[6450-01-P]

DEPARTMENT OF ENERGY

Privacy Act of 1974; System of Records

AGENCY: U.S. Department of Energy.

ACTION: Notice of a modified system of records.

SUMMARY: As required by the Privacy Act of 1974 and the Office of Management and Budget (OMB) Circulars A-108 and A-130, the Department of Energy (DOE or the Department) is publishing notice of a modification to an existing Privacy Act System of Records. DOE proposes to amend System of Records DOE-27 Foreign Travel Management System (FTMS). This System of Records Notice (SORN) is being modified to align with new formatting requirements, published by OMB, and to ensure appropriate Privacy Act coverage of business processes and Privacy Act information.

DATES: This modified SORN will become applicable following the end of the public comment period on [**INSERT THE DATE 30 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER***] unless comments are received that result in a contrary determination.

ADDRESSES: Written comments should be sent to Ken Hunt, Chief Privacy Officer, U.S. Department of Energy, 1000 Independence Avenue SW, Rm 8H-085, Washington, DC 20585, by facsimile at (202) 586-8151, or by email at *privacy@hq.doe.gov*.

FOR FURTHER INFORMATION CONTACT: Ken Hunt, Chief Privacy Officer, U.S. Department of Energy, 1000 Independence Avenue SW, Rm 8H-085, Washington, DC 20585, by facsimile at (202) 586-8151, by email at *privacy@hq.doe.gov*, or by telephone at (240) 686-9485.

SUPPLEMENTARY INFORMATION: On January 9, 2009, DOE published a Compilation of its Privacy Act Systems of Records, which included System of Records DOE-27 Foreign Travel Management System (FTMS). This notice proposes amendments to the system locations section

of that system of records by removing the following system location where DOE-27 is no longer applicable: Environmental Management Consolidated Business Center. In the "Routine Uses" section, this modified notice deletes a previous routine use concerning efforts responding to a suspected or confirmed loss of confidentiality of information as it appears in DOE's compilation of its Privacy Act systems of records (January 9, 2009) and replaces it with one to assist DOE with responding to a suspected or confirmed breach of its records of Personally Identifiable Information (PII), modeled with language from OMB's Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (January 3, 2017). Further, this notice adds one new routine use to ensure that DOE may assist another agency or entity in responding to the other agency's or entity's confirmed or suspected breach of PII, as appropriate, as aligned with OMB's Memorandum M-17-12. The "System Manager" has been changed from "Office of Security Operations" to the "Office of the Chief Financial Officer." An administrative change required by the FOIA Improvement Act of 2016 extends the length of time a requestor is permitted to file an appeal under the Privacy Act from 30 to 90 days. Both the "System Locations" and "Administrative, Technical and Physical Safeguards" sections have been modified to reflect the Department's usage of cloud-based services for records storage. Language throughout the SORN has been updated to align with applicable Federal privacy laws, policies, procedures, and best practices.

SYSTEM NAME AND NUMBER: DOE-27 Foreign Travel Management System (FTMS).

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Systems leveraging this SORN may exist in multiple locations. All systems storing records in a cloud-based server are required to use government-approved cloud services and follow National Institute of Standards and Technology (NIST) security and privacy standards for access and data retention. Records maintained in a government-approved cloud server are accessed through secure data centers in the continental United States.

U.S. Department of Energy, Director, Office of the Chief Financial Officer, 1000 Independence Avenue SW, Washington, DC 20585.

U.S. Department of Energy, Germantown, 19901 Germantown Road, Germantown, MD 20874-1290.

U.S. Department of Energy, Bonneville Power Administration, P.O. Box 3621, Portland, OR 97208.

U.S. Department of Energy, Idaho Operations Office, 1955 Fremont Avenue, Idaho Falls, ID 83415.

SYSTEM MANAGER(S): U.S. Department of Energy, Director, Office of the Chief Financial Officer, 1000 Independence Avenue SW, Washington, DC 20585.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 42 U.S.C. 7101 *et seq*.; 50 U.S.C. 2401 *et seq*.; 5 U.S.C. Chapter 3, Section 301; 5 U.S.C. Chapter 57; Federal Travel Regulation; Department of Energy Order 550.1, current version.

PURPOSE(S) OF THE SYSTEM: Records in this system are maintained and used by DOE to document all official foreign travel by DOE employees and contractor employees, and any approvals.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DOE employees, including National Nuclear Security Administration (NNSA) and contractor employees, authorized to travel to foreign countries on official government business.

CATEGORIES OF RECORDS IN THE SYSTEM: Traveler's name and the last four digits of their Social Security number, background data relating to proposed foreign travel; authorization number, travel itinerary; official or personal passport information, visa information, and summary report following completion of travel.

RECORD SOURCE CATEGORIES: Individual travelers, supervisors, and travel offices.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

1. A record from this system may be disclosed as a routine use to the General Services Administration for verification of transportation services.
2. A record from this system may be disclosed as a routine use to DOE contractors in performance of their contracts, and their officers and employees who have a need for the record in the performance of their duties. Those provided information under this routine use are subject to the same limitations applicable to Department officers and employees under the Privacy Act.
3. A record from this system may be disclosed as a routine use to the Department of State or border control or immigration services for purpose of obtaining foreign country clearance for the traveler.
4. A record from this system may be disclosed as a routine use to the appropriate local, Tribal, State, or Federal agency when records, alone or in conjunction with other information, indicate a violation or potential violation of law whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program pursuant thereto.
5. A record from this system may be disclosed as a routine use to a member of Congress submitting a request involving a constituent when the constituent has requested assistance from the member concerning the subject matter of the record. The member of Congress must provide a copy of the constituent's signed request for assistance.
6. A record from this system may be disclosed as a routine use to appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOE (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 Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

7. A record from this system may be disclosed as a routine use to another Federal agency or Federal entity, when the Department 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored as paper records or electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name, Social Security number, or travel authorization number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Retention and disposition of these records is in accordance with the National Archives and Records Administration-approved records disposition schedule with a retention of 6 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Electronic records may be secured and maintained on a cloud-based software server and operating system that resides in Federal Risk and Authorization Management Program (FedRAMP) and Federal Information Security Modernization Act (FISMA) hosting environment. Data located in the cloud-based server is firewalled and encrypted at rest and in transit. The security mechanisms for handling data at rest and in transit are in accordance with DOE encryption standards. Records are protected from unauthorized access through the following appropriate safeguards:

- **Administrative**: Access to all records is limited to lawful government purposes only, with access to electronic records based on role and either two-factor authentication or password protection. The system requires passwords to be complex and to be changed

frequently. Users accessing system records undergo frequent training in Privacy Act and information security requirements. Security and privacy controls are reviewed on an ongoing basis.

- **Technical**: Computerized records systems are safeguarded on Departmental networks configured for role-based access based on job responsibilities and organizational affiliation. Privacy and security controls are in place for this system and are updated in accordance with applicable requirements as determined by NIST and DOE directives and guidance.
- **Physical**: Computer servers on which electronic records are stored are located in secured Department facilities, which are protected by security guards, identification badges, and cameras. Paper copies of all records are locked in file cabinets, file rooms, or offices and are under the control of authorized personnel. Access to these facilities is granted only to authorized personnel and each person granted access to the system must be an individual authorized to use or administer the system.

RECORD ACCESS PROCEDURES: The Department follows the procedures outlined in title 10 CFR 1008.4. Valid identification of the individual making the request is required before information will be processed, given, access granted, or a correction considered, to ensure that information is given, corrected, or records disclosed or corrected only at the request of the proper person.

CONTESTING RECORD PROCEDURES: Any individual may submit a request to the System Manager and request a copy of any records relating to them. In accordance with 10 CFR 1008.11, any individual may appeal the denial of a request made by him or her for information about or for access to or correction or amendment of records. An appeal shall be filed within 90 calendar days after receipt of the denial. When an appeal is filed by mail, the postmark is conclusive as to timeliness. The appeal shall be in writing and must be signed by the individual. The words “PRIVACY ACT APPEAL” should appear in capital letters on the envelope and the

letter. Appeals relating to DOE records shall be directed to the Director, Office of Hearings and Appeals (OHA), 1000 Independence Avenue SW, Washington, DC 20585.

NOTIFICATION PROCEDURES: In accordance with the DOE regulation implementing the Privacy Act, 10 CFR part 1008, a request by an individual to determine if a system of records contains information about themselves should be directed to the U.S. Department of Energy, Headquarters, Privacy Act Officer. The request should include the requester's complete name and the time period for which records are sought.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: This SORN was last published in the *Federal Register*, 74 FR 1028-1029, on January 9, 2009.

Signing Authority

This document of the Department of Energy was signed on November 18, 2024, by Ann Dunkin, Senior Agency Official for Privacy, pursuant to delegated authority from the Secretary of Energy. That document with the original signature and date is maintained by DOE. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned DOE Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Energy. This administrative process in no way alters the legal effect of this document upon publication in the *Federal Register*.

Signed in Washington, DC, on November 18, 2024.

Treena V. Garrett,
Federal Register Liaison Officer,
U.S. Department of Energy.

[FR Doc. 2024-27345 Filed: 11/21/2024 8:45 am; Publication Date: 11/22/2024]