U.S. General Services Administration

PRIVACY IMPACT ASSESSMENT

E-Travel Initiative

Electronic Data Systems (EDS)
FedTraveler.com

August 20, 2007

Prepared by:

GSA Office of Governmentwide Policy (OGP)
E-Travel Program (MO)
1800 F Street NW
Washington DC 20405

PART II. SYSTEM ASSESSMENT

A. Data in the System

Question	Response
1. Describe all information to be included in the system, including personal data.	a. E-Gov Travel Service (ETS) is a web-based, end-to-end travel management system to plan, authorize, arrange, process, and manage official Federal Travel. ETS enables travelers and/or travel arrangers to plan and make reservations (air, rail, lodging, car rental, etc.) on-line, prepare travel authorizations and vouchers on-line, and produce itineraries, have tickets issued, and obtain receipts on-line. To register to become a user of ETS, a traveler enters identifying information such as name and password, and completes a profile with personal information, including social security number (SSN), home address, home telephone number, travel preferences, frequent flyer and rental car club account numbers, passport information, emergency contract name, address and telephone number, personal credit card number (official travel charge care account at a minimum), and other information as required by the agency's Travel Authorization and Voucher System (TAVS), Travel management Center (TMC), and transportation providers for making reservations and issuing tickets. b. Name, SSN, UserID, home address, home and office email, home and office telephone numbers, current passport and/or visa number(s), credit card numbers and related information; bank account information needed for electronic funds transfer; frequent traveler account information; travel claim information; destinations; and individual charges and balances. In addition, other passport information (i.e. issuing country, expiration date), and emergency contact information are included.
1.a. What stage of the life cycle is the system currently in?	Implementation
2.a. What are the sources of the information in the system?	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 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. In some cases, the information is entered programmatically from another system.
2.b. What GSA files and databases are used?	None
2.c. What Federal agencies are providing data for use in the system?	Federal agencies with task orders issued under GSA's master contracts for ETS provide data for users in the system. There may be initial uploads (manual and/or programmatic) and periodic updates of data from financial and HR systems of participating Federal agencies.
2.d. What State and local agencies are providing data for use in the system?	None.
2.e. What other third party sources will the data be collected from?	Credit card companies. Other possible sources are the Travel Management Centers (TMC) and GDS which provide hotel, car rental, and airlines information.
2.f. What information will be collected from the individual whose record is in the system?	Name, SSN, UserID, home address, home and office email, home and office telephone numbers, current passport and/or visa number(s), credit card numbers and related information; bank account information needed for electronic funds transfer; frequent traveler account information; travel claim information; destinations; individual charges and balances, and agency specified TAVS information and other accounting data. Other information gathered is emergency contract information, and additional passport information. Additional information may be entered at the traveler's discretion for enhanced service, such as air, hotel, and car rental preferences, and frequent traveler or club membership numbers.

	When travel arrangements are made, the following information is entered: travel dates and times, departure and arrival cities and airports or terminals, selected airline flight or train tickets reserved, hotel reservations, and car rentals reserved. Any special requests or accommodations required are also entered.
3.a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	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 System Administrator will assure that agency data, e.g., default accounting data, official travel card vendor payment data, etc., are current and accurate.
3.b. How will data be checked for completeness?	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 intends to stay with friends or relatives, 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 travel arranger's responsibility to assure the data is complete; else payment will likely not be accomplished.
3.c. Is the data current? How do you know?	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.
4. Are the data elements described in detail and documented? If yes, what is the name of the document?	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 FedTraveler Administrator Guide.

B. Access to the Data

Question	Response
1. a. Who will have access to the data in the system?	Access controls within the FedTraveler.com.com 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 "group access." Users with no group access can only access their own documents; users with access to a given group can access the documents and profiles and other users in the specified group. 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. Confidentiality of sensitive data at the operating system level is accomplished through ensuring that the file and directory permissions are properly configured. Information in the system may be disclosed as a routine use as follows: a. 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. b. To another Federal agency or a court when the Federal government is party to a judicial proceeding. c. To a Member of Congress or staff on behalf and at the requests of the individual who is the subject of

	the record. d. 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. e. To a credit card company for billing purposes, including collection of past due amounts. f. 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. g. 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. h. 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. i. 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. j. 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. k. 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. l. To a travel services provider for billing and refund purposes. m. 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. n. 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. o. Summary or statistical data from the system with no reference to an identifiable individual may be released publicly. p. To the National Archives and Records Administration (NARA) for record management purposes.
1.b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.	Yes. The majority of the records will contain personally identifiable information (PII). Records containing personal information may be considered "personal records" rather than "agency records" with an agency. An agency will need to determine what the file was created for and the nature of the file. Freedom of Information Act, Exemption 6 *Dept. of Justice guidance on exemptions:* *http://www.usdoj.gov/oip/foi-act.htm* *FOIA text:* *http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm,*
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	A user's access to travel documents is controlled based on a concept of "group access." The agency determines what the policies and procedures are for determining a person's access based on their need-to-know. User controls restrict access. Users with access to FedTraveler.com will follow their agency's policies, procedures, and guidance for data access. The System Administrator sets user access levels based on agency sensitivity requirements. Criteria, procedures, controls, and responsibilities regarding access are outline in the System Administrator's Guide. Federal travelers, managers, and System Administrators will access the on-line system through a FIPS-compliant encrypted connection. System safeguards include forced logout, system time-out, password expiration, and lockout after a specified number of failed login attempts. The System Administrator can control and enable these safeguards which are configurable at the agency level and can be customized to meet the Federal agency's needs. Ref: The System Security Plan

3. Will users have access to all data in the system or will the user's access be restricted? Explain.	Access controls within FedTraveler.com.com limit the functions and data available to a given user based on a need-to-know and job responsibilities. The potential for sensitive data to be viewed, modified, or deleted by unauthorized personnel is minimized. An IV&V] was performed on the FedTraveler.com system to ensure that users did not have access to data they were not authorized to view. Traveler access is restricted to that individuals own TAVS, profile, and reservation data, as well as general non-personal reservation and system-use information. A traveler designated travel arranger also has access to the traveler's TAVS, profile, and/or reservation data, when given the proper permissions. In general, access to data is given on a need-to-know basis. The agency will determine the access level based on this need-to-know. The approver will have access to some data but not all data, and this right to use/see specific data will be determined by the agency's policies and procedures and the access control permission granted to see the appropriate information.
4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?	Procedural controls at the Agency level must be used to ensure that data is appropriately protected commensurate with its sensitivity. Application of these local polices and procedures will minimize that risk that users at a site can read, copy, alter, or steal printed or electronic information for which they are not authorized; and ensure that only authorized user's pick-up, receive, or deliver input and output information and media. Warning banners are displayed at login to all users to warn them that the FedTraveler.com system is For Official Use Only and that it contains information the Privacy Act of 1974 covers. These warning banners must be acknowledged by the user prior to the user being granted system access, and advise users of their obligations to protect the system and data it contains in accordance with Federal Policy. In addition, all personnel must read and acknowledge the Rules of Behavior prior to being granted access to the system. Warning individuals with appropriate access about the misuse of data will be accomplished through policy and by the distribution and acceptance of the Rules of Behavior to users. In addition, there are technology controls, such as auditing, in place which will reveal the misuse of data in a

	timely manner. The administrator allows access control on a need-to-know basis. These are periodically reviewed and updated. Logs are audited for inappropriate or unauthorized activity. Obligation and payment data may be changed only by authorized users, i.e., the traveler, travel arranger, System Administrator, or TAVS approving officials. Credit card numbers that are stored in the profiles cannot be viewed-the numbers are masked (X'd) out except for the last four digits. Social Security Numbers are masked except for the last four digits. Obligation and payment data may be changed only by authorized users, i.e., the traveler, travel arranger, System Administrator, or TAVS approving officials. Auditing controls are required as part of the ETS.
5.a. Do other systems share data or have access to data in this system? If yes, explain.	Federal agency accounting systems can interface with the TAVS component of ETS for proper recording of obligations when travel authorizations are approved, and for recording expenses when voucher payments are made. (Data will be passed between systems. The agency accounting systems will not have direct access to ETS databases.) The Travel Management Center (TMC) will have access to the profile and reservation data input by the traveler. This access is necessary for the TMC to complete reservation and ticketing actions. The on-line booking engine directs reservations to the TMC for fulfillment, i.e., ticketing for transportation and confirmation of hotel and/or car reservations. The reservation systems, or Global Distribution Systems (GDS), provide the link between the on-line booking engine and the TMC.
5.b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface?	The EDS Program Manager is responsible for ensuring that the access controls are in place within the system. The agency is responsible for assuring that the data is properly used. The agency should have Policies in place which are enforced and protect the data against misuses, and each user should be given and sign the "The Rules of Behavior". The TMC Master Contracts include FAR 52.224-2, Privacy Act Notification (APR 1984) and FAR 52.224-2, Privacy Act (APR 1984)

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	An agency will neither share data nor have free access to another agency's data in ETS but data may be provided to other agencies in accordance with the "*Routine uses of records*…" section in System of Records, Contracted Travel Services program: GSA/GOVT-4
6.b. How will the data be used by the agency?	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: a. 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. b. To another Federal agency or a court when the Federal government is party to a judicial proceeding. c. To a Member of Congress or staff on behalf and at the requests of the individual who is the subject of the record. d. 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. e. To a credit card company for billing purposes, including collection of past due amounts. f. 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. g. 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. h. 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. i. 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. j. 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. k. 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. l. To a travel services provider for billing and refund purposes. m. 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. n. 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. o. 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 purposes.
6.c. Who is responsible for assuring proper use of the data?	The EDS Program Manager has responsibility for assuring the access controls are in place within the FedTraveler.com.com system. Agency management and Agency-wide System Administrators are responsible for assuring proper use of the date within the agency.

	Security and auditing controls will be implemented to prevent or identify unauthorized access to data.
6.d. How will the system ensure that agencies only get the information they are entitled to?	All user sessions between the user's workstation and FedTraveler.com.com web server are encrypted using FIPS-compliant encrypted connection. The agencies are logically separated within the ETS. There is no access between agency systems. FedTraveler.com uses a multi-tiered architecture to provide isolation between the various network ties. Only authorized connections are allowed to and between the various tiers. System login, passwords, and FIPS-compliant encrypted connection are in place to protect the data and prevent unauthorized access. Security controls will be placed on the data to allow "need-to-know" access only. To initiate any travel process, travelers access the on-line system via the Internet and login using an agency name, login name, and user-defined password. They will be required to be authenticated to the system via an accepted authentication mechanism. With a valid login, the system presents travelers with a menu of options, which System Administrators customize according to agency policies, the traveler's level of expertise, job position, and/or travel grouping. In addition, an IV&V was performed to test access and ensure that data was not accessed by anyone other than the one who had access based on the ETS roles. Other agencies may obtain data from the system only submitting a request for specific information to the agency which "owns' the data.
7. What is the life expectancy of the data?	The data will be used, processed and then stored. Data will be stored for six years three months; this is specified by the National Archives and Records Administration (NARA) and in the vendor contracts. The EDS contract stipulates: "The ETS should provide online access to detailed transaction information for a minimum period of 36 months, and permit access to archived detailed transaction information for a period of 6 years and 3 months. NARA guidelines regarding records disposition are to be followed. As specified in the contract "The ETS shall prevent the purging of historical records prior to the proper retention period, and permit purging only of those records authorized for disposal by the National Archives and

	Records Administration (NARA) per 36 CFR 1228 and 1234. NARA General Records Schedule 9 for Travel and Transportation Records and General Records Schedule 20 for Electronic Records shall apply."
8. How will the data be disposed of when it is no longer needed?	Sensitive FedTraveler.com information will be properly disposed of when no longer needed. Hard copy materials will be shredded using shredders located in office areas or placed in locked sensitive waste disposal bins for collection and destruction by EDS Security. Electronic media will be securely overwritten (at least six passes) or degaussed, or turned into EDS Security for destruction in accordance with applicable government requirements. Appropriate audit trails/logs are maintained to record the receipt or disposition of sensitive media or hardcopy information. NARA guidelines regarding records disposition are to be followed. These guidelines are specified in their contract and states that "The ETS shall prevent the purging of historical records prior to the proper retention period, and permit purging only of those records authorized for disposal by the National Archives and Records Administration (NARA) per 36 CFR 1228 and 1234. NARA General Records Schedule 9 for Travel and Transportation Records and General Records Schedule 20 for Electronic Records shall apply."

C. Attributes of the Data

Question	Response
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes. The individual traveler's profile data is needed to accurately reserve and ticket travel, and to have expenses charged to the proper travel charge card account. The reservation data is needed to accomplish the required travel, and to estimate trip costs for authorization purposes. The TAVS data are required to properly record the obligation of funds, to accurately calculate and accomplish reimbursement of the traveler and/or payment to the travel card vendor and to liquidate the obligation when payment is made.
2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No
2.b. Will the new data be placed in the individual's record (client or employee)?	No
2.c. Can the system make determinations about individuals that would not be possible without the new data?	No. This type of analysis is not done within the system.
2.d. How will the new data be verified for relevance and accuracy?	Not Applicable
3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	Some consolidation may be done. Data may be consolidated, if there are multiple travel programs existing within an agency before its migration to ETS. Reports generated of aggregate activity may be accessed only by agency management and System Administrators. Such reports do not contain information on or impact individual authorization or payment records, profiles, or reservations in the system. As the system interfaces with agency financial systems, information regarding invoices and reimbursement will

	be red to the appropriate systems. They act as feeder systems and no direct user interface is applicable. A Federal Agency post-migration may consolidate data for reporting purposes either internally to the agency or to GSA and/or OMB.
3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Consolidation of the authorization, reservation, and payment processes in the system does not negate any of the access controls. Total system access has the same limited access and security protections of each of its components.
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Travel data may be retrieved by personal identifier. The approver will retrieve data based on traveler name. Reports may be run based on 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, with retrieval limited to the individuals who may input the data elements, except that agency travel managers and the System Administrator may also access data in the system.
5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; c. Accelerated information processing and decision making; and d. Use of new technologies. How are the effects to be mitigated?	The potential effects on the privacy rights of employees include: a. Connectivity to agency back office systems (e.g. Human Resources and Financial). b. There is no derivation of data. c. There is decision making based on the Federal Travel Regulations and agency business rules. d. The ETS will facilitate and expedite the authorization, arranging, and payment of travel within a secure electronic environment. Personal information may be revealed due to this new technology (e.g. faxing of receipts). Travelers who cannot make on-line reservations may continue to call the TMC for reservations. Separate authorization and payment processes may be required in such cases. Some privacy information such as the

	social security number is masked so that the entire number is not displayed. Other information is likewise masked so that the entire number is not displayed.

D. Maintenance of Administrative Controls

Question	Response
1.a. Explain how the system and its use will ensure equitable treatment of individuals.	The ETS provides an electronic means for Federal travelers to accomplish their travel needs. All agency restrictions and controls apply to every user of the system.
1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	This is a web-based system. The system is operated in only one site. Users will be geographically separated, accessing the system via a web browser over the "Internet".
1.c. Explain any possibility of disparate treatment of individuals or groups.	Travelers who do not have access to the Internet or access to ETS, must call the TMC for reservations, and may be required to use a different authorization and vouchering process.
2.a. What are the retention periods of data in this system?	The data will be used, processed, and then stored. Data will be stored for six years three months; this is specified by NARA and in the vendor's contract. The EDS contract stipulates "The ETS should provide online access to detailed transaction information for a minimum period of 36 months, and permit access to archived detailed transaction information for a period of 6 years and 3 months." The TAVS data are maintained in accordance with the General Records Retention Schedules issued by the National Archives and Records Administration. Traveler profile data may be updated by the traveler, the TMC, or the System Administrator as needed. The profile is maintained as long as the individual travels, or may travel, at Government expense. The on-line booking engine database holds post-travel data for reporting purposes for 90 days.
2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Sensitive FedTravler.com information will be properly disposed of when no longer needed. Hard copy materials will be shredded using shredders located in office areas or placed in locked sensitive waste disposal bins for EDS Security collection and

	destruction. Electronic media will be securely overwritten (at least six passes) or degaussed, or turned in to EDS Security for destruction in accordance with applicable government requirements. TAVS data that exist only in electronic form are to be permanently deleted at the end of the prescribed records retention period. Hard copy data are to be destroyed at that time. NARA guidelines regarding records disposition are to be followed. As specified in the contract, "The ETS shall prevent the purging of historical records prior to the proper retention period, and permit purging only of those records authorized for disposal by the National Archives and Records Administration (NARA) per 36 CFR 1228 and 1234. NARA General Records Schedule 9 for Travel and Transportation Records and General Records Schedule 20 for Electronic Records shall apply."
2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Traveler initiated changes may occur, for example, because a different bank account is desired for EFT reimbursement. Financial systems may make updates to all travelers' files periodically to assure timely and accurate payment. Profile data elements are as accurate as the traveler keeps them. Trip data is as accurate as the last "refreshed" version the on-line booking engine saw of the Passenger Naming Record (PNR).
3.a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)?	No. The Internet access is similar to that already in use for the Thrift Savings Plan (TSP) and Employee Express.
3.b. How does the use of this technology affect individuals' privacy?	The ETS has no independent impact on Federal traveler privacy. Some of the data entered into the system is already collected and maintained by travel agencies under contract to the Government, and some are currently maintained by authorization and voucher payment systems of agencies.

4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	Yes. Federal agency travel managers, System Administrators, and the TMC may view a group of individuals' reservations before, during and after travel. However, deviations from reservations outside the ETS will not be known or detectable from the system. For example, if a traveler changes flights at an airport counter, the changes will not be reflected in ETS.
4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	Yes. Federal agency travel managers, System Administrators, and the TMC may view a group of individuals' reservations before, during and after travel. However, deviations from reservations outside the ETS will not be known or detectable from the system. For example, if a traveler changes flights at an airport counter, the change will not be reflected in ETS.
4.c. What controls will be used to prevent unauthorized monitoring?	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.
5.a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name.	General Services Administration, System of Records under the Privacy Act of 1974, contracted Travel Services program: GSA/GOVT-4.
5.b. If the system is being modified, will the SOR require amendment or revision? Explain.	The subject SOR (GSA/GOVT-4) will be modified to include provision of data to the ETS as another routine use of traveler data. The SOR may also need to be modified if agencies determine that the E-Travel SOR does not cover specifics covered under their travel SOR. The SOR already identifies the majority of the data and uses the ETS holds. The ETS is another medium for accessing the data.