



DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

Privacy Act of 1974; System of Records

AGENCY: Federal Energy Regulatory Commission (FERC), DOE.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, all agencies are required to publish in the **Federal Register** a notice of their systems of records. Notice is hereby given that the Federal Energy Regulatory Commission (FERC) is publishing a notice of modifications to an existing FERC system of records, FERC - 42 titled “*Commission Security Access and Control Records*.”

DATES: Please submit comments on this modified system of records on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**]. These new routine uses are effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**]. If no public comment is received during this period or unless otherwise published in the **Federal Register** by FERC, the modified system of records will become effective a minimum of 30 days after the date of publication in the **Federal Register**. If FERC receives public comments, FERC shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted in writing to Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426 or electronically to privacy@ferc.gov. Comments should indicate that they are submitted in response to “Commission Security Access and Control Records” (FERC – 42).

FOR FURTHER INFORMATION CONTACT: Mittal Desai, Chief Information Officer & Senior Agency Official for Privacy, Office of the Executive Director, Federal Energy Regulatory Commission, 888 First Street, NE Washington, DC 20426, (202) 502-6432.

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, and to comply with the Office of Management and Budget (OMB) Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017, this notice will incorporate two new routine uses that permit FERC to disclose information as necessary in response to an actual or suspected breach that pertains to a breach of its own records or to assist another agency in its efforts to respond to a breach that was previously published separately at 87 FR 35543 and added 11 routine uses that are consistent with OPM guidance. The following sections have been updated: dates; addresses; for further contact information; system name and number; system location; system manager; authority for maintenance of the system; purpose; categories of individuals covered by the system; categories of records in the system; routine uses of records maintained in the system, including categories of users and the purpose of such; policies and practices for storage of records; policies and practices for retrieval of records; policies and practices for retention and disposal of records; administrative, technical, and physical safeguards; record access procedures; contesting record procedures; notification procedures; and history.

SYSTEM NAME AND NUMBER: Commission Security Access and Control Records (FERC – 42)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Federal Energy Regulatory Commission, Office of the Executive Director, Chief Security Officer Directorate, Mission Integrity Division, 888 First Street, Washington, DC 20426.

SYSTEM MANAGER(S): Director, Federal Energy Regulatory Commission, Chief Security Officer Directorate, Mission Integrity Division, 888 First Street, NE, Washington, DC 20426.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 41 CFR 102-74.375

PURPOSE(S) OF THE SYSTEM: Records in this system of records are maintained for the following purposes: providing access control permission to FERC's facilities as well as visitors' security and management.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The following categories of individuals are covered by this system: current and former FERC employees, current and former FERC contractors, and members of the public visiting FERC facilities.

CATEGORIES OF RECORDS IN THE SYSTEM: Records maintained in this system include: full name; telephone number; badge access permission; signature; driver license and/or ID information including ID number, date of issuance, state of issuance, expiration date, and other identifying information contained therein; passport information including number, issuance date, expiration date, and other identifying information contained therein; digital copies of driver license, ID, and passport; and the date, time and entry point of building access.

RECORD SOURCE CATEGORIES: Records in the system are obtained from the individual to whom the records pertain.

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, information maintained in this system may be disclosed to authorized entities outside FERC for purposes determined to be relevant and necessary as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. To appropriate agencies, entities, and persons when (1) FERC suspects or has confirmed that there has been a breach of the system of records; (2) FERC 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 (3) 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.
2. To another Federal agency or Federal entity, when FERC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
3. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

4. To the Equal Employment Opportunity Commission (EEOC) when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law or regulation.
5. To the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.
6. To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding. In those cases where the Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a judge.
7. To the Department of Justice (DOJ) for its use in providing legal advice to FERC or in representing FERC in a proceeding before a court, adjudicative body, or other administrative body, where the use of such information by the DOJ is deemed by FERC to be relevant and necessary to the advice or proceeding, and such proceeding names as a party in interest: (a) FERC; (b) any employee of FERC in his or her official capacity; (c) any employee of FERC in his or her individual capacity where DOJ has agreed to represent the employee; or (d) the United States, where FERC determines that litigation is likely to affect FERC or any of its components.
8. To non-Federal Personnel, such as contractors, agents, or other authorized individuals performing work on a contract, service, cooperative agreement, job, or

other activity on behalf of FERC or Federal Government and who have a need to access the information in the performance of their duties or activities.

9. To the National Archives and Records Administration in records management inspections and its role as Archivist.
10. To the Merit Systems Protection Board or the Board's Office of the Special Counsel, when relevant information is requested in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, and investigations of alleged or possible prohibited personnel practices.
11. To appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the information may be relevant to a potential violation of civil or criminal law, rule, regulation, order.
12. To appropriate agencies, entities, and person(s) that are a party to a dispute, when FERC determines that information from this system of records is reasonably necessary for the recipient to assist with the resolution of the dispute; the name, address, telephone number, email address, and affiliation; of the agency, entity, and/or person(s) seeking and/or participating in dispute resolution services, where appropriate.
13. To Department of Energy (DOE) to manage visitors access to FERC facilities.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic records are stored in FERC IT system and access to electronic records is controlled by User ID and password combination and/or the organizations Single Sign-On and Multi-Factor Authentication solution. Paper records are stored in a lockable file room. Access to

electronic and paper records is restricted to those individuals whose official duties require access.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by the individual's name, date, employee badge number, card reader, or other identifying information provided by the individual.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retained and disposed of in accordance with the schedule approved under the National Archives and Records Administration's General Records Schedule 5.6: Security Management Records:

Item 110: Visitor Processing Records, areas requiring highest level security awareness, Disposition Authority: DAA-GRS-2017-0006-0014. Temporary. Destroy when 5 (five) years old, but longer retention is authorized if required for business use.

Item 111: Visitor Processing Records, all other facility security areas, Disposition Authority: DAA-GRS-2017-006-0015. Temporary. Destroy when two (2) years old but longer retention is authorized if required for business use.

Item 120: Personal Identification Credentials and Cards, Application and Activation Records, Disposition Authority: DAA-GRS-2021-0001-0005. Temporary. Destroy six (6) years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: *See* Policies and Practices for Storage of Records.

NOTIFICATION PROCEDURES: Generalized notice is provided by the publication of this notice. For specific notice, see Records Access Procedure, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 65 FR 21756

Issued: September 15, 2023.

Kimberly D. Bose,
Secretary.

[FR Doc. 2023-20457 Filed: 9/20/2023 8:45 am; Publication Date: 9/21/2023]