



FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 332367]

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-2, Business Contacts and Certifications, 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 Commission uses this system to collect and maintain points of contact and to ensure compliance with FCC rules through certifications of information provided to the Commission. This modification adds two routine uses.

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 will become effective on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless written comments are received that require a contrary determination.

ADDRESSES: Send comments to Shana Yates, at privacy@fcc.gov, or at Federal Communications Commission (FCC), 45 L Street NE, Washington, DC 20554.

FOR FURTHER INFORMATION CONTACT: Shana Yates, (202) 418-0683, or privacy@fcc.gov.

SUPPLEMENTARY INFORMATION: This notice serves to update and modify FCC-2 as a result of various necessary changes and updates. The substantive changes and modifications to the previously published version of the FCC-2 system of records include:

1. Adding two new routine uses (listed by the routine use number provided in this notice):
(13) Department of Treasury (as required by Executive Order 14249, Protecting America's Bank Account Against Fraud, Waste, and Abuse); and (14) Prevention of Fraud, Waste, and Abuse Disclosure;
2. Updating and/or revising language in the following routine uses (listed by the routine use number provided in this notice): (3) Federal Agencies; (4) State, Local, U.S. Territorial, and Tribal Government Entities; and (7) Law Enforcement and Investigation.

SYSTEM NAME AND NUMBER: FCC-2, Business Contacts and Certifications

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Federal Communications Commission (FCC), 45 L Street NE, Washington, DC 20554; Universal Service Administrative Company, 700 12th Street NW, Suite 900, Washington, DC 20005; or FISMA compliant contractor.

SYSTEM MANAGER(S): Federal Communications Commission (FCC), Office of the Managing Director, 45 L Street NE, Washington, DC 20554, (888) 225-5322; Universal Service Administrative Company (USAC), 700 12th Street NW, Suite 900, Washington, DC 20005; or FISMA-compliant contractors.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 47 U.S.C. 151, 152, 154 (i)-(j) & (o), 155, 251(e)(3), 254, 257, 301, 303, 332, 402, 1302; and 5 U.S.C. 602(c) and 609(a)(3).

PURPOSES OF THE SYSTEM: The FCC and organizations administering programs on behalf of the FCC use this system to collect and maintain points of contact and certifications from: (1) entities regulated by the FCC and in related industries, as well as contractors, vendors, and those performing collateral duties for the FCC; (2) other Federal, state, local, U.S. territorial, and Tribal government entities that administer, support, participate in, or receive information related to, FCC programs and activities; and (3) public interest organizations, nonprofit

organizations, international organizations, and other non-business entities that participate in FCC proceedings or are included in FCC programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals, including points of contact for and those who certify on behalf of, businesses, public interest organizations, nonprofit organizations, government organizations, international organizations, and other non-business entities that participate in FCC proceedings or are included in FCC programs; points of contact for Federal, state, local, U.S. territorial, or Tribal governmental entities.

CATEGORIES OF RECORDS IN THE SYSTEM: Contact information, such as name, username, signature, phone numbers, emails, and addresses, as well as work and educational history.

RECORD SOURCE CATEGORIES: Information in this system is provided by individuals, including points of contact for and those who certify on behalf of: FCC contractors; vendors; those providing collateral duties to the FCC; regulated entities and entities in related industries; Federal, state, local, U.S. territorial, and Tribal government entities; public interest organizations, nonprofit organizations, government organizations, international organizations, and other non-business entities that participate in FCC proceedings.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: 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.

1. Public Access—Contact information and certifications made by individuals contained in this system may be made available for public inspection to comply with FCC regulations that require public disclosure of this information, or in Commission releases, including

notices of proposed rulemaking, public notices, orders, and other actions released by the Commission.

2. Authorized Third Parties—Contact information and certifications made by individuals contained in this system may be shared with authorized third parties, including individuals and businesses in regulated and related industries, FCC vendors, and their contractors, to administer, support, participate in, or receive information related to, FCC programs and activities; or to ensure compliance with the confidentiality and other rules regarding information sharing in the FCC’s programs and activities.
3. Federal Agencies—Contact information and certifications made by individuals contained in this system may be shared with other Federal agencies in order to administer, support, participate in, or receive information related to: FCC programs and activities; and programs and activities the FCC supports.
4. State, Local, U.S. Territorial, and Tribal Government Entities—Contact information and certifications made by individuals contained in this system may be shared with authorized state, local, U.S. territorial and Tribal government entities to administer, support, participate in, or receive information related to: FCC programs and activities; and programs and activities the FCC supports.
5. 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 DOJ is for a purpose that is compatible with the purpose for which the FCC collected the records.

6. Adjudication—Records may be disclosed in a proceeding before a court or adjudicative body, 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; 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.
7. 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.
8. 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.
9. Government-wide Program Management and Oversight—Records may be disclosed 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.

10. 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 PII maintained in 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; 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.
11. 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.
12. 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.
13. Department of Treasury—Records may be disclosed to the U.S. Department of Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the United States, the District of Columbia,

a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.

14. Prevention of Fraud, Waste, and Abuse Disclosure—Records may be disclosed to Federal agencies, non-Federal entities, their employees, and agents (including contractors, their agents or employees; employees or contractors of the agents or designated agents); or contractors, their employees or agents with whom the FCC has a contract, service agreement, cooperative agreement, or computer matching agreements for the purpose of:
- (1) detection, prevention, and recovery of improper payments;
 - (2) detection and prevention of fraud, waste, and abuse in Federal programs administered by a Federal agency or non-Federal entity;
 - (3) detection of fraud, waste, and abuse by individuals in their operations and programs, but only to the extent that the information shared is necessary and relevant to verify pre-award and prepayment requirements prior to the release of Federal funds, prevent and recover improper payments for services rendered under programs of the FCC or of those Federal agencies and non-Federal entities to which the FCC provides information under this routine use.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: This is an electronic system of records that resides on the FCC’s network, USAC’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 maintained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule 6.5, Item 020 (DAA-GRS-2017-0002-0002).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The electronic records, files, and data are stored within FCC, USAC, or a vendor accreditation boundaries and

maintained in a database housed in the FCC's, USAC's, or a 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, USAC, 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 IT 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: 88 FR 77580 (Nov. 13, 2023).

Federal Communications Commission.

Marlene Dortch,
Secretary.

[FR Doc. 2026-03738 Filed: 2/24/2026 8:45 am; Publication Date: 2/25/2026]