



## DEPARTMENT OF ENERGY

### Privacy Act of 1974; System of Records

**AGENCY:** United States Department of Energy.

**ACTION:** Notice of a new 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 newly established Privacy Act System of Records. DOE proposes to reestablish system of records DOE-21 “Asset Readiness Management System (ARMS).” The Office of Nuclear Incident Response uses ARMS to quantify, monitor, and track readiness of and deploy personnel and equipment as part of a coordinated Federal government response to an emergency involving nuclear or radiological materials.

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

**ADDRESSES:** Written comments should be sent to Nicole Sanchez, Chief Privacy Officer, U.S. Department of Energy, 1000 Independence Avenue, S.W., Rm 8H-085, Washington, D.C. 20585, by facsimile at 202-586-8151, or by email at [privacy@hq.doe.gov](mailto:privacy@hq.doe.gov).

**FOR FURTHER INFORMATION CONTACT:** Nicole Sanchez, Chief Privacy Officer, U.S. Department of Energy, 1000 Independence Avenue, S.W., Rm 8H-085, Washington, D.C. 20585, 202-586-0166, or by email at [privacy@hq.doe.gov](mailto:privacy@hq.doe.gov).

**SUPPLEMENTARY INFORMATION:** On January 9, 2009, DOE published a Compilation of its Privacy Act systems of records, which included system of records DOE-21 “Asset Readiness Management System (ARMS).” DOE rescinded the SORN on September 11, 2024. At this time,

DOE proposes reestablishing this SORN as this SORN is applicable to the U.S. National Nuclear Security Administration (NNSA).

**SYSTEM NAME AND NUMBER:** DOE-21 Asset Readiness Management System (ARMS).

**SECURITY CLASSIFICATION:** Classified and Unclassified.

**SYSTEM LOCATION(S):**

Headquarters: U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585.

Headquarters: U.S. Department of Energy, National Nuclear Security Administration HQ, 1000 Independence Ave SW, Washington, DC 20585

**SYSTEM MANAGER(S):** *Headquarters:* U.S. Department of Energy, Director, Office of Nuclear Incident Response, NA-84, National Nuclear Security Administration, 1000 Independence Avenue, S.W., Washington, D.C. 20585.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 42 U.S.C. 7101 *et seq.*; 50 U.S.C. 2401 *et seq.*; Homeland Security Presidential Directive 5 (HSPD-5), “Management of Domestic Incidents,” The Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (Nov. 25, 2002), Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 106-390, 114 Stat. 1552—1575 (October 30, 2000).

**PURPOSE(S) OF THE SYSTEM:** For those records described in *Categories of Records in the System*, such records are maintained and used by the Office of Nuclear Incident Response to quantify, monitor, and track readiness of and deploy personnel and equipment as part of a coordinated Federal government response to an emergency involving nuclear or radiological materials.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Federal employees, including DOE and National Nuclear Security Administration (NNSA) employees, military personnel, contractors, and subcontractors.

**CATEGORIES OF RECORDS IN THE SYSTEM:** The following information may be maintained in the system: Names, home addresses, home and work telephone numbers, e-mail addresses, Social Security numbers (SSNs), employee numbers, dates of hire, DOE badge number, security clearance number, dates of birth, tourist passport numbers, official passport numbers, education level, blood types, immunization records, training records, and other medical information.

**RECORD SOURCE CATEGORIES:** Personally identifiable information (PII) is sourced directly from the individual to whom it pertains as well as from training records.

**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 officials of the Federal Bureau of Investigation, Department of Defense, Nuclear Regulatory Commission, Environmental Protection Administration, National Aeronautics Space Administration, Department Homeland Security, and Department of State who have been approved as agents by NNSA Office of Nuclear Incident Response for purposes of managing and assessing state of readiness, to obtain visas for official foreign travel, and to provide information to gain access to incident areas controlled by one or more U.S. government agencies under the National Response Plan.
2. A record from the system may be disclosed as a routine use to the appropriate local, state or Federal agency when records alone or in conjunction with other information indicates 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.
3. A record from this system may be disclosed as a routine use for the purpose of an investigation, settlement of claims, or the preparation and conduct of litigation to (1) persons representing the Department in the investigation, settlement or litigation, and to individuals assisting in such representation; (2) others involved in the investigation,

settlement, and litigation, and their representatives and individuals assisting those representatives; and (3) witness, potential witness, or their representatives and assistants, and any other person who possesses information pertaining to the matter when it is necessary to obtain information or testimony relevant and necessary to the matter.

4. A record from this system may be disclosed as a routine use in court or administrative proceedings to the tribunals, counsel, other parties, witnesses, and the public (in publicly available pleadings, filings or discussion in open court) when such disclosure: (1) is relevant to, and necessary for, the proceeding; (2) is compatible with the purpose for which the Department collected the records; and (3) the proceedings involve:
  - a. The Department, its predecessor agencies, current or former contractor of the Department, or other United States Government agencies and their components, or
  - b. A current or former employee of the Department and its predecessor agencies, current or former contractors of the Department, or other United States Government agencies and their components, who is acting in an official capacity or in any individual capacity where the Department or other United States Government agency has agreed to represent the employee.
5. A record from the system may be disclosed as a routine use to DOE contractors in the 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.
6. A record from the system may be disclosed as a routine use to a Federal, state, or local agency to obtain information relevant to a Departmental decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit. The Department must deem such

disclosure to be compatible with the purpose for which the Department collected the information.

7. A record from this system may be disclosed to a member of Congress submitting a request involving a constituent when the constituent has requested assistance from the member concerning the subject of the record; the member must provide a copy of the constituent's request for assistance.
8. 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 economic or property interests, identity theft or fraud 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.
9. 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 will be stored as electronic records in a computer database.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records are retrieved by name, employee number, e-mail address, work telephone number, or home telephone number.

## **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Records retention and disposal authorities are contained in the General Records Schedule and DOE record schedules that have been approved by the National Archives and Records Administration (NARA). Some records in this system are currently unscheduled, which requires the records to be retained as permanent until NARA approves a DOE Records Disposition Schedule, while other records will be destroyed between 3-250 years.

## **ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

- **Administrative:** Access to all records is limited to need-to-know personnel 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 the National Institute for Standards and Technology (NIST) including NIST Special Publication (SP) 800-53.
- **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 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 individual authorized to use the system.

**RECORD ACCESS PROCEDURES:** The Department follows the procedures outlined in 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 processed 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. 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 Ave., S.W., Washington, D.C 20585.

**NOTIFICATION PROCEDURES:** In accordance with the DOE regulation implementing the Privacy Act, 10 CFR 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 originally published in the *Federal Register*, 74 FR 1022, pages 1022-1023, on January 9, 2009. This SORN was rescinded on September 11, 2024, in the *Federal Register*, 89 FR 155, pages 65618-65619.

### **Signing Authority**

This document of the Department of Energy was signed on March 19, 2026, by Dawn Zimmer, 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 March 20, 2026.

**Jennifer Hartzell,**  
*Alternate Federal Register Liaison Officer,*  
*U.S. Department of Energy.*

[FR Doc. 2026-05690 Filed: 3/23/2026 8:45 am; Publication Date: 3/24/2026]