[6450-01-P]

DEPARTMENT OF ENERGY

Privacy Act of 1974; System of Records

AGENCY: U.S. 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 new Privacy Act System of Records. DOE proposes to establish System of Records DOE-78 Data Analytics Program Records. The Office of the Inspector General (OIG) proposes to establish this System of Records to undertake such analytics inquiries necessary to support OIG efforts to effectuate audits, inspections, evaluations, and investigations relating to Departmental programs and operations and to accommodate the requirements of the Digital Accountability and Transparency Act of 2014 (DATA Act).

DATES: This new SORN will become applicable 30 days after the publication of the Final Rule associated with the "Exemptions Promulgated for the System" detailed below.

ADDRESSES: Written comments should be sent to the DOE Desk Officer, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 10102, 735 17th Street NW, Washington, DC 20503 and to Ken Hunt, Chief Privacy Officer, U.S. Department of Energy, 1000 Independence Avenue SW, Rm 8H-085, Washington, DC 20585 or 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 or by facsimile at 202-586-8151 or by email at *privacy@hq.doe.gov*.

SUPPLEMENTARY INFORMATION: Under the Inspector General Act of 1978, Inspectors General, including the DOE Inspector General, are responsible for determining, conducting, supervising, and coordinating audits, inspections, evaluations, and investigations relating to

programs and operations of the Federal agency for which their office is established to recognize and mitigate fraud, waste, and abuse. OIG is already utilizing existing systems of records which will remain in effect. This System of Records supports OIG's performance of its statutory responsibility through a data analytics program to conduct such activities necessary to: (1) assess risk to Departmental programs and operations; (2) determine, conduct, supervise, and coordinate audits, inspections, evaluations, and investigations relating to Departmental programs and operations; (3) promote economic efficiency and effective administration of programs; (4) prevent and detect fraud, waste and abuse in Departmental programs and operations; and (5) to accommodate the requirements of the DATA Act, Public Law 113–101, 31 31 U.S.C. 6101 note, 128 Stat. 1146.

Such activities may include, but are not limited to, analyzing (1) financial, operational, and performance information for fraud, inconsistencies, or unauthorized expenses; (2) contractor, subcontractor, grantee, subgrantee, and other awardees' corporate relationships, operations, and legal assertions as well as compliance with laws, rules, regulations, and best practices; (3) individual compliance with laws, rules, regulations, legal guidance, and Departmental orders; (4) program and operational adherence to laws, rules, regulations, and best practices; and (5) Departmental risks.

The data analytics program will provide OIG with timely insights from the data: (1) developed and maintained by OIG, General Accountability Office, and other DOE-related oversight organizations; (2) stored in DOE databases that OIG has legal authorization to access and maintain; (3) held by DOE contractors, subcontractors, grantees, and subgrantees that OIG has legal and Departmental authority to obtain and maintain; (4) collected by the Offices of Inspectors General of other Federal Departments and Agencies; and (5) publicly available data and data purchased from commercial vendors related to Departmental programs and operations. Commercial data supplements other data and is not a primary data source.

Pursuant to 5 U.S.C. 552a(b)(12), records maintained in this System of Records may be disclosed to a consumer reporting agency without the prior written consent of the individual to whom the record pertains. Such disclosure will only be made in accordance with 31 U.S.C. 3711(e). In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new System of Records.

Definitions: Any reference to the "Department" or "DOE" includes Departmental elements, the National Nuclear Security Administration, Energy Information Administration, Power Marketing Administrations, and Federal Energy Regulatory Commission. Any reference to "contractor(s)" in this System of Records Notice (SORN) includes management and operating (M&O) contractors, prime contractors, and any business entity with a direct contractual relationship with the Department. Any reference to "subcontractor(s)" in this SORN includes any business entity with an indirect contractual relationship with the Department as well as any business entity with a contractual relationship with the Department's contractors. Any general reference to "employee(s)" in this SORN includes, but is not limited to, federal employees, contractor employees, subcontractor employees, grantee employees, subgrantee employees, and any other individual, paid or unpaid, who provides goods or services to the Department or its contractors (*e.g.,* interns).

SYSTEM NAME AND NUMBER: DOE-78 Data Analytics Program Records.

SECURITY CLASSIFICATION: Unclassified and classified.

SYSTEM LOCATION: This System of Records will primarily be held in a Federal Risk and Authorization Management Program (FedRAMP)-approved Government Cloud. Access to these electronic records includes any locations that the Department's OIG operates or that support OIG operations, including but not limited to, OIG Headquarters in the Forrestal Building (1000 Independence Ave., SW, Washington DC, 20585). Some or all system information may also be duplicated at other locations where the Department has granted direct access to support OIG operations, system backup, emergency preparedness, or continuity of operations. To determine

the location of particular records, contact the system manager, whose contact information is listed in the System Managers section.

SYSTEM MANAGER(S): Assistant Inspector General for Cybersecurity Assessments and Data Analytics, Kshemendra Paul, Office of the Inspector General, Department of Energy, 1000 Independence Ave., SW, Rm. 5B-250, Washington DC, 20585.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 42 U.S.C. 7101 *et seq.*; 50 U.S.C. 2401 *et seq.*; Inspector General Act of 1978, as amended, 5 U.S.C. 401-424, P.L. 95-452; DATA Act, Public Law 113–101, 31 U.S.C. 6101 note, 128 Stat. 1146; 31 U.S.C. 3521 *et seq*.; Inspector General Empowerment Act of 2016, Public Law 114–317, 130 Stat. 1595.

PURPOSE(S) OF THE SYSTEM: The system will aggregate, store, and use data OIG has the legal authority to collect and maintain to perform statistical analytics, data science, link analysis, and other mathematical techniques. The primary goal of this work is to identify anomalies that may indicate systemic or specific risks as well as fraudulent, abusive, wasteful, unlawful, or unethical activity in DOE programs and operations. The analysis may support other parts of OIG by helping to identify specific areas for OIG attention or the development of risk indicators. Other parts of OIG may use the analytic output of the system to determine predication or indication for audits, inspections, evaluations, and investigations, including joint refinement of preliminary analysis, under their specific authorities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The categories of individuals covered by the system include current and former: DOE employees; DOE contractor, subcontractor, or consultant employees; persons suspected of violating DOE regulations, policies, or laws; recipients of DOE grants, awards, or funds, whether direct or indirect; parties to DOE cooperative agreements; non-appropriated funded employees; and interns of DOE.

CATEGORIES OF RECORDS IN THE SYSTEM: In connection with OIG's broad oversight responsibilities to recognize and mitigate fraud, waste, abuse, and mismanagement in the programs and operations of the Department, this system may retain any or all the categories of

records available in current and prior, previously approved DOE SORNs, such as those available at 74 FR 994 (January 9, 2009).

In connection with OIG's broad oversight responsibilities of the programs and operations of the Department to recognize and mitigate fraud, waste, abuse, and mismanagement, examples of data the system may contain, link, or access include the following types of data:

- Any unique identifiers for Department employees and applicants for employment with the Department (*e.g*., DOE OneID, employee number, and any other government identifier);
- Any personally identifiable information (PII) or combination of PII that can be used to identify a specific individual (*e.g.,* name, date of birth, Social Security numbers, corporate-issued identifier such as a frequent flyer number);
- Department charge card data (*e.g.*, travel, purchase, fleet and integrated card transactions);
- Records of purchases of goods and services by the Department, contractors, subcontractors, grantees, and subgrantees;
- Federal, contractor, and subcontractor contracting actions and every modification thereof;
- Single audit results;
- Lists of Departmental contractors, subcontractors, grantees, and subgrantees; their ownership, officers and directors, auditors, and significant vendors;
- Lists of Departmental contractor, subcontractor, grantee, and subgrantee employees; their work unit, compensation, and timekeeping records;
- Financial awardees (grants and contracts) related to scientific research, indirect programs, etc.;
- Any bidding information related to procurement or any type of financial assistance, including grants and cooperative agreements;

- Any attempt to form a monetary or non-monetary (*e.g.*, intellectual property) relationship with the Department;
- Lists of IP addresses maintained by the Department and contractors that support Departmental activities (*e.g.*, online transactions);
- Lists of system identifiers/location information assigned to Departmental network;
- Travel records (*e.g.*, Department travel records and General Services Administration travel records);
- Timekeeping, project charge codes, and payroll information (including banking data); or
- Records, reports, and files from other parts of the Department, its contractors, subcontractors, and other Federal Agencies.

RECORD SOURCE CATEGORIES: The records within this System of Records are sourced from the following: the subjects of audits, inspections, evaluations, and investigations; individuals with whom the subjects of investigations are associated; current and former Departmental officers and employees; Federal, State, local, foreign, tribal, and territorial agencies; other Offices of Inspectors General; other Federal databases; private citizens; witnesses; informants; public source materials; contractors, subcontractors, grantees, and subgrantees; financial institutions including those managing Department credit card and payroll information; and the system managers, or individuals acting on a system manager's behalf, for the DOE systems of records OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits, inspections, evaluations, and investigations of Department programs and operations to recognize and mitigate fraud, waste, and abuse.

Public source materials (open data) can include information derived from websites, maps, and other similar information. Open data may be used on an *ad hoc, predicated* basis to support situations when there is a specific need. The collection of information from open data sources

will be managed in accordance with the legal and regulatory framework protecting the civil rights and civil liberties of individuals.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND 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 of DOE as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. A record from the 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.
2. 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; (3) witnesses, potential witnesses, or their representatives and assistants; and (4) any other persons who possess information pertaining to the matter when it is relevant and necessary to obtain information or testimony relevant to the matter.
3. 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.

4. A record from the system may be disclosed as a routine use to DOE contractors, subcontractors, grantees, and subgrantees 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.
5. A record from this system of records may be disclosed as a routine use to a Federal, state, tribal, or local agency to facilitate the requesting agency's decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter. The Department must deem such disclosure to be compatible with the purpose for which the Department collected the information.
6. 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.
7. 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.

8. 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.
9. A record from this system may be disclosed as a routine use to another federal, state, local, foreign, territorial, or tribal unit of government, including an Office of Inspector General, Congressional oversight committees/subcommittees, and Government Accountability Office, for the purposes of identifying fraud, waste, abuse, or improper payments related to federal programs, employees, contractors, subcontractors, grantees, subgrantees, or other beneficiaries of federal funds.
10. A record from this system may be disclosed as a routine use to complainants or victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigations or cases arising from the matters of which they complained or of which they were a victim.
11. A record from this system may be disclosed as a routine use to any person or entity that OIG has reason to believe possesses information regarding a matter within the jurisdiction of OIG, to the extent deemed to be necessary by OIG in order to elicit such

information or cooperation from the recipient for use in the performance of an authorized activity.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored in an electronic form in a framework of computer systems that allows distributed processing of data sets in a cloud infrastructure. Records are stored securely in accordance with applicable executive orders, statutes, and agency implementing recommendations. Any electronic records that are stored on hard disks, removable storage devices, or other physical media are similarly stored securely in accordance with applicable executive orders, statutes, and agency implementing recommendations. Records may be stored as paper records and maintained in locked cabinets.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records in this system of records can be retrieved by name or other identifiers, including but not limited to: a surname; Social Security number; Taxpayer Identification Number, including Employer Identification Number; email address; physical address; telephone number; bank account numbers; data elements from government-issued identification, such as driver's license or photo identification number; OIG-assigned case numbers; Alien Registration Number; assigned DOE charge card information; DOE unique identifier; any other DOE-assigned numbers; geo-code location (e.g., physical addresses converted into geographic coordinates on a map); Internet Protocol (IP) address; organizational name; employee payroll identifier; General Services Administration (GSA) Unique Entity Identifier; Data Universal Numbering System (DUNS number); grant awards; financial assistance awards; photographs; biometric information; or any other unique identifier that can be linked to an individual.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retained and disposed of in accordance with the applicable records schedule for the systems from which they were collected. Any unscheduled records will be retained indefinitely,

until they have been scheduled with the National Archives and Records Administration and have become eligible for disposition under those schedules.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Electronic records may be secured and maintained on a cloud-based software server and operating system that resides in 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 the National Institute of Standards and Technology 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 and/or administer the system.

RECORD ACCESS PROCEDURES: The Department follows the procedures outlined in title 10 Code of Federal Regulations (CFR) part 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, 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 of denials relating to records maintained in government-wide System of Records reported by Office of Personnel Management (OPM), shall be filed, as appropriate, with the Assistant Director for Agency Compliance and Evaluation, OPM, 1900 E Street NW, Washington, DC 20415. All other appeals relating to DOE records shall be directed to the Director, Office of Hearings and Appeals (OHA), 1000 Independence Ave. 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: The Secretary plans to exempt this system from subsections (c)(3) and (4); (d)(1)-(4); (e)(1)-(3), (4)(G), (4)(H), and (4)(I); (e)(5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the system has

been exempted from the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5). The exemptions will be applied only to the extent that the information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) or (k)(5). Rules are in the process of being promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e), and will be published in the Federal Register.

HISTORY: This notice proposes to establish DOE-78 Data Analytics Program Records as a new System of Records. There has been no previous publication in the *Federal Register* pertaining to this System of Records.

Signing Authority

This document of the Department of Energy was signed on November 9, 2023, 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 20, 2023.

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

[FR Doc. 2023-25983 Filed: 11/24/2023 8:45 am; Publication Date: 11/27/2023]