Affects Members Of the Public?	X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: **https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file**

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	02/07/2023
Departmental Element & Site	FECM (Fossil Energy and Carbon Management/National Energy Technology Laboratory /NETL/EDX
Name of Information System or IT Project	Energy Data Exchange (EDX), Google Cloud Platform Deployment
Exhibit Project UID	
New PIA ☒ **Update** ☐	

	Name, Title	Contact Information Phone, Email
System Owner	Kelly Rose	(O) (541) 967-5883 Kelly.Rose@netl.doe.gov
Local Privacy Act Officer	Ann Guy	(M) (202) 555-1212 Ann.Guy@netl.doe.gov

PRIVACY PROGRAM

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Justin Woodford	(D) 541-918-4508 justin.woodford@netl.doe.gov
Person Completing this Document	Timothy Jones (T.J.)	(M) 304-276-4967 timothy.jones@netl.doe.gov / timothy.jones@avncorp.com
Purpose of Information System or IT Project	The purpose of this PIA is to explain the migration of the on-prem EDX production environment to Google Cloud Platform. EDX is the Department of Energy (DOE)/Fossil Energy's (FECM) virtual library and data laboratory built to find, connect, curate, use and re-use data to advance fossil energy and environmental Research & Development. Developed and maintained by the National Energy Technology Laboratory (NETL), Energy Data eXchange (EDX) supports the entire life cycle of data by offering secure, private collaborative workspaces for ongoing research projects until they mature and become catalogued, curated, and published. NETL has been working with IM-50 to have Google Cloud Platform (GCP) projects established and GCP accounts created. EDX developers have been developing the entire ecosystem, Dev/Test/Prod projects, Continuous Integration/ Continuous Delivery (CI/CD) pipelines for automated deployments, infrastructure for each, Kubernetes containerization, Security Command Center tools, and network firewalls, etc. This migration is done to keep up with growth within industry, increase dynamic scalability, performance benefits, network connectivity performance increase, automation (deployments, CI-CD pipeline optimizations), future growth for cloud compute for the EDX community. Users of EDX wants the work to be attributable. EDX adheres to DOE Cyber policies as well as domestic and international standards for data curation and citation. This ensures data products pushed public via EDX are afforded a citation for proper accreditation and complies with journal publication requirements.	
Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number	

MODULE I – PRIVACY NEEDS ASSESSMENT

☐ Clearance Information e.g. "Q"

☐ Biometric Information e.g. finger print, retinal scan

☐ Mother's Maiden Name

☐ DoB, Place of Birth

☒ Employment Information (examples)* Employment information is 100% optional and is not required. That specific information in simply Job Occupation Title, Organization Name, and Phone number. Again, all optional.

☐ Criminal History

☒ Name, Phone, Address When registering, NETL only requires users to generate a username, provide First and Last name (as Full Name), valid email address, a password (stored encrypted), an NETL POC's Name and Email address if they are not registering with a .gov / .mil email address for proof of collaboration, and Organization Affiliation Type. That is all that is required.

☒ Other

Optional content can be completed after registration was successful and account was approved. Those fields are Job Occupation Title, Organization Name, and Phone number. Users can only show that information to logged in users, all users, or not provide it at all.

Website for registration can be found here:

https://edx.netl.doe.gov/user/register

Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1,** *Department of Energy Privacy Program,* **defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	No
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

MODULE I – PRIVACY NEEDS ASSESSMENT

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	YES (If "Yes," place an "X" in the box at the top of first page.) *Member of the Public* refers to individuals in a non-employee or DOE contractor context. *Members of the Public* includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE
4. Is the information about DOE or contractor employees?	YES (If Yes, select with an "X" in the boxes below) ☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

MODULE I – PRIVACY NEEDS ASSESSMENT

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. Seq
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Individuals can refuse to register for an account. An account on EDX is optional at the registrant's discretion. When registering NETL only requires users to generate a username, provide First and Last name (as Full Name), valid email address, a password (stored encrypted), an NETL POC's Name and Email address if they are not registering with a .gov / .mil email address for proof of collaboration, and Organization Affiliation Type.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Yes, Contractors are involved with the development, design, and maintenance of the system. The Privacy Act Clause is a part of the contract.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed the EDX system has been identified as a moderate risk system for confidentiality, integrity, and availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. EDX is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • Encryption While EDX contains some PII, the ensuing risk to the privacy of individuals is generally low as the focus of EDX is to keep up with growth within industry, increase dynamic scalability, performance benefits, network connectivity performance increase, automation (deployments, CI-CD pipeline optimizations), and future growth for cloud compute for the EDX community. This does not require or encourage collection of sensitive PII and is not driven by analysis of PII. EDX observes several protections to protect privacy and via the Fair Information Practice Principles (FIPPs). EDX maintains the minimum PII necessary for its operational purpose to mitigate privacy harm. In addition, use of the PII in EDX is limited to clearly defined business purposes furthering privacy interests at DOE. Access to and use of PII in EDX and the GCP is protected by role and permission-based monitoring controls. Access is restricted to authorized users with a need to know and is verified through a series of technical controls to ensure user privacy is protected. The only PII collected by EDX includes administrative PII pertaining to contact information. Information in this system is limited to name and work information.

MODULE II – PII SYSTEMS & PROJECTS

5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Yes. Searches could potentially show full name, email address, and business affiliation. Business affiliation and email address are hidden by default. Users can determine if they want their email address and business affiliation visible.
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	• OPM GOVT-1
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Individuals provide their own information when signing up for system use. Full Name and email address are required fields on EDX. The default visibility for each user's email address is set to private. However, users can customize their email to be private, visible to registered EDX users, or public. Phone Number, Occupation, and Organization are optional fields on a user's profile. These fields' visibility is private by default. However, a user may choose to make these fields public or accessible to registered EDX users.
9. Will the information system derive new or meta data about an individual from the information collected?	No

MODULE II – PII SYSTEMS & PROJECTS

10. Are the data elements described in detail and documented?	Yes
DATA USE	
11. How will the PII be used?	Full Name can be used for user searches. Names may also appear within a published research product within EDX if the user chooses to be attributed to the content.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	N/A – The system is not deriving additional metadata.
13. With what other agencies or entities will an individual's information be shared?	Authors of a published data citation is public and can be shared with anyone including any agency or entity.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	None
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	If needed, we can locate individuals that are registered in the system and monitor their user sessions via system logging.

MODULE II – PII SYSTEMS & PROJECTS

18. What kinds of information are collected as a function of the monitoring of individuals?	User sessions with the system.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Role based, with only system administrator access to system logs.

DATA MANAGEMENT & MAINTENANCE

20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	Full name, email address, phone, and organization are entered and maintained by the user.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A – Migration of EDX from on-prem to GCP, we will not be running both locations concurrently.

Records Management

22. Identify the record(s).	Project Data, Technical Reports, Journal Articles, Fact Sheets, Geospatial Data, and other project related information.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. X Unscheduled ☐ Scheduled *(cite NARA authority(ies) below)* Currently, EDX is Unscheduled. While most of the individual records identified are scheduled (Projects, Technical reports, Journal Articles, Fact Sheets) it has yet to be determined how EDX, and the information contained within, will be handled. Until that determination is made, likely later this year, EDX will be considered unscheduled and treated as Permanent (not eligible for destruction).
24. Records Contact	Ryan Morrone, ryan.morrone@netl.doe.gov (O) (412) 386-4693

MODULE II – PII SYSTEMS & PROJECTS

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	EDX uses role-based security. Only registered users can contribute to EDX and their account privileges determine what they have access to. Truly public data and information is accessible to registered and non-registered users. Anything on EDX that is public (on EDX website) can be accessible by the public. Only name and work email are made public on website, all users are aware of this. Additionally, original contributors and/or assigned editors of a public data submission can modify published submissions at any time. Only the original contributor can assign additional editors to a submission. No other user in the system can modify a public submission.
26. Who will have access to PII data?	Full Name is accessible to all users. Email, Phone, Occupation, and Organization are visible based on the registrant's discretion. The EDX Operations Manager will also have access to registrant data to aid in support and/or verification/validation of user personnel.
27. How is access to PII data determined?	Full Name is accessible to all users. Email, Phone, Occupation, and Organization are visible based on the registrant's discretion. The EDX Operations Manager will also have access to registrant data to aid in support and/or verification/validation of user personnel.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	NETL Privacy Officer NETL Authorizing Official

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	_____ **(Print Name)** _____ **(Signature)**	_____
Local Privacy Act Officer	_____ **(Print Name)** _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** _____ **(Signature)**	_____