Affects Members Of the Public? □

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: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

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	August 20, 2024	
Departmental Element & Site	Office of the Chief Financial Officer, Headquarters - Office of the Chief Information Officer (OCIO) EITS Data Center and Cloud Services (DCCS) environment	
Name of Information System or IT Project	Integrated Data Warehouse (IDW)	
Exhibit Project UID	019-000000122	
New PIA □ **Update** ☒	Reviewed for 2024 A&A. Removed coverage of NNSA Tableau. NNSA Tableau will have its own PIA.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Richard Tomlinson Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-0937 Richard.Tomlinson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Ana Manchester Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ana Manchester, ISSM Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Person Completing this Document	Richard Tomlinson Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-0937 Richard.Tomlinson@hq.doe.gov
Purpose of Information System or IT Project	The IDW links common data elements from each of the Department's corporate business systems. As the Data Warehouse evolves, each manager will use the IDW as a "knowledge bank" of information about portfolios, programs or projects including budget execution, accumulated costs, performance achieved, and critical milestones met. The IDW Portal provides personalized dashboards, messaging (thresholds/alerts), reporting, graphing, and data exchange capabilities to DOE executives, managers, and staff.	
Type of Information Collected or Maintained by the System:	☒ Social Security number (SSN) - used as a unique identifier for backend queries, but only in hashed format. ☐ Medical & Health Information ☒ Financial Information - includes budgeting information, financial accounting, cost accounting, and performance measurement ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ Date of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ Other	

MODULE I – PRIVACY NEEDS ASSESSMENT

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

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?	No
4. Is the information about DOE or contractor employees?	Yes ☒ 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. There are no other additional sources of authority for this system.
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)?**	Data provided through an interface with a corporate repository (DOEInfo) contains information on the DOE Federal workforce. The IDW Rules Of Behavior (ROB) explicitly advises users that "All information, including personal information, placed on or sent over this system may be monitored, recorded and audited". Additionally, there are two buttons that grant the user the option to either agree or disagree with the rules stated. If they do not accept the rules of behavior, they will not be able to use the system. IDW users can provide additional voluntary information about themselves on their Profile section in IDW.

MODULE II – PII SYSTEMS & PROJECTS

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?**	Contractors are involved in the design, development, and maintenance of the system. Contractor roles include both system administration and information administration and processing. Personal information may be disclosed to these contractors and their officers and employees in performance of their contracts. The individuals provided this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis in accordance with least privilege. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed IDW as a moderate-risk systems according to the criteria set forth in Federal Information Processing Standard 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. The unauthorized disclosure of information is expected to have adverse effect on organizational operations, organizational assets, or individuals. DOE recognizes there are risks involved with all Information Technology systems, and the steps that are later described in this document have been taken to limit access and secure the system. IDW 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 and least privilege • Audit logs Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of IDW being compromised. These include role-based access, further restricted to only the data authorized for their organizations use except for system administrators and display of the SSNs are limited to only the last four digits.
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.**	Data can be retrieved by an employee username or employee number through ad hoc queries and reports within IDW, including audit logs.

MODULE II – PII SYSTEMS & PROJECTS

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*.**	The system operates under the following Privacy Act systems of records: • DOE-2 Supervisory Maintained Personnel Records • DOE-11 Emergency Locator Records • DOE-18 Financial Accounting System • DOE-53 Access Authorization for ADP Equipment
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	The system is not collecting new or additional information. The current Systems of Records do not require amendment or revision.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The data is being provided through an interface with a corporate repository (DOEInfo) containing personnel and payroll information on the DOE Federal workforce. The IDW users can also provide information about themselves. The information can be provided on the Profile section in IDW. This information does not require PII, but at the user's discretion, may include information such as name, work e-mail, work telephone number, business mobile number, business postal address, and employee's expertise.
9. Will the information system derive new or meta data about an individual from the information collected?	Aggregate and trend data about groups of employees will be derived from the information from DOEInfo.
10. Are the data elements described in detail and documented?	The Data Interface Agreement (DIA) with DOEInfo lists the tables from which data is being extracted. There is currently no document from the DOEInfo source system describing the data elements.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The IDW links common data elements from each of the Department's corporate business systems. As the Data Warehouse evolves, each manager will use the IDW as a "knowledge bank" of information about portfolios, programs or projects including budget execution, accumulated costs, performance achieved, and critical milestones met. The IDW Portal provides personalized dashboards, messaging (thresholds/alerts), reporting, graphing, and data exchange capabilities to DOE executives, managers, and staff.
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?**	The data will be used to look at general employee statistics such as employee hiring data, age ranges of employees and employees approaching retirement. The meta data will not be part of an individual's record.
13. With what other agencies or entities will an individual's information be shared?	N/A
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Travel and training reports are produced at the summary and detail level. At the detail level the report displays the information by employee; with the exception of the name, there is no personal information. A report showing the organization, displays information about an individual listing their name, service start date, years of service, projected retirement date and veteran's preference. Other reports show trends or summary data related to the hiring process, workforce training, diversity, performance summary and succession; they contain no individual data (other than name). Some reports, accessible only by top management, show individual's information on an organization chart and on reports related to awards, details by pay period and Quality Step Increases (QSIs).
15. What will be the use of these reports?	Includes reports on succession planning, trend analysis and employee mobility and diversity.

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	For any given DOE organization, the managers in that organization have access to the dashboards and reports. No other agencies or governmental organizations have access to these reports.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, for the limited use of security purposes, system audit logs are maintained to record system activity and user activity.
18. What kinds of information are collected as a function of the monitoring of individuals?	For security purposes, system audit logs are maintained to record system activity and user activity. This activity includes invalid logon attempts and access and modification to data in the system. The Operating System/Server logs maintained by the EITS environment contains IP information; this is separate from the application/database logging specific to IDW.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	IDW established policies and procedures for controlling and monitoring access to the system. These are defined in the Security Plan and are compliant with privacy controls in NIST 800-53, rev 5.
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.	New and updated data is received from DOEInfo and used to update IDW on a daily basis. However, it has not impacted the PII already declared in prior and current Privacy Impact Assessments.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	IDW is hosted in Microsoft Azure Gov Cloud in Virginia through the Energy Information Technology Services Data Center and Cloud Services (EITS DCCS) – though it may be accessed by authorized users from any internal DOENET access point.
Records Management	

MODULE II – PII SYSTEMS & PROJECTS	
22. Identify the record(s).	IDW contains records related to Strategic Planning, Reporting & Information, Capital Planning, Workforce Planning, Travel, Official Information Dissemination, Information System Security, and Personal Identity and Authentication.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 1.1 and GRS 1.3.030 are applicable.
24. Records Contact	Sean Kennedy, Records Manager Sean.Kennedy@hq.doe.gov 240-315-6772
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Through the Office of the Chief Financial Officer's (CF) Assessment and Accreditation program and annual assessment processes, all baseline security controls have been implemented and tested as appropriate to its Federal Information Processing (FIPS) categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE Directives. The system was certified and accredited with full Authority To Operate and found to have mitigated risk to an acceptable level. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via user-id and password based on user responsibility and job function. These access controls are defined in the system security plan. All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a prerequisite for the system access. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non-disclosure agreements, role-based access so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system.

MODULE II – PII SYSTEMS & PROJECTS

26. Who will have access to PII data?	DOE Federal and contractor personnel with authorized access to DOE networks will have access to their own data in the system. Access to PII of others in the system will be strictly controlled based on job responsibility and function. System Administrators and help desk staff will have access to all data in the system. Payroll personnel have access to data for those individuals they are responsible to administer.
27. How is access to PII data determined?	If a user is authorized to access the data, then the DBAs will assign a role to that user allowing them to access the dashboards or reports containing the PII data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. All existing connections between IDW and non-CF-40 systems have a data interface agreement
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?	Yes
30. Who is responsible for ensuring the authorized use of personal information?	System Owner, the Chief Financial Officer, and the Director for Corporate Business Systems.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Richard Tomlinson** **(Print Name)** RICHARD TOMLINSON Digitally signed by RICHARD TOMLINSON Date: 2024.09.12 11:56:01 -04'00' **(Signature)**	
Local Privacy Act Officer	**Ana Manchester** **(Print Name)** ANA MANCHESTER Digitally signed by ANA MANCHESTER Date: 2024.09.24 08:08:04 -04'00' **(Signature)**	
Chief Privacy Officer	**William K. Hunt** **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.09.12 09:11:11 -04'00' **(Signature)**	