6712-01

This document is scheduled to be published in the Federal Register on 12/22/2023 and available online at **https://federalregister.gov/d/2023-27896**, and on **https://govinfo.gov**

**FEDERAL COMMUNICATIONS COMMISSION**

**[FR ID: 191216]**

**Privacy Act of 1974; System of Records**

**AGENCY:** Federal Communications Commission.

**ACTION:** Notice of a new system of records.

**SUMMARY:** The Federal Communications Commission (FCC, Commission, or Agency) proposes to add a new system of records, FCC-3, FCC Identity, Credentialing, and Access Management (ICAM), 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.

**DATES:** This new 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 Brendan McTaggart, at privacy@fcc.gov, or at Federal Communications Commission (FCC), 45 L Street, NE, Washington, D.C. 20554 at (202) 418-1738.

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

**SUPPLEMENTARY INFORMATION:** The FCC is establishing the Identity, Credentialing, and Access Management (ICAM) system of records. This system of records covers the FCC's, its administrators', its contractors', and its vendors' (collectively FCC's) systems that collect and maintain records about internal and external users of the FCC's, its administrators', its

contractors', and its vendors' (collectively FCC's) network and information systems.

**SYSTEM NAME AND NUMBER:** FCC-3, FCC Identity, Credentialing, and Access Management (ICAM).

**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; and FISMA compliant contractors and vendors.

**SYSTEM MANAGER(S):** Federal Communications Commission (FCC); Universal Service Administrative Company (USAC); and FISMA compliant contractors and vendors.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 47 U.S.C. 151 *et seq*.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 *et seq*.

**PURPOSES OF THE SYSTEM:** The FCC uses the systems that comprise this system of records to maintain an Active Directory of FCC staff and contractors who are authorized to access the FCC network; to monitor, log, and audit usage of the FCC's network and information systems; to support server and desktop hardware and software; to ensure the availability and reliability of the FCC's network and information systems; to help document and/or control access to the FCC's network and information systems; to identify the need for and to conduct training programs, which can include the topics of information security; to monitor the security of the FCC's network and information systems; to add and delete users; to investigate and make referrals for disciplinary or other action if improper or unauthorized use is suspected or detected; and to collect and maintain information necessary for FCC staff to perform key activities, including analyzing effectiveness and efficiency of FCC programs and informing rule-making and policy-making activity.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Commission employees, and employees of FCC contractors and administrators with access to the FCC network; individuals and representatives of entities that register to do business with the

Commission; and members of the public who access the FCC's public-facing information systems.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Contact information, such as name, username, password, phone numbers, email address, street address; network information, such as IP/MAC address, geolocation, web browser, timestamps, and activity logs.

**RECORD SOURCE CATEGORIES:** Information in this system is provided by Commission employees and employees of FCC contractors and administrators with access to the FCC network; individuals and representatives of entities that register to do business with the Commission; members of the public who access the FCC's public-facing information systems; vendors that provide DNS, CDN, cloud hosting, firewall, and related services; other FCC information systems that collect network information from users, including the FCC's Financial Operations Information Systems.

**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. 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 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.
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 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.

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, or order.
4. 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 written request of that individual.
5. Government-wide Program Management and Oversight—To provide 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.
6. 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 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.

7. 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.
8. 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 service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records to perform their activity.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS**: This an electronic system of records that resides on the FCC's network, USAC's network, and FCC contractors' and vendors' networks.

**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 GRS 3.2, Information Systems Security Records (DAA-GRS-2013-0006).

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** The electronic records, files, and data are stored within FCC, USAC, other program administrator, contractor, and vendor accreditation boundaries and maintained in databases housed on their network

databases. Access to the electronic files is restricted to authorized employees, staff 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 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 Procedure below.

**CONTESTING RECORD PROCEDURES:** Individuals wishing to request access to and/or amendment of records about themselves should follow the Notification Procedure 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:** None.

Federal Communications Commission.

**Marlene Dortch**,

*Secretary*.

[FR Doc. 2023-27896 Filed: 12/19/2023 4:15 pm; Publication Date: 12/22/2023]