FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 194271]

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/OMD-24, Physical Access Control System (PACS), 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 maintain records on those individuals to whom the FCC has issued credentials. This modification makes various necessary changes and updates, including formatting changes required by the Office of Management and Budget (OMB) Circular A-108 since its previous publication, the addition of three new routine uses, and the revision of five existing 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 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, D.C. 20554, or to privacy@fcc.gov.

FOR FURTHER INFORMATION CONTACT: Brendan McTaggart, (202) 418-1738, or privacy@fcc.gov (and to obtain a copy of the Narrative Statement and the Supplementary Document, which includes details of the modifications to this system of records).

SUPPLEMENTARY INFORMATION: This notice serves to update and modify FCC/OMD-24, as a result of various necessary changes and updates. The substantive changes and modifications to the previously published version of the FCC/OMD-24 system of records include:

1. Updating the language in the Security Classification to follow OMB guidance.
2. Updating the language in the Purposes section to be consistent with the language and phrasing currently used generally in the FCC's SORNs and to reflect how the system is currently used (*e.g.*, the system no longer covers frequent visitors, credit union employees, restaurant employees, or parking permit data).
3. Modifying the language in the Categories of Individuals and Categories of Records for clarity; and for consistency with the current uses of the system (which now excludes frequent visitors, credit union employees, restaurant employees, and parking permit data) and with the language and phrasing currently used in the FCC's SORNs.
4. Updating and/or revising language in five routine uses (listed by current routine use number): (1) Litigation; (2) Adjudication; (3) Law Enforcement and Investigation; (4) Congressional Inquiries; and (5) Government-wide Program Management and Oversight.
5. Adding three new routine uses (listed by current routine use number): (11) Breach Notification, the addition of which is as required by OMB Memorandum No. M-17-12; (12) Assistance to Federal Agencies and Entities Related to Breaches, the addition of which is required by OMB Memorandum No. M-17-12; and (13) Non-Federal Personnel.
6. Updating the SORN to include the relevant National Archives and Records Administration (NARA) records schedules.

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 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-24, Physical Access Control System (PACS).

SECURITY CLASSIFICATION: No information in the system is classified.

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

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; Federal Information Security Management Act (44 U.S.C. 3541 *et. seq.*); Electronic Government Act (Pub. L. No. 107-347, sec. 203); Homeland Security Presidential Directive (HSPD) 12, ‘‘Policy for a Common Identification Standard for Federal Employees and Contractors,” (2004); Federal Property and Administrative Act of 1949, as amended (Pub. L. No. 81-152); and Department of Justice Report, ‘‘Vulnerability Assessment of Federal Facilities,” (1995).

PURPOSE(S) OF THE SYSTEM: OMD uses the information in this information system for purposes that include, but are not limited to the following:

1. To ensure the safety and security of FCC facilities, systems, and information,

2. To ensure the safety and security of FCC employees, contractors, interns, and guests;

3. To verify that all people entering the FCC facilities, using FCC and Federal information resources (or accessing classified information), are authorized to do so;

4. To track and control FCC badges (PIV cards) issued to individuals entering and exiting these facilities, using FCC systems, or accessing classified information; and

5. To provide a method by which the FCC may ascertain the times each person was in these facilities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The categories of individuals whose records are maintained in this system include, but are not limited to, individuals who require regular, on-going access to FCC facilities and information technology systems, *e.g.*:

1. Current FCC employees and contractors;

2. Temporary hires and day contractors;

3. Applicants for Federal employment or contract work;

4. FCC students, interns, volunteers, affiliates, and individuals formerly in these positions, *e.g.*, retired FCC employees; and

5. Non-FCC employees who are authorized to perform or use services in FCC facilities on an on-going basis, *e.g.*, building maintenance and cleaning employees.

This system also applies to occasional visitors or short-term guests to whom the FCC will issue temporary identification and credentials, who may include:

1. All visitors to FCC, *e.g.*, non-FCC federal employees and contractors, students, interns, volunteers, and affiliates; and

2. Individuals authorized to perform or use services provided in FCC facilities on an infrequent basis, *e.g.*, service and maintenance workers performing cleaning, maintenance, and repair duties in the Commission's buildings and facilities.

CATEGORIES OF RECORDS IN THE SYSTEM: The records in this system include, but are not limited to, records on those individuals to whom the FCC has issued credentials, including the following:

1. FCC employee/temporary hire database, which may include contact information and other personally identifiable information (PII) such as the following: full name (first, middle, and last names), Social Security Number (SSN), birth date, signature, image (photograph), fingerprints, hair color, eye color, height, weight, FCC telephone number, FCC Bureau/Office, FCC office/room number, personal identification number (PIN), background investigation form data and results, date the personal identity verification (PIV) card was issued and expiration dates, PIV registrar approval signature, PIV card serial number, emergency responder designation, copies of documents verifying identification or information derived from such documents (*e.g.*, document title, document issuing authority, document number, document expiration date, other document information), national security level clearance and expiration date, computer system user name, user access and permission rights, authentication certificates, and digital signature information.

2. Contractor database, which may include contact information and other PII such as the following: first, middle, and last name, SSN, birth date, signature, image (photograph), fingerprints, hair color, eye color, height, weight, contractor company name, Federal supervisor, telephone number, FCC point of contact, FCC Bureau/Office, FCC office/room number, FCC telephone number, and FCC contractor badge number, personal identification number (PIN), background investigation form data and results, date the PIV card was issued and expiration dates, PIV registrar approval signature, PIV card serial number, emergency responder designation, copies of documents verifying identification or information derived from such documents (*e.g.*, document title, document issuing authority, document number, document expiration date, other document information), national security level clearance and expiration date, computer system user name, user access and permission rights, authentication certificates, and digital signature information.

3. Day contractor database, which may include contact information and other PII such as the following: First and last name along with badge number, date of issuance and expiration date.

4. Visitor database, which may include contact information and other PII such as the following: first and last name, image (photograph), FCC point of contact and date of issuance.

RECORD SOURCE CATEGORIES: Sources of records include individual FCC employees to whom the information applies, contractors, or applicants for employment; sponsoring agencies; former sponsoring agencies; other federal agencies; contract employers; former employees; and visitors.

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, 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.

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, and

that the use of such records is for a purpose that is compatible with the purpose for which the agency collected the records.

3. Law Enforcement and Investigation—When the FCC becomes aware of an indication of a violation or potential violation of a civil or criminal statute, law, regulation, order, or other requirement, to disclose pertinent information to 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 requirement.

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 DOJ to obtain that Department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or to OMB to obtain that office's advice regarding obligations under the Privacy Act.

6. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the Agency—To a Federal, State, or local government 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 retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit.

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by Other Than the Agency—To a Federal, State, local, or tribal government, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a

request supported by the written consent of the individual for the complete 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.

8. 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.

9. 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.

10. Invalid PIV Card Notification—To notify another Federal agency, when, or to verify whether, a PIV card is no longer valid.

11. 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 compromise 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.

12. 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.

13. 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: The electronic system of records resides on the FCC's or a vendor's network.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The information in the electronic database can be retrieved by searching electronically using a variety of parameters including: (1) The name of the individual; (2) Social Security Number (SSN); (3) other ID number (*e.g.*, FCC employee, contractor, or frequent visitor badge number); or (4) PIV card serial number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The information in this system related to individuals with FCC access cards is maintained and disposed of in accordance with NARA General Records Schedule (GRS) 5.6 Security Management Records, DAA-GRS-2021-0001; and GRS 4.2, Information Access and Protection Records, DAA-GRS-2019-0001-0002.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The electronic database is located in FCC facilities that are secured by limited access card readers. The

computer servers are password-protected. Access by individuals working at guard stations is password-protected. Each person granted access to the system at guard stations must be individually authorized to use the system. FCC Information Technology backs up these files daily, which are stored in the Cloud at an alternate secure location. The security protocols and features 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 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 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: 71 FR 55787 (Sept. 25, 2006)

Federal Communications Commission.

Katura Jackson,

Federal Register Liaison Officer.

[FR Doc. 2023-28752 Filed: 12/28/2023 8:45 am; Publication Date: 12/29/2023]