PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Payroll Modeling Application (PMA)

Affects Members Of the Public? Mark if Applicable w/ an 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-chg1-minchg/@@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	April 10, 2023
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	Payroll Modeling Application (PMA)
Exhibit Project UID	019-000000122
New PIA ☐ **Update** ☒	April 10, 2023 "Other – DOE Employee ID" has been added (checked) in the "Type of Information Collected or Maintained by the System" section and several pages have been updated with the names of new officials.

	Name, Title	Contact Information Phone, Email
System Owner	Pavani Gundamraju Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	202-853-0442 Pavani.Gundamraju@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	Pavani Gundamraju Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	202-853-0442 Pavani.Gundamraju@hq.doe.gov
Purpose of Information System or IT Project	The Payroll Modeling Application (PMA) is a web-based application used to forecast future payroll expenses. Actual historic costs and forecasted projections allows Department of Energy (DOE) budget analysts and administrative officers to create various payroll forecasting models. Within the PMA application, expenses are compared against actual salaries and costs to project costs for the remainder of the year. By retaining the detailed payroll information necessary to support the forecasted salary expense, PMA allows Department of Energy (DOE) budget analysts and administrative officers to create various payroll forecasting models. Within the system individuals can be identified by organization, grade/step, and health benefit codes. PMA was split from CF40 SBS enclave in 2022. CF40 is the division and Small Business Systems (SBS) which is an enclave of several other FISMA systems. PMA is now it's own separate FISMA system. The application is used by all offices in the Department but is only available within DOENET to those users with DOE HQ Domain accounts maintained by The Enterprise Information Technology Services (EITS) group.	
Type of Information Collected or	☐ Social Security Number (SSN) ☐ Medical & Health Information ☒ Financial Information - Personnel events actual or planned that affect compensation or benefits. ☐ Clearance Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

Maintained by the System:	☐ Biometric Information ☐ Mother's Maiden Name ☒ Date of Birth and Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – DOE Employee ID (a 5-digit unique identifier used only within DOE)
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?	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 I – PRIVACY NEEDS ASSESSMENT

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.

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.

MODULE II – PII SYSTEMS & PROJECTS	
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 on the employees (individuals) in the system is pre-populated and updated periodically through a data feed from the Department's employee database, DOEInfo. The consent of individuals to provide this information flows from the source system to DOEInfo. PMA provides DOE with the ability to model and predict personnel costs for budget and planning purposes. As part of PMA's functionality, access to DOE workforce information is needed. This interface allows PMA to access, in a read-only mode, the DOEInfo database for the purposes of obtaining needed information in support of the PMA system
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 were involved with the design and development of the system and will be involved with the maintenance of the system. Personal information may be disclosed to contractors and their officers and employees in performance of their contract. Individuals provided this information are subject to the same limitation 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 are required to safeguard all information they may obtain in accordance with the provisions of the Privacy Act and the requirements of 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 PMA 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 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 PMA from being compromised. Security controls such as Role Based Access Controls (RBAC) and Single Sign On (SSO) leveraging OneID integration. These access controls are defined in the system security plan**.**
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 is retrieved by organization code, and then by name.
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-13 Payroll and Leave Records

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	The PMA 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 source of all data in the system is a nightly data feed from DOEInfo.
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, the data elements are described in the security documentation.
DATA USE	
11. How will the PII be used?	The Payroll Modeling Application (PMA) is a web-based application used to forecast future payroll expenses. These expenses are compared against actual salaries and costs to project costs for the remainder of the year. By retaining the detailed payroll information necessary to support the forecasted salary expense, PMA allows Department of Energy (DOE) budget analysts and administrative officers to create various payroll forecasting models. Within the system individuals can be identified by organization, grade/step, and health benefit codes (but not by date-of-birth, address, or SSN). The system uses Employee ID not SSN to uniquely identify individuals.

MODULE II – PII SYSTEMS & PROJECTS	
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
13. With what other agencies or entities will an individual's information be shared?	None
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Payroll/salary budget forecasts can be created and used to generate reports.
15. What will be the use of these reports?	PMA is a budget tool for what-if scenarios (e.g., how much money will be needed next year, depending on direction headed).
16. Who will have access to these reports?	Authorized analysts can see payroll/salary budget forecasts based on their permissions within the system.
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 PMA.

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	PMA 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 4.
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.	There is a daily data feed from DOEInfo. Access to DOEInfo must be authorized by the DOEInfo System Owner, and that access must be necessary for the potential user to carry out assigned job functions. Privileges granted for that purpose must comply with the principles of separation of duties and of least privilege. That is, a potential user has no access to Enterprise resources or applications unless authorized by the owner of the resource or application and the user has only as much access privilege as is needed to perform the assigned tasks. This interface will be restricted to data in six specific views created for the PMA granted to the application server user ID. The Application Server ID and password will be provided to the individual listed above. This individual will maintain the ID and will abide by the password rules outlined in the DOEInfo Rules of Behavior. This interface with DOEInfo is a "pull" process; no notification is provided by DOEInfo. DOEInfo does not expect any notification by PMA that the interface has occurred.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system is only maintained at DOE HQ in the Energy Information Technology Services (EITS) Data Center and Cloud Services (DCCS), though it may be accessed by authorized users directly from DOE intranet. Privileged access to the database is only available within DOENET, using 2 factor authentication.
Records Management	
22. Identify the record(s).	Employee Compensation and Benefits Records

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	DOE 2.4, item 010 Employee Payroll Record for each Pay Period
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 Role Based Access Controls (RBAC) and Single Sign On (SSO) leveraging OneID integration. 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?	Authorized budget officials and administrative officers have access to the data.
27. How is access to PII data determined?	Authorized users of the system are assigned rights in the system based on their job requirement for access to the information in the system.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, see Data Interface Description between PMA and DOEInfo.
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, a Data Interface Description is in place between PMA and DOEInfo.
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	**Pavani Gundamraju** (Print Name) PAVANI GUNDAMRAJU Digitally signed by PAVANI GUNDAMRAJU Date: 2024.03.01 15:52:44 -05'00' (Signature)	
Local Privacy Act Officer	**Ana Manchester** (Print Name) Ana M. Manchester Digitally signed by Ana M. Manchester Date: 2024.03.05 09:25:14 -05'00' (Signature)	
Chief Privacy Officer	**William K. Hunt** (Print Name) WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.02.28 12:59:31 -05'00' (Signature)	