Department of Energy

Privacy Impact Assessment (PIA)

| Affects Members Of the Public? | X |

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

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	July 28, 2009
Departmental Element & Site	General Services Administration NORTHROP GRUMMAN MISSION SYSTEMS (NGMS) GovTrip
Name of Information System or IT Project	GovTrip (DOE data)
Exhibit Project UID	N/A
New PIA ☐ **Update** ☒	This is an update to the PIA for the DOE data contained within the Government-wide system GOVTRIP, hosted by GSA. GSA is responsible for the official PIA for GovTrip, and a copy can be found on the GSA Privacy website.

	Name, Title	Contact Information Phone, Email
System Owner	Miriam Kurtyka Office of Corporate Information Systems	301-903-2970 Miriam.Kurtyka@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
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Phil Knopp Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy	(301) 903-0364 Phil.Knopp@hq.doe.gov

PRIVACY PROGRAM

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Miriam Kurtyka Office of Corporate Information Systems	301-903-2970 Miriam.Kurtyka@hq.doe.gov
Purpose of Information System or IT Project	This is a PIA for the DOE data contained within the Government-wide system GOVTRIP, hosted by GSA. GSA is the sponsoring Federal agency for the GovTrip 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 GovTrip system is a proprietary system owned and managed by Northrop Grumman Mission Systems (NGMS). GovTrip 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. GovTrip is an automated, web-based travel administration system and is configured on hardware and software maintained and owned by NGMS. 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. 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:	☒ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☒ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☒ DoB, Place of Birth (new due to Secure Flight Information) ☒ Employment Information ☐ Criminal History	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Name, Phone, Address ☒ Other – Please Specify (Gender, Passport # for international flights, Traveler Number, Redress Number for travelers having identical names, travel location address) (new due to Secure Flight 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 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, PII does exist in the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	The processes supporting the system provide the verification.

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 or relocate 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: Only Contractors supporting the application**

MODULE I – PRIVACY NEEDS ASSESSMENT

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, 42 U.S.C. 7101 et seq., 52, U.S.C. 2401 et seq.

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)?**	Individuals who travel or relocate 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. The new user registration web page contains a link 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 CRD or Privacy Act clauses included in their contracts?**	Contractors were involved in the design, development, and maintenance of the system. Personal information from GovTrip may be disclosed to these contractors and their officers and employees in performance of their contracts. Those individuals provided with 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 in furtherance of the contract. 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?**	Due to the amount of PII information, the number of travelers and certain of those being members of the public, security controls must be in place and operational to guard against a breach of the system.

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 may be retrieved by name, social security number, and travel authorization number.
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 DOE Systems of Records DOE-26, Official Travel Records.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Information is obtained from the individual to whom it pertains.
9. Will the information system derive new or meta data about an individual from the information collected?	No

MODULE II – PII SYSTEMS & PROJECTS

10. Are the data elements described in detail and documented?	Yes, data elements are described in GOVTRIP Documentation.
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. SSN is required for interface with STARS for payments.
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?**	The system will not derive meta data.
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?	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. For more details on GovTrip reporting capabilities, see link below. http://www.govtrip.com/govtripWBT/basics/reports_tlbr.htm
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 then become standard reports in GovTrip.

MODULE II – PII SYSTEMS & PROJECTS

16. Who will have access to these reports?	DOE Federal employees and support contractors of the DOE Travel staff.

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.
18. What kinds of information are collected as a function of the monitoring of individuals?	Data may be retrieved by name, social security number, and travel authorization number.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	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.	GovTrip does not verify the accuracy or completeness of the DOE federal employees or authorized invitational travelers. The data in the system is provided by the individual to whom it pertains. Therefore, it is determined that the information is accurate, timely and complete at the time it is provided.
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 only at the NG Facility and accessed by DOE personnel across the complex. Consistent use of this system across the DOE complex will be maintained by requiring user training and providing users with system operational documentation.

Retention & Disposition

22. What are the retention periods of data in the information system?	Data retention for travel records of individuals traveling or relocating at the expense of DOE is in accordance with DOE Administrative Records Schedule 9: Travel and Transportation Records, dated 8/18/03.

MODULE II – PII SYSTEMS & PROJECTS

23. What are the procedures for disposition of the data at the end of the retention period?	The procedures for disposition of data in the system for travel records of individuals traveling or relocating at the expense of DOE are defined in DOE Administrative Records Schedule 9: Travel and Transportation Records, dated 8/18/03.

ACCESS, SAFEGUARDS & SECURITY

24. 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 cyber security program plan. All system team members (Federal and contractor) are required to participate in a 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 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 will have access to the data in the system. Access to personal data in the system will be strictly controlled based on job responsibility and function.
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 GovTrip system provides a travel reimbursement file to the DOE Standard Accounting and Reporting System (STARS) three times a day using Secure File Transfer Protocol (SFTP). This allows STARS to reimburse individuals for allowable expenses for authorized DOE travel.
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?	There is an Interconnection Security Agreement (ISA) between GovTrip and STARS.

MODULE II – PII SYSTEMS & PROJECTS

29. 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

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
PIA Approval Signatures	**Original Copy Signed and On File with the DOE Privacy Office**	