PRIVACY IMPACT ASSESSMENT:
Office of Chief Financial Officer
DOEInfo-ESS

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: 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 15, 2023
Departmental Element & Site	Office of the Chief Financial Officer, Headquarters
Name of Information System or IT Project	DOE Employee Data Repository (DOEInfo) Employee Self Service (ESS) General Support System (GSS)
Exhibit Project UID	019-000000121
New PIA ☐ **Update** X	This is an annual update for the PIA. An updated PIA for this system will be submitted to the Chief Privacy Officer for review within twelve (12) months.

	Name, Title	Contact Information Phone, Email
System Owner	Logan Kwedar Office of Corporate Business Systems, CF-40 Germantown, U.S. Department of Energy	(301)-903-2145 Logan.Kwedar@hq.doe.gov
Local Privacy Act Officer	Ana Manchester, ISSM Office of Corporate Business Systems, CF-40 Germantown, U.S. Department of Energy	(301)-903-9360 ana.manchester@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ana Manchester, ISSM Office of Corporate Business Systems, CF-40 Germantown, U.S. Department of Energy	(301)-903-9360 ana.manchester@hq.doe.gov
Person Completing this Document	Gene Hughes Office of Corporate Business Systems, CF-40 Germantown, U.S. Department of Energy	(301)-903-4281 Gene.Hughes@hq.doe.gov
Purpose of Information System or IT Project	DOEInfo is a repository of information relating to the DOE Federal workforce. This information covers a wide range of data, including, but not limited to, Personnel, Payroll, Salary, Benefits, and Manpower (FTE) data. One critical function DOEInfo provides to the department is its ability to combine various Personnel information with Payroll information for reporting purposes. The Employee Self Service (ESS) system enables DOE employees to view their own payroll, personal and training information and update certain information on the Internet. Currently, employees are able to update the following information online: home address, emergency contacts, education, license and certification information, voluntary allotments, federal and state tax withholdings, direct deposit of the paycheck, locator information and their Thrift Savings Plan (TSP). Employees can also connect to Learning Nucleus to complete and submit Individual Development Plan (IDP) and other training tasks.	
Type of Information Collected or Maintained by the System:	☒ Social Security number (SSN) ☐ Medical & Health Information ☒ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ Date of Birth and Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify - Payroll, Salary and Benefits, Leave, Earnings, & Deductions, Diversity, FECA (Workmans Comp), Comp Time, Time Off Awards,	

MODULE I – PRIVACY NEEDS ASSESSMENT

	Security, Education & Training, Emergency Contact, Personnel Actions (SF-50), Disability Information.
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.*	N/A
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?	Yes – Dependents associated with an active or inactive (retired/deceased) employee only Information includes SSN and emergency contact information
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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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.

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., 50 U.S.C. 2401 et. seq.; Freedom of Information Act, 5 U.S.C. 552. 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)?**	Federal Employees: Employees are required to provide PII in order to be employed at DOE. This information is used only for employee payroll, benefits, leave, training, security, personnel actions to manage workforce planning and diversity requirements. The consent of individuals to provide this information flows from the source system to DOEInfo, this includes employee consent to provide information for their dependents and beneficiaries, as needed, for them to be covered and receive benefits afforded to them through employment at the Department. Contractor Employees: Employees are required to provide PII only to facilitate communications between the DOE federal and contractor workforce, including sponsorship verification by federal contracting officers and technical representatives.

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. 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. 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.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed DOEInfo-ESS as a moderate risk system according to the criteria set forth in the 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. DOEInfo is also selected as one of DOE's High Value Assets (HVA) and monitored for meeting HVA requirements set for by federal and DOE guidelines. The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of DOEInfo-ESS from being compromised. This includes encrypting data at rest, role-based access, (further restricted to only the data authorized for their organizations use), and display of a full 9 digit SSN to a few key users (primarily within HC) – all others with any SSN access are limited to only the last 4 digits of the SSN. Any issues previously identified are evaluated and corrected consistent with Managements direction as documented within the A&A process.

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.**	Data may be retrieved by name, last 4 digits of SSN, full SSN (limited to certain members within HC and DOEInfo-ESS support staff), and DOE issued employee id (5 digit internal identifier – not to be confused with the DOE OneID).
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: • OPM/Gov-1 • DOE-2 Supervisory Maintained Personnel Records • DOE-3 Employee Concerns Program Records • DOE-5 Personnel Records of Former Contractor Employees • DOE-11 Emergency Locator Records • DOE-13 Payroll and Leave Records • DOE-16 Federal Employee Subsidy Program Records • DOE-28 General Training Records
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	

MODULE II – PII SYSTEMS & PROJECTS	
8. What are the sources of information about individuals in the information system or project?	Personal employee information is not obtained from individuals, but is obtained from the following sources: • Corporate Human Resource Information System (CHRIS) • Defense Civilian Payroll System (DCPS) • Standard Accounting and Reporting System (STARS) • HRMIS (Bonneville Power Administration (BPA) Personnel/Payroll Application) • Employee Self Service (ESS) • Automated Time & Attendance Production System (ATAAPS) External • Defense Civilian Payroll System (DCPS)
9. Will the information system derive new or meta data about an individual from the information collected?	No
10. Are the data elements described in detail and documented?	Yes, data elements are described in detailed under "Database Information" (login required).
DATA USE	
11. How will the PII be used?	The primary purpose of the DOE*Info* system is to serve as a repository of information relating to the DOE Federal and contractor workforce. This information covers a wide range of data, including federal employee personnel, payroll, salary and benefits, manpower (FTE) data, and federal and contractor employee locator information.
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

MODULE II – PII SYSTEMS & PROJECTS	
13. With what other agencies or entities will an individual's information be shared?	• Equal Employment Opportunity Commission (EEOC) • Bureau of Labor Statistics (BLS) • Subsidy for Energy Employee Transit (SEET – Sent to Department of Transportation) • Freedom of Information Act (FOIA) requests.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports may be produced to contain any of the information maintained in the system database. Types of standard reports include: • Retirement Eligibility Summary/Detail • Trend Analysis • Retention Allowance • On Board Counts • Workforce Reporting • SF-50 Reporting • Projected Use/Loss • Training Reports • SF113G Report (OPM Requirement)
15. What will be the use of these reports?	Reports are generated by authorized users on an ad hoc basis. These reports will be used only to conduct required departmental human resources responsibilities and activities and is not available to the public.
16. Who will have access to these reports?	The system allows authorized DOE HR staff to query and produce reports on individuals or groups of individuals. Data can be viewed or extracted as files or through ad hoc queries based on user permissions.
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.

MODULE II – PII SYSTEMS & PROJECTS	
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 contain IP information, this is separate from the application/database logging specific to DOEInfo-ESS.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	DOEInfo-ESS established policies and procedures for controlling and monitoring access to the system. These are defined in "Security Plan for Employee Data Repository (DOEInfo)" and are compliant with privacy controls in NIST 800-53.
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.	DOEInfo is a set of entities, databases, and tables, holding data from all DOE corporate systems containing employee data. The systems feeding data to DOEInfo are considered the authoritative sources. DOEInfo does not attempt to validate or correct the data as part of its function, it only hosts the data as a central repository and makes the data available to authorized users/systems. System Data Interconnection Agreements (DIA's) are documented and maintained by the DOEInfo-ESS System Owner. Data received from source systems is not duplicative, but rather integrated and consolidated to make current and historical data accessible efficiently by the department's authorized users.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	System is only maintained at DOE HQ Azure GovCloud in the EITS DC&SS – though it may be accessed by authorized users from any internal DOENET access point.
Records Management	
22. Identify the record(s).	Employee records such as compensation and benefits, employee ratings, awards, and training records.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	The records in DOEInfo have not yet been scheduled electronically but would fall under: Employee Management Records: GRS 2.2, items 030, 070, 072 Employee Compensation and Benefits Records: GRS 2.4, item 040 Employee Training Records: GRS 2.6, items 030
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 necessary 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.
26. Who will have access to PII data?	DOE Federal and contractor personnel with authorized access to DOE networks will have access to their individual data in the system. System Administrators and help desk staff will have access to all data in the system. Human resource and payroll personnel have access to data for those individuals they are responsible to administer. Program users may have access only to data for their organizations.

MODULE II – PII SYSTEMS & PROJECTS	
27. How is access to PII data determined?	System Access control lists are established to allow users access to only view and change their own data in the system. Human resource and payroll personnel have access to data for those individuals they are responsible to administer. Program users may have access only to data for their organizations.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. All existing connections between DOEInfo-ESS and other systems have a Data Interconnection Agreement (DIA)
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	**Logan Kwedar** (Print Name) LOGAN KWEDAR Digitally signed by LOGAN KWEDAR Date: 2024.04.22 14:30:15 -04'00' (Signature)	
Local Privacy Act Officer	**Ana Manchester** (Print Name) ANA MANCHESTER Digitally signed by ANA MANCHESTER Date: 2024.04.23 08:05:23 -04'00' (Signature)	
Chief Privacy Officer	**William K. Hunt** (Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.22 11:00:21 -04'00' (Signature)	