PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Concur Government Edition (CGE)
E-Gov Travel Service (ETS2)

Affects Members Of the Public?	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	June 11, 2024
Departmental Element & Site	Sponsoring Federal Agency: General Services Administration (GSA) Hosted by Concur Technologies Inc. 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	E-Gov Travel Service (ETS2) (DOE Data)
Exhibit Project UID	019-000000117 00-60-01-17-02-00
New PIA [ ] **Update** [X]	No substantive changes from previously approved PIA. Minor editorial changes have been made and the signature page has been updated.

MODULE I – PRIVACY NEEDS ASSESSMENT

	Name, Title	Contact Information Phone, Email
System Owner	Paul Riggs Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-0969 Paul.Riggs@hq.doe.gov
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.)	Lee Canda Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-2077 lee.canda@hq.doe.gov
Person Completing this Document	Paul Riggs Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-0969 Paul.Riggs@hq.doe.gov
Purpose of Information System or IT Project	This is a PIA for the DOE data contained within the Government-wide system ETS2, hosted by Concur Technologies Inc. GSA is the sponsoring Federal agency for the ETS2 system and, in this role, has made the system available for use by other Federal Agencies. As the sponsoring agency, GSA assumes much of the risk for the system. The ETS2 system is a proprietary system owned and managed by CONCUR Technologies Inc. ETS2 travel services are provided to DOE under a contractual agreement and travel services are purchased based on the number of travel vouchers processed for official DOE business travel for both domestic and foreign travelers. ETS2 is an automated, web-based travel administration system and is configured on hardware and software maintained and owned by CONCUR Technologies Inc. The function of the system is to provide travel services for DOE employees on official business. The process includes preparation of travel vouchers, authorizations, approvals, expense payment and/or re-imbursements.	

MODULE I – PRIVACY NEEDS ASSESSMENT

	This system provides authorized DOE employees the ability to make travel plans and reservations, approve travel requests and vouchers, and supports reimbursement of allowable travel expenses. The records in the system are maintained and used by DOE to document official domestic and foreign travel and relocation expenditures and to support reimbursement of allowable expenses.
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 ☐ Criminal History ☒ Name, Phone, Address ☒ Other – (Gender, Passport # for international flights, Traveler Number (optional), Redress Number for travelers having identical names, travel location address)
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

MODULE I – PRIVACY NEEDS ASSESSMENT

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 The system contains information about individuals who travel at the expense of DOE. This may include DOE Federal employees and DOE invitational travelers (e.g., scientists or dignitaries).
4. Is the information about DOE or contractor employees?	Yes ☒ Federal Employees ☒ Contractor Employees NOTE: For contractors this is limited to only those contractors supporting the application and then only to non- sensitive PII.

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., 50 U.S.C. 2401 et. seq.; Freedom of Information Act, 5 U.S.C. 552. 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)?**	Individuals who travel at the expense of DOE are required to provide personal identifying information. The information is used to approve and plan travel, and to receive reimbursement for allowable travel expenses. When an employee initially logs into the system, or changes their password, they must agree to the Privacy Act statement concerning the data collected for individuals.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order**	Contractors are involved in the 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.

MODULE II – PII SYSTEMS & PROJECTS	
CRD or Privacy Act clauses included in their contracts?	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 ETS2 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 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 moveLINQ from being compromised. 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 can be retrieved by the traveler's name, traveler's e-mail address, travel authorization number, or document name. Personally Identifiable Information can be retrieved by the traveler's name, traveler's e-mail address, or traveler ID. Report output may include Personally Identifiable Information as well. The various data elements can be retrieved in the same manner in which they are input, i.e., via secure Internet connection, system login, and password. Retrieval is limited to the individuals who may input the data

MODULE II – PII SYSTEMS & PROJECTS	
	elements, except that agency travel managers and the System Administrator may also access data in the system.
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*.**	General Services Administration, System of Records under the Privacy Act of 1974, contracted Travel Services program: • GSA/GOVT-4 • DOE 26 Official Travel Records
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	ETS2 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?	Travelers or an authorized travel arranger with the permission of the traveler will enter traveler profile data. Travelers, travel arranger, or in some instances the System Administrator will enter TAVS data. In addition, there may be an initial upload and periodic updates of financial, HR, and travel card account data, to permit proper Electronic Fund Transfer (EFT) payments to the travel card vendor and to the traveler. The updates contain existing data which already resides within agency applications. The user or a designated individual on behalf of the user enters the privacy information. The privacy information is entered by the user or entered on behalf of the user.

MODULE II – PII SYSTEMS & PROJECTS	
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?	The data elements required for making reservations are described and documented in the "Help" feature of the on-line profile and booking engine systems. All data elements, including TAVS requirements as well as on-line booking data, are also included in the System Administrator Guide. Data Schema designs are also provided as a source for documented data elements.
DATA USE	
11. How will the PII be used?	All data in the system is relevant and necessary for DOE to perform its required responsibilities for administering and managing the DOE travel program. PII data, specifically DoB and other Secure Flight Information is needed for on-line reservations. The agency will use this data to complete travel arrangements end-to-end. The data will be used to make travel reservations, produce a voucher for payment, and update the financial system and possible interface with the Human Resource system. They can use the data to provide statistics on many areas, provide the average length of trips, and designate obligated money, to mention a few of the uses for the data. The "Routine uses of records…" section in System of Records, Contracted Travel Services Program: GSA/GOVT-4 states: Information in the system may be disclosed as a routine use as follows: • To a Federal, State, local or foreign agency responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order, where agencies become aware of a violation or potential violation of civil or criminal law or regulation. • To another Federal agency or a court when the Federal government is party to a judicial proceeding.

MODULE II – PII SYSTEMS & PROJECTS

	• To a Member of Congress or staff on behalf and at the requests of the individual who is the subject of the record. • To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler profile information. • To a credit card company for billing purposes, including collection of past due amounts. • To a Federal agency, expert, consultant, or contractor for accumulating reporting data, conducting surveys, and monitoring the • system in the performance of a Federal duty to which the information is relevant. • To a Federal agency by the contractor in the form of itemized statements or invoices, and reports of all transactions, including refunds and adjustments to enable audits of charges to the Federal government. • To a Federal agency in response to its request, in connection with the hiring or retention of any employee; the issuance of a security clearance; the reporting of an investigation to the extent that the information is relevant and necessary to the requesting agency's decision on the matter. • To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee to whom the information pertains. • To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes. • To officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions. • To a travel services provider for billing and refund purposes.

MODULE II – PII SYSTEMS & PROJECTS	
	• To a carrier of an insurer for settlement of an employee claim for loss of or damage to personal property incident to service under 31 U.S.C. Sec. 3721, or to a party involved in a tort claim against the Federal government resulting from an accident involving a traveler. • To a credit reporting agency or credit bureau, as allowed and authorized by law, for the purpose of adding to a credit history file when it has been determined that an individual's account with a creditor with input to the system is delinquent. • Summary or statistical data from the system with no reference to an identifiable individual may be released publicly. • To the National Archives and Records Administration (NARA) for record management.
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?	The system allows authorized DOE staff to query and produce reports on individuals or groups of individuals. The system can produce the following reports: travel summary information for individuals or organizations, authorization, voucher, audit, traveler status and funds tracking.

MODULE II – PII SYSTEMS & PROJECTS	
15. What will be the use of these reports?	EP (Electronic Processing) Reports show what actions have been taken (or not taken) on a document (adjustments, outstanding advances, etc.). Travel Reports include reports showing first class travel and travel requiring additional authorization. Other Reports display detailed trip and traveler information. Ad Hoc Reports are reports that are requested by an agency that become standard reports in ETS2.
16. Who will have access to these reports?	DOE Federal employees and support contractors of the DOE Travel staff whose role within the system provides access to said reports.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Passenger itinerary allows for tracking of individuals when they are on travel. Reports can be produced showing traveler destinations. Access is strictly controlled by permission level and job function. 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 .
19. Are controls implemented to prevent unauthorized monitoring of individuals?	ETS2 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. Individuals are given various levels of access to the system. Only agency travel managers, the System Administrator, and the TMC may access others' records in a manner that constitutes monitoring. In addition, there are policies in place such as the Rules of Behavior which helps to prevent unauthorized monitoring.

MODULE II – PII SYSTEMS & PROJECTS	
	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. 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 nondisclosure agreements and system logs to monitor access and user activity in the system.
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 traveler and travel arranger may review and change profile data at any time, and it is the traveler's responsibility to assure that all profile data is current. Reservation data is current since the on-line system is a real-time booking engine providing confirmation numbers at session's end. If a traveler changes duty location with the agency, certain TAVS data (primarily accounting data) may change, and the traveler, travel arranger, or System Administrator must make the necessary changes at that time. The traveler or travel arranger will verify the accuracy of all employee-entered TAVS data, traveler profile data, and reservation data. In addition, the fulfillment center which issues tickets, typically a TMC, will verify that reservation data are consistent, i.e., that airline tickets rental cars, and hotel reservations are coordinated, and separate hotel and/or car rental reservations do not overlap. The appointed System Administrator for each agency will assure that agency data, e.g., default accounting data, official travel card vendor payment data, etc., are current and accurate. The on-line system will automatically check profile data for completeness, prompting the individual entering data when required fields are not completed. The traveler or travel arranger will check reservation data for completeness. The on-line booking engine will prompt the individual entering reservations, but the automated system will not know whether a traveler requires a hotel room or not, it will not know whether a rental car is required, etc. It is ultimately the traveler's responsibility to assure that reservations are complete and accurate. It will be the traveler's or

MODULE II – PII SYSTEMS & PROJECTS	
	travel arranger's responsibility to assure the data is complete; else payment will likely not be accomplished.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	ETS a web-based SaaS system. The ETS2 Solutions TAVS system is operated and hosted in at one site with components (Online Booking Engine, Help Desk and Receipt Imaging functions) integrated through teaming partner relationships. Continuous monitoring and A&A activities are required to ensure continuity of operations is maintained across vendor component solutions. Users will be geographically separated, securely accessing the system via a web browser over the "Internet".
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.	GRS 1.1 (Financial Management and Reporting Records), Item 010 (Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting) DAA-GRS-2013-0003-0001.
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

MODULE II – PII SYSTEMS & PROJECTS	
	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?	Access controls within the ETS2 Solutions application limit the set of data to which any given user has access. Specifically, a user's access to travel documents is controlled based on a concept of "role-based access" and hierarchical design grouped by (Agency, Organization, Major and Minor Customer). Users are assigned according to their organizational hierarchy which is determined during implementation workshops. Access to an individual's TAVS, profile, and reservation data will be available to the traveler and to the travel arranger. No traveler will have access to another traveler's data, and travel arrangers will have access only to the data of those travelers whom they have been authorized to assist. The Federal Supervisory Traveler Approver (FSTA) and the Federal Financial Travel Approver (FFTA) will have access only to the data of those travelers whom they have been authorized to approve. Access to all individuals' TAVS, profile, and reservation data will be available to Federal agency travel managers and the System Administrator. The profile and reservation data will only be available to the servicing TMC on a need-to-know basis. The TMC and airlines, hotels, and rental car providers will receive system output for reservation, confirmation, and ticketing actions. TSA will also receive information that is in accordance with the Secure Flight requirements. Confidentiality of sensitive data at the operating system level is accomplished through ensuring that the file and directory permissions are properly configured.
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 ETS2 system provides a travel reimbursement file to the DOE Standard Accounting and Reporting System (STARS) two times a day

MODULE II – PII SYSTEMS & PROJECTS	
the data in the system? If yes, explain.	using Secure File Transfer Protocol (SFTP). This allows STARS to reimburse individuals for allowable expenses for authorized DOE travel.
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?	There is an Interconnection Security Agreement (ISA) between ETS2 and STARS. There is also an Interconnection Security Agreement (ISA) between Foreign Travel Management System (FTMS) and Concur.
30. Who is responsible for ensuring the authorized use of personal information?	U. S General Services Administration, Federal Acquisition Service, Office of Travel and Transportation Services, the DOE System Owner, and the Director for Corporate Information Systems.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Paul Riggs** **(Print Name)** PAUL RIGGS Digitally signed by PAUL RIGGS Date: 2024.08.12 06:20:56 -04'00' **(Signature)**	
Local Privacy Act Officer	**Ana Manchester** **(Print Name)** ANA MANCHESTER Digitally signed by ANA MANCHESTER Date: 2024.08.19 13:00:05 -04'00' **(Signature)**	
Chief Privacy Officer	**William K. Hunt** **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.07.26 10:33:59 -04'00' **(Signature)**	