SDARS licensees, and certain individuals are required to either submit to the FCC or to post in the FCC's Online Public Inspection File.

RECORD SOURCE CATEGORIES:

The sources for the information in the Online Public Inspection File include the documents, files, and records (including Form 396, EEO Public File Reports, and, as applicable, responses to audit letters) that television and radio broadcasters, cable operators, DBS providers, and SDARS licensees are required to make available for public inspection in OPIF, as well as information imported from the FCC Licensing and Management System (LMS).

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 in the Online Public Inspection File are available for public inspection on the FCC's website.

2. 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, or order.

3. Litigation—Records may be disclosed to the Department of Justice (DOJ) 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 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, and the use of such records by the Department of Justice is for a purpose that is compatible with the purpose for which the FCC collected the records.

4. Adjudication—Records may be disclosed 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 his or her official capacity; or (c) any employee of the FCC in his or her 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, and that the use of such records is for a purpose that is compatible with the purpose for which the agency collected the records.

5. Congressional Inquiries—Information may be provided to a Congressional office in response to an inquiry from that Congressional office made at the written request of the individual to whom the information pertains.

6. Government-wide Program Management and Oversight—Information may be disclosed to 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.

7. Breach Notification—Records may be disclosed 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 system, 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—Records may be disclosed 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.

9. Non-Federal Personnel—Records may be disclosed 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 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

This an electronic system of records that resides on the FCC's network or on an FCC vendor's network.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

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

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

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. National Archives and Records Administration (NARA) Records Schedule N1–173–86–2, authorizes permanent retention of original documents of information reported pursuant to 47 CFR 73.3526, 73.3527, 25.701, 25.702, and 76.1700 of the Commission's rules. EEO audit records are retained in accordance with NARA records schedule DAA–0173–2020–0003, EEO Audits. In the absence of a more specific NARA-approved records schedule, such as the schedule for EEO audits, any information in this system that is not covered by the agency records control schedule N1–173–86–2 will also be treated as permanent.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to the information, *e.g.,* electronic records, files, and data, in the Online Public Inspection File, which is housed in the FCC computer network databases, is posted on the internet to be publicly accessible. Only the entities that upload information into the files can alter their information. 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 electronic files is restricted to authorized employees and contractors; and to 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 electronic 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), the Office of Management and Budget (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 request access to and/or amendment of records about themselves 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 access must also comply with the FCC's Privacy Act regulations regarding verification of identity to gain access to records as required under 47 CFR part 0, subpart E.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

77 FR 32111 (May 31, 2012).

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2024–20848 Filed 9–12–24; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[OMB 3060–1044; FR ID 244093]

Information Collection Being Reviewed by the Federal Communications Commission Under Delegated Authority

AGENCY: Federal Communications Commission.

ACTION: Notice and request for comments.

SUMMARY: As part of its continuing effort to reduce paperwork burdens, and as required by the Paperwork Reduction Act (PRA) of 1995, the Federal Communications Commission (FCC or