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	July 24, 2023
Departmental Element & Site	Office of the Chief Financial Officer DOE Headquarters, Germantown, Data Center System Services (DC&SS)
Name of Information System or IT Project	The Foreign Travel Management System (FTMS)
Exhibit Project UID	019-000000450 00-60-01-17-02-00
New PIA ☐ **Update** ☒	No substantive changes from previously approved PIA. Minor editorial changes have been made and the signature page has been updated.

	Name, Title	Contact Information Phone, Email
System Owner	Paul Riggs Office of Corporate Information Systems, CF-40, Germantown, U.S. Department of Energy	(301) 903-0969 Paul.Riggs@hq.doe.gov
Local Privacy Act Officer	Ana Manchester Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy	(301) 903-4792 Ana.manchester@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Lee Canda, ISSM, Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy	(301) 903-2077 lee.canda@hq.doe.gov
Person Completing this Document	Paul Riggs Office of Corporate Information Systems, CF-40, Germantown, U.S. Department of Energy	(301) 903-0969 Paul.Riggs@hq.doe.gov
Purpose of Information System or IT Project	The Foreign Travel Management System provides automated support to the official foreign travel trip approval process as defined in DOE Order 551.1C, Official Foreign Travel. The system provides for the routing of travel requests to the various DOE program offices that must approve the trip before a DOE federal employee or contractor may travel abroad. FTMS serves as the DOE official source of foreign travel information, including names of DOE employees and contractors who travel abroad, passport information, countries visited, number of trips taken per year and purpose of travel. The system maintains records of international conferences and keeps a tally of the number of DOE participants in order to stay within DOE attendance guidelines.	
Type of Information Collected or Maintained by the System:	☐ Social Security Number (SSN) ☐ Medical & Health Information ☐ Financial Information ☒ Clearance Information - "Q" ☐ Biometric Information ☐ Mother's Maiden Name ☒ Date of Birth, Place of Birth – DoB, City are encrypted via Oracle's encryption ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other –Traveler Itinerary, Passport 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*	N/A	

MODULE I – PRIVACY NEEDS ASSESSMENT

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?	Yes
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.

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. Title 41 Code of Federal Regulations (CFR), Chapter 301, Federal Travel Regulations, Temporary Duty (TDY) Travel Allowances 41 CFR, Chapter 304, Federal Travel Regulations, Payment from a Non-Federal Source for Travel Expenses. Presidential Decision Directive 12, Security Awareness and Reporting of Foreign Contacts, dated 8-5-93. Title 5 United States Code (U.S.C.) 5703 (see 10 CFR Part 1060, Payment of Travel Expenses of Persons Who Are Not Government Employees).
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)?**	A basic set of data elements are required to support the foreign travel process. However, certain elements are optional and may or may not be provided based on the traveler's determination. Even if the traveler does provide the optional data, she/he cannot determine the uses of the information. DOE senior management has the authority to deny/release reports containing this information within DOE if there is a job related need.

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. 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.
4. IMPACT ANALYSIS: How does this project or information system impact privacy?	DOE has assessed FTMS 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. FTMS is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • Audit Logs • Security Training • System reviews 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 FTMS from being compromised. Any issues previously identified are evaluated and corrected consistent with Management's 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 is currently retrieved by the use of a unique ID assigned to each traveler. The traveler's name is used to obtain the unique ID and retrieve the data.
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 27- Official Foreign Travel
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?	FTMS receives data on new trips from ETS2 (DOE's travel management system for federal employees) via secure FTP using private key authentication. Currently DOE's Los Alamos National Laboratory, Oak Ridge National Laboratory, Lawrence Livermore National Laboratory, Fermi National Accelerator Laboratory and Pacific Northwest Laboratory upload data to FTMS via a Web Service connection. The IP addresses and user ID/password for any incoming data are checked against the authorized set of IP addresses and users established by the system owner to ensure only those authorized are able to perform an upload of data are able to run the process. Information about individuals is also manually entered into the FTMS system.
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 FTMS System User Guide, Data Dictionary, and input screens via screen help functionality.
DATA USE	
11. How will the PII be used?	The Foreign Travel Management System provides automated support to the official foreign travel trip approval process as defined in DOE Order 551.1C, Official Foreign Travel. The system provides for the routing of travel requests to the various DOE program offices that must approve the trip before a DOE federal employee or contractor may travel abroad. FTMS serves as the DOE official source of foreign travel information, including names of DOE employees and contractors who travel abroad, passport information, countries visited, number of trips taken per year, and purpose of travel. The system maintains records of international conferences and keeps a tally of the number of DOE participants in order to stay within DOE attendance guidelines.

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?	N/A
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	There are reports including names of DOE employees and contractors who travel abroad, passport information, countries visited, number of trips taken per year, and purpose of travel.
15. What will be the use of these reports?	These reports are used to review trip information prior to approving the individuals travel request and can be used by the traveler to review his/her travel information. These reports are also used by the Office of Intelligence staff to determine whether or not a pre-briefing of the traveler is necessary prior to the individual departing.
16. Who will have access to these reports?	Access to reports is determine by role within the application. Authorized Emergency Management Office and the Intelligence / Counter Intelligence Office users have access to information on travelers including their names and trip information across all sites.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	FTMS provides the capability to report a traveler's identity and travel location based on the information submitted. It does not have the capability to monitor individuals. Data is currently retrieved by the use of a unique number assigned to each traveler. 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 MoveLINQs.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	FTMS 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.	Data in the system are reviewed by DOE's program office officials prior to their approval of individual travel requests.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	FTMS is only maintained at DOE HQ via the Azure GovCloud – though it may be accessed by authorized users from any internal DOENET access point.

Records Management

22. Identify the record(s).	FTMS keeps records of Foreign Travel, Dates, destinations, and passports. The only financial information in the system is the estimated travel cost, which is an optional field.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	The records in FTMS have not yet been scheduled electronically but would fall under: Financial Management and Reporting Records: GRS 1.1, item 011.- travel costs if provided Admin 9.1.1a for travel information details

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 CF's Assessment and Accreditation program and annual assessment processes, all baseline security controls have been implemented and tested as 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 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 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, 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.
26. Who will have access to PII data?	The application is controlled by roles with privileges ranging from view only which can only see reports for their specific site through System Administrator who have access to all of the data in the system. External requests for data require CFO management approval.

MODULE II – PII SYSTEMS & PROJECTS

27. How is access to PII data determined?	FTMS Senior Administrators determine what access users will be provided by selecting the user's role when approving their account. The available roles are: System Administrator – has access to all functions in the application. Can only be granted by another System Administrator. Limited to the FTMS application support team. Senior Organizational Point of Contact (OPOC) - oversees his/her site and is able to create, route, approve, and closeout trips; and approve user accounts. Headquarter OPOC - has the same functions as Senior OPOC plus manages conferences. Site OPOC – is able to create, route, approve, and closeout trips at their site. Web Service User- Able to connect to the FTMS Web Service Senior Data Entry – is able to create, route and closeout trips at their site. Data Entry - is able to create and closeout trips at their site. Traveler - is able to create and closeout only his/her trips. Approver - can approve trips routed to the individual approver. View Only - security personnel who need to review travel. They can access reports (read only) for their site.

MODULE II – PII SYSTEMS & PROJECTS

28. Do other information systems share data or have access to the data in the system? If yes, explain.	Various other applications share data with FTMS; including the State Department's electronic Country Clearance System (eCC), DOEs ETS2 system and various laboratory travel systems. ETS2 only sends data to FTMS, there is no access to information stored in FTMS. The eCC system is similar; FTMS pushes data to eCC (triggered by an FTMS user), but the eCC system itself has no way of accessing data in FTMS. The various laboratory systems are limited to the personnel data of their travelers located at their site. They are limited through the connection to the same information each individual user would be able to see logging into FTMS. Web services hosted as part of FTMS provide upload access to FTMS data and allows the remote Lab's system both push and pull from FTMS.
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. All existing connections between FTMS and other systems have a Data Interconnection Agreement (DIA).
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	**Paul Riggs** —————————————— (Print Name) —————————————— (Signature)	———————
Local Privacy Act Officer	**Ana Manchester** —————————————— (Print Name) —————————————— (Signature)	———————
Chief Privacy Officer	**William K. Hunt** —————————————— (Print Name) —————————————— (Signature)	———————