PRIVACY IMPACT ASSESSMENT:
Office of Chief Financial Officer
SEPA

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	Jamaury 6, 2025
Departmental Element & Site	Office of the Chief Financial Officer, Headquarters
Name of Information System or IT Project	Standard Accounting and Reporting System - Southeastern Power Administration (SEPA)
Exhibit Project UID	019-000000122
New PIA ☐ **Update** X	This is an updated PIA from the one approved April 9, 2018.

	Name, Title	Contact Information Phone, Email
System Owner	Somashekar Krishnamurthy Office of Corporate Business Systems, CF-40 Germantown, U.S. Department of Energy	(301)-903-2145 Somashekar.krishnamurthy@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	Suzette Bailey-Jones Office of Corporate Business Systems, CF-40 Germantown, U.S. Department of Energy	240-243-5532 suzette.bailey-jones@hq.doe.gov
Purpose of Information System or IT Project	The Southeastern Power Administration has a separate instance of Oracle Federal Financials Application, to support the accounting needs of the Southeastern Power Administration. This system is referenced throughout the remainder of this document by its system acronym "SEPA". SEPA is built upon the Financial Systems Integration Office (FSIO) certified Oracle Federal Financials Applications and provides a centralized system operated from a single accounting center. Oracle U.S. Federal Financials is a Commercial Off-The-Shelf (COTS) software package that provides the basis for an integrated financial management solution for federal agencies, providing features such as budgetary control, fund accounting, online funds checking, cost accumulation and allocation, United States Standard General Ledger (US SGL) accounts, Treasury cash accounts, regulatory and ad hoc reporting, multiple fund receivables accounting, and multiple organization capabilities.	
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 - Taxpayer Identification Number (TIN) of corporations	
Has there been any attempt to verify PII does not exist on the system?		N/A

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	
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 The categories of individuals include employees, contractor employees, and vendors who are either due money from or owe money to the Southeastern Power Administration

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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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.
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)?**	In order for individuals to be reimbursed for products and services provided, they are required to provide this information. This information is used only to perform the required accounting functions.
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. 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 SEPA 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 SEPA from being compromised. These include 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 the Payment Services Center) – all others with any SSN access are limited to only the last four digits of the SSN. Any issues previously identified are evaluated and corrected consistent with Management's direction as documented within the A&A process.
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 retrievable only by name, taxpayer identification number, voucher, and invoice or payment reports.
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-18 Financial Accounting System

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	SEPA 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?	Information is entered manually into the system regarding requisitions, purchase orders, invoices, and payments.
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 the Oracle documentation.
DATA USE	
11. How will the PII be used?	The system generates invoice monitoring and payment status reports, and reports for the Department of Treasury that contains personal information. These reports are used to verify, certify and batch payments and monitor the status of invoices. PII information is only used to perform the required accounting functions.
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?	Accounting and financial information will be shared with Department of Treasury and Federal Reserve Bank.
Reports	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Standard Oracle reports may be produced to contain any of the information maintained in the system database.
15. What will be the use of these reports?	These reports will be used to verify, certify and batch payments and monitor the status of invoices. Reports are generated by authorized users. Reports are not available to the general public.
16. Who will have access to these reports?	Data can be accessed and viewed based on user permissions at the Southeastern Power Marketing Administration.
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 contain IP information, this is separate from the application/database logging specific to SEPA.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	SEPA established policies and procedures for controlling and monitoring access to the system. These are defined in the Security Plan for SEPA and are compliant with privacy controls in NIST 800-53.
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS	
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.	The system is designed to automatically verify the accuracy, including whether the data is current, and the completeness of data input to the system. The system will compare the data inputted using field edits. For example, a name, address and taxpayer identification number would be checked against the system record data, which are DOE records collected and verified by other systems prior to being placed in SEPA. If this information does not match, transactions involving this data will fail and a notification requiring corrective measures and actions will be sent to the appropriate responsible person. This may involve manual verification and correction of data in the system.
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).	Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting; records related to agency financial statements and related audits; and property, plant, and equipment
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	The records in SEPA have not yet been scheduled electronically but would fall under: Financial Management and Reporting Records: GRS 1.1, items 010, 011, 020, 030, 040, and 050
24. Records Contact	Sean Kennedy, Records Manager Sean.Kennedy@hq.doe.gov 240-315-6772
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
	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.
25. What controls are in place to protect the data from unauthorized access, modification or use?	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 have access to the data in SEPA. Access to personal data in the system will be strictly controlled based on job responsibility and function. Generally, personal data has been removed or masked within the inquiry, non-system set-up, and non-Treasury payment related responsibilities. Senior manager review and approval is required prior to assigning access rights to users. Since the production environment is fluid (i.e., new users being added/ user access being removed/changing job responsibilities) reports are generated on a regular basis and reviewed to ensure access rights continue to align with roles/job responsibilities assigned to an individual and minimize access to privacy information to only those requiring it in order to perform their job responsibilities. Information including PII data is shared as required with Department of Treasury and the Federal Reserve Bank to facilitate financial transactions.

MODULE II – PII SYSTEMS & PROJECTS	
27. How is access to PII data determined?	Access to data is determined by evaluation of personnel job responsibilities and functions. Based on the evaluation, access control lists are documented and applied to the system. System controls and integrity reports are reviewed on a regular basis to ensure users have the appropriate level of access.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. All existing external interfaces have a Data Interconnection 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. Data Interface Agreements (DIAs) are in place for system interconnections: Internal: • Vendor Inquiry Payments Electronic Reporting System (VIPERS)
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	**Somashekar Krishnamurthy** (Print Name) Somasheka Krishnamurthy Digitally signed by Somasheka Krishnamurthy Date: 2024.12.05 11:26:46 -05'00' (Signature)	
Local Privacy Act Officer	**Ana Manchester** (Print Name) ANA MANCHESTER Digitally signed by ANA MANCHESTER Date: 2024.12.09 13:59:14 -05'00' (Signature)	
Chief Privacy Officer	**William K. Hunt** (Print Name) WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.12.03 13:42:26 -05'00' (Signature)	