MA-5049

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 electronically: no hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	May 5, 2010
Departmental Element & Site	Office of the Chief Financial Officer, Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy, DOE Headquarters, Germantown, hosted in the OCIO's Application Hosting Environment (AHE) in the CA-007 server room.
Name of Information System or IT Project	iManage Standard Accounting and Reporting System (STARS) STARS is a module within the Integrated Management Navigation System (iManage) enclave, a major general support system (GSS).
Exhibit Project UID	019-60-01-01-01-1028-00
New PIA ☐ **Update** X	iManage Standard Accounting and Reporting System (STARS)

	Name, Title	Contact Information Phone, Email
System Owner	Laura Kramer, STARS Project Manager Office of Corporate Information Systems, CF-40, Germantown, U.S. Department of Energy	(301) 903-9932 Laura.Kramer@hq.doe.gov
Local Privacy Act Officer	Jerry Hanley Chief Privacy Officer, U.S. Department of Energy	(202) 287-1563 Jerry.Hanley@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Phil Knopp, CF Cyber Security Program Mgr. Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy	(301) 903-0364 Phil.Knopp@hq.doe.gov
Person Completing this Document	Laura Kramer, STARS Project Manager	(301) 903-9932 Laura.Kramer@hq.doe.gov
Purpose of Information System or IT Project	The Standard Accounting and Reporting System (STARS) is a project within the Integrated Management Navigation System (iManage) program. iManage is a key cornerstone in the Department's efforts to implement improved financial performance, integrated budget and performance, and expanded electronic government, as outlined in the President's Management Agenda. iManage STARS replaced the Department's legacy financial system, the Departmental Integrated Standardized Core Accounting System (DISCAS) in April of 2005. iManage STARS provides a centralized system operated from a single accounting center, and a single payment center. iManage STARS is built upon Joint Financial Management Improvement Program (JFMIP) certified Oracle Federal Financials Applications. It provides support for general ledger, accounts payable / receivable, fixed assets, funds control, and financial and cost accounting, and limited purchasing functionality. iManage STARS includes budget execution functionality associated with recording appropriations, apportionments, allotments, sub-allotments, commitments, obligations, costs, and funds control. iManage STARS integrates performance metrics with budget, obligations, and costs, and provides standard federal financial reporting and strong, ad-hoc query and reporting capability.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☒ Financial Information e.g. credit card number Note: Credit card information is stored in STARS for individual users; however, the credit card numbers are for DOE travel accounts, which would not be considered personal information. ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify - Taxpayer Identification Number (TIN)
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.*	Yes
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Information is reviewed by DOE officials to verify if PII is contained in the system.

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 Department of Energy (DOE).

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of

MODULE I – PRIVACY NEEDS ASSESSMENT

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.

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?**	As provided in DOE O 206.1, "The Privacy Act allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President." 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.

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)?**	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 were involved with the design and development of the system and will be involved with the maintenance of the system. 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. Pertinent 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.

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	STARS rates a Moderate for Privacy Impact Analysis. The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The current implementation of the STARS security controls mitigates any impact on privacy.
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, 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*.**	Yes. DOE-18 Financial Accounting System
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	No. The system is not being modified. Based on current and planned activities, the SORN will not require amendment or revision.
DATA SOURCES	

8. What are the sources of information about individuals in the information system or project?	Personal information residing in the system on an individual is placed in the system by the individual themselves; however, the process of vouchers for monies due to individuals or collect monies owed to the Department information is obtained from the following interfaced systems: • GovTrip interfaces with the system to process authorizations and vouchers and creates the accounting entries required to process employee travel. • CHRIS provides training obligations. • The Strategic Integrated Procurement Enterprise System (STRIPES) interfaces with the system to check funding availability, commit, and obligate funding, and update the obligation with the vendor profile when the procurement is awarded to a vendor. • DOEInfo: Employee extracts information from the DOEInfo repository and updates the iManage STARS with the banking information in the Accounts Payable module, and the vendor tables in the Purchase Order module.
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?	Data elements are described in the iManage STARS design 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 only 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. The system does not derive meta data.

13. With what other agencies or entities will an individual's information be shared?	Required accounting and financial information will be shared with Department of Treasury and Federal Reserve Bank.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The system will generate invoice monitoring and payment status reports, and reports for the Department of Treasury that contain personal information.
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.
16. Who will have access to these reports?	Access to these reports is restricted to employees based on their job responsibilities and functions as defined in "Access Control Policies and Procedures for the Department of Energy iManage Program-STARS Project." Users assigned the following system responsibilities/roles can see SSN via employee entry or from output files: AP and FV Administrator PO Application Administrator DOE Employee Update DOE GL Superuser DOE GovTrip Interface DOE Employee Interface DOE PO CHRIS Interface DOE Debug STARS access control lists are maintained internally within the STARS Oracle database structure and as such, the Oracle Applications security layer programmed logic within the system enforces user access rights to roles/functions a user can perform. Hardware or software features are designed to permit only authorized access to or within the application - to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). Senior manger 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.
Monitoring	

17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. iManage STARS does not have the capability to identify, locate, and monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
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.	The system software 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 and trial balance. For example, a name, address and tax payer identification number would be checked against the system record data, which are DOE records collected and verified by other DOE systems prior to being placed in STARS. 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 system administrator. 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?	The system is operated at one site only.
Retention & Disposition	
22. What are the retention periods of data in the information system?	Data retention for this system is conducted in accordance with DOE Administrative Records Schedule 6: Accountable Officers Accounts Records, dated 6/14/2007. (see http://www.cio.energy.gov/documents/ADM_6.pdf)
23. What are the procedures for disposition of the data at the end of the retention period?	Data retention for this system is conducted in accordance with DOE Administrative Records Schedule 6: Accountable Officers Accounts Records, dated 6/14/2007. (see http://www.cio.energy.gov/documents/ADM_6.pdf)
ACCESS, SAFEGUARDS & SECURITY	

24. What controls are in place to protect the data from unauthorized access, modification or use?	Laura Kramer (System Owner and STARS Project Manager), through CF's Certification and Accreditation and annual assessment processes, has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system was certified and accredited with full Authority To Operate on March 12, 2008, and found to have mitigated risk to an acceptable level." Additionally, iManage STARS has developed policies and procedures for controlling and monitoring access to the system. These are defined in "IT0031, ARC 309 Access Control Policies and Procedures for the Department of Energy iManage Program-STARS Project." 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 "IT0031, ARC 309 Access Control Policies and Procedures for the Department of Energy iManage Program-STARS Project." 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, separation of duties so individuals only have access to appropriate pieces of personal information, and use of system audit logs to monitor access and user activity in the system.

25. Who will have access to PII data?	DOE Federal and contractor personnel have access to the data in the system as well as Department of Treasury and Federal Reserve Bank. Access to personal data in the system will be strictly controlled based on job responsibility and function. STARS Users assigned the following system responsibilities/roles can see SSN via employee entry or from output files: AP and FV Administrator PO Application Administrator DOE Employee Update DOE GL Superuser DOE GovTrip Interface DOE Employee Interface DOE PO CHRIS Interface DOE Debug Additionally STARS users assigned the following responsibilities/roles can see banking information (not included if noted above for SSN): Invoice Entry Invoice Exception Entry PO Exception Approver PO Maintenance (PO Entry) Payment Entry Payment Exception Entry Supplier entry Supplier Entry without banking Supplier Merge STRIPES PO Exception Approver DOE AP IPAC Entry DOE AP IPAC Exception Entry STARS access control lists are maintained internally within the STARS Oracle database structure and as such, the Oracle Applications security layer within the system enforces user access rights to roles/functions a user can perform. Hardware or software features are designed to permit only authorized access to or within the application - to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). Senior manger 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.

26. 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.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	The iManage STARS system interfaces with several systems. These systems are listed below in one of three categories: Inbound, Outbound, and Inbound/Outbound. Inbound means that data only flows in one direction - from STARS to the system. Outbound means that data only flows in one direction - from the system to STARS. Inbound/Outbound means that data flows in both directions between the system and STARS: Inbound ▪ DOEInfo ▪ Working capital Fund ▪ Corporate Human Resource Information System ▪ Non-Integrated Contractor Cost Driver ▪ Integrated Contractor Outbound ▪ Vendor Inquiry Payments Electronic Reporting System ▪ iManage Data Warehouse Inbound/Outbound ▪ Funds Distribution System ▪ Labor Distribution System ▪ DOE/C-Web and Small Purchase System (SPS) ▪ iManage Strategic Integrated Procurement Enterprise System (In Progress) ▪ Financial Management Service – Automated Standard Application for Payment ▪ Financial Management Service - Host-to-Host ▪ GovTrip
28. 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. Interconnection Security Agreements are in place and operating for all systems that interface with iManage STARS.
29. 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	Laura Kramer (Print Name) Laura J. Kramer (Signature)	5/5/2010
Local Privacy Act Officer	Jerry Hanley (Print Name) N/A (Signature)	
Jerry Hanley **Chief Privacy Officer**		06/01/10
Ingrid Kolb **Senior Agency Official for Privacy (SAOP)**	N/A NONPUBLIC	