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	July 1, 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	Financial Accounting Support Tool (FAST)
Exhibit Project UID	019-000000122
New PIA ☐ **Update** ☒	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	Katie Shular Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	240-562-1879 Katie.Shular@hq.doe.gov

PRIVACY PROGRAM

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	Katie Shular Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	240-562-1879 Katie.Shular@hq.doe.gov
Purpose of Information System or IT Project	FAST is a web-based system that allows the Department of Energy to review/approve invoices electronically and delivers these approvals to the DOE accounting system, Standard Accounting and Reporting System (STARS), through a secure portal. FAST services the approving official community for the DOE. The system is used to approve, route or reject invoices as well as provide a mechanism for approving officials to notify payment staff of vendor information updates. The users are DOE approving officials. FAST is also used to process corporate billed purchase and travel card distributions, month/year-end contract cost accruals, invoice entry such as miscellaneous invoices and to track erroneous payments. The system supports paperless payments using electronic records retention.	
Type of Information Collected or Maintained by the System:	☒ Social Security Number (SSN) ☐ Medical & Health Information ☒ Financial Information - Personnel events actual or planned that affect compensation or benefits ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ Date of Birth and Place of Birth ☐ Employment Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

☐ 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. Vendors are not considered members of the public for privacy purposes.
4. Is the information about DOE or contractor employees?	☒ 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. There are no other additional sources of authority for this system.

PRIVACY
PROGRAM

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)?**	Vendor's and Federal employees submitting invoices for fitness and training costs do not have a choice in providing information into FAST. This information was supplied by them through Vendor Invoicing Portal & Electronic Reporting System (VIPERS) and is automatically pulled by FAST or entered through the FAST invoicing modules (MISC, Employee Reimbursement). FAST validates the employment status of federal employees and contractor invoice processors by checking authoritative sources of this information. These individuals approve the use of their information as part of their job duties.
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 FAST as a moderate-risk system 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 an 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 FAST from being compromised. These include role-based access, and further restricting access to authorized users, including the display of a full 9-digit SSN.
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.**	Information is retrieved by invoice number, not PII; however, PII information may be present on invoices.
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 in accordance with the following DOE Systems of Records (SORs): 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?**	The system is not collecting new or additional information. The 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?	FAST accesses DOE's accounting system, STARS, to retrieve invoice information which will have information on vendors and federal employees submitting invoices. FAST also accesses HQ DOEINFO to retrieve federal employee data for the purpose of employee validation. FAST maintains a database of contractors with invoice approval authority. For invitational travelers or new employees traveling soon after their hire date, DOE collects SSNs to setup employee records in STARS. If a convenience check is written to an individual, the card holder provides their SSN so that they will receive the correct 1099 tax forms for the IRS.
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. FAST PII data include the following government vendor data elements: TIN/SSN, bank account numbers, routing numbers, and the name/address of the vendor. Federal employee data include SSN, bank account numbers, routing numbers, and the name of the federal employee.
DATA USE	

PRIVACY
P R O G R A M

MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	PII data is used within FAST modules for data validation purposes. It is necessary to ensure that the accurate payments are made to the correct vendors. The FAST Supplier Portal validates data records against TIN or SSN, and Organization/Individual Name in order to qualify the data for supplier data changes. Within the convenience check/international transaction log PII data captured is used in tax reporting.
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?	Invoice approving officials and payment staff can run invoice reports from FAST. PII information may be present on invoices.
15. What will be the use of these reports?	The invoices are reviewed to make a payment approval determination.
16. Who will have access to these reports?	Access to the reports is limited to the Program Official, Approving Official, and the Contract Specialist of a Purchase Order.
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 contains IP information; this is separate from the application/database logging specific to FAST.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	FAST 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.	Individuals submitting invoices maintain the accuracy of their information through VIPERS or through the Employee Reimbursement Module. Invoice Approving Officials are maintained in STARS. The Supplier Portal promotes data accuracy. It facilitates changes to the supplier records. Data is validated with external sources before changes are manually made to the source database (STARS).
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 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
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Financial Management and Reporting Records: GRS 1.1, items 010, 011, 030, 040, and 050

PRIVACY
PROGRAM

MODULE II – PII SYSTEMS & PROJECTS

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?	Federal employees and contractor invoice processors will have access. Access to personal information is controlled through MFA.
27. How is access to PII data determined?	Access is determined by user roles and is limited to Federal and support service contractor personnel involved in the payment processing.

PRIVACY PROGRAM

MODULE II – PII SYSTEMS & PROJECTS

28. Do other information systems share data or have access to the data in the system? If yes, explain.	There is a FAST data transfer to STARS.
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 both system interconnections: Internal: • DOEINFO • STARS External: • CITI • Wright Express.
30. Who is responsible for ensuring the authorized use of personal information?	System Owner, the Chief Financial Officer, and the Director for Corporate Information Systems.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Katie Shular** _____ (Print Name) _____ (Signature)	_____
Local Privacy Act Officer	**Ana Manchester** _____ (Print Name) _____ (Signature)	_____
Chief Privacy Officer	**William K. Hunt** _____ (Print Name) _____ (Signature)	_____