Privacy Impact Assessment (PIA) for the

Carlson Wagonlit Government Travel, Inc., d.b.a. CWTSatoTravel

E2 Solutions TAVS

January 11, 2018

Contact Point
Roy M. Smith II
CWTSatoTravel
202-262-0368

Abstract
CW Government Travel, Inc., d.b.a as CWTSatoTravel, in accordance with the General Service Administration E-Gov Travel Master Contract (ETS2), provides an end-to-end travel authorization and voucher system (TAVS) which includes travel fulfillment called E2 Solutions for) servicing civilian federal employees. E2 Solutions system was developed to support the E-Gov initiative and contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). The information requested in E2 Solutions is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code for the purpose of recording travel information provided by the user to create travel itineraries, reserve any method or mode of travel accommodations, and claim entitlements and allowances prescribed in applicable Federal travel regulations.

Overview
The E-Gov Travel Service (ETS2) is a government wide, web-based, world-class travel management service. This streamlined service continually applies commercial best practices to realize travel efficiencies and deliver a transparent, accountable, and sustainable service that yields exceptional customer satisfaction sponsored by the U.S. General Services Administration Program Management Office (GSA PMO). CWTSatoTravel is the corporate contracting entity within Carlson Wagonlit Travel (CWT) responsible for soliciting and managing travel for the U.S. military and government clients. CWTSatoTravel's E2 Solutions is a web-based, end-to-end travel management system to plan, authorize, arrange, process, and manage official federal travel. E2 Solutions 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.

The Privacy Act statement for E2 Solutions is configured at the application level, and available from all pages in the E2 Solutions application. The information requested in E2 Solutions is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code for the purpose of recording travel information provided by the user to create travel itineraries, reserve any method or mode of travel accommodations, and claim entitlements and allowances prescribed in applicable Federal travel regulations. The purpose of the collection of this information is to establish a comprehensive travel services system which enables travel service providers under contract with the Federal Government to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal Government business.

Sensitive E2 Solutions 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 authorized personnel for collection and destruction. Electronic media will be securely overwritten (at least six passes) or degaussed, or turned in to CWTSatoTravel 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. There is a situation in which trips/data are deleted from the active database, however, this information will be stored in the archival files: A user that has no system activity.
NARA guidelines regarding records disposition are to be followed. As specified in the contract, "ETS2 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".

An agency will neither share data nor have free access to another agency's data in E2 Solutions TAVS 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, "Contracted Travel Services Program."

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the application in question?

GSA collects, maintains, and uses personal information on individuals to carry out the agency's mission and responsibilities, and to provide services to the public. By federal law and regulation, privacy issues and protections must be considered for information technology systems that contain any personally identifiable information. GSA uses the Privacy Impact Assessment (PIA) as a key tool in fulfilling these legal and regulatory obligations. By conducting PIAs, GSA ensures that:

- The information collected is used only for the intended purpose;
- The information is timely and accurate;
- The information is protected according to applicable laws and regulations while in GSA's possession;
- The impact of the information systems on individual privacy is fully addressed; and

The public is aware of the information GSA collects and how the information is use

The GSA Privacy Program (ID) is responsible for determining and documenting the legal authority permitting the handling of GSA "personally identifiable information" (PII). Pursuant to 5 U.S.C. §552a (e) (3), GSA provides what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records [i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security Number (SSN)]. GSA policy is to provide a Privacy Act Statement regardless of whether the collection is part of a system of

records or not. All Privacy Act statements must be reviewed by the GSA Privacy Office. When drafting a Privacy Act Statement for review by the GSA Privacy Office, the legal authority for collecting the information (statute, executive order, regulation, etc.) is included.

In accordance with the ETS2 Master Contract, CWTSatoTravel ensures data privacy and protection, safeguarding all user data in full compliance with the Privacy Act and other provisions protecting sensitive data.

E2 Solutions system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed must be protected from unauthorized disclosure. The information requested in E2 Solutions is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code for the purpose of recording travel information provided by the user to create travel itineraries, reserve any method or mode of travel accommodations, and claim entitlements and allowances prescribed in applicable Federal travel regulations.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

GSA manages its privacy risk management process by conducting PIAs and SORNs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. Systems are categorized as low, moderate, or high risk in accordance with Federal Information Processing Standard 199 (FIPS 199) and NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. General Services Administration, System of Records under the Privacy Act of 1974: GSA/GOVT-4, "Contracted Travel Services Program."

1.3 Has a System Security Plan (SSP) been completed for the information system(s) supporting the application?

E2 Solutions maintains its Authority to Operate in accordance with the GSA policy governing Assessment and Authorization activities. Supporting the GSA ETS2 Travel Contract Vehicle, the current ATO was granted on July 6th 2017.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

NARA guidelines regarding records disposition are to be followed. As specified in the contract "ETS2 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." 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 CWGT contract stipulates "The ETS2 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."

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not Applicable

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the application collects, uses, disseminates, or maintains.

To use E2 Solutions, a traveler must enter unique identifying information such as user id and password. A user profile is established for each traveler which contains personal information, including organization address, telephone number, travel preferences, frequent flyer and rental car club account numbers, passport information, emergency contract name, alternative address and telephone number, personal credit card number (official travel charge care account at a minimum), date of birth, gender, redress number, known traveler number, and other information as required by the agency's Travel Authorization and Voucher System , Travel Management Center (TMC), and transportation providers for making reservations and issuing tickets.

Information gathered includes Traveler Profile data, Name, SSN (if applicable by agency requirements), 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; date of birth; gender; redress number; known traveler number; and individual charges and balances. In addition, other passport information (i.e. issuing country, expiration date), and emergency contact information are included.

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.

Federal agency accounting systems will interface with the E2 Solutions component 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 E2 Solutions 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 (e.g. in order to email the traveler her itinerary). The TMC does not have access to E2 Solutions..

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.

GDSX, the interface between the GDS and E2 Solutions provides updates to the traveler's reservations if modifications are made. This is an interface which data securely traverses between E2 Solutions and the GDS to maintain the integrity of the travelers' reservations.

2.2 What are the sources of the information and how is the information collected for the application?

Federal agencies with task orders issued under GSA's ETS2 Master Contract for ETS2 provide data for users 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, an agency's 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, entered on behalf of the user, or comes programmatically from another system.

There may be initial uploads and periodic updates of data from financial and HR systems of participating Federal agencies Other possible sources are the Travel Management Centers

(TMC) on-line booking, and the Global Distribution System (GDS) which provides hotels, car rental, and airlines information.

2.3 Does the application use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Not applicable

2.4 Discuss how accuracy of the data is ensured.

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 travel arranger's responsibility to assure the data is complete; else payment will likely not be accomplished.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Principal of Purpose Specification: E-Gov Travel Service (ETS2) is a web-based, end-to-end travel management system to plan, authorize, arrange, process, and manage official Federal travel. E2 Solutions 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.

GSA collects, maintains, and uses personal information on individuals to carry out the agency's mission and responsibilities, and to provide services to the public. By federal law and regulation, privacy issues and protections must be considered for information technology systems that contain any personally identifiable information. GSA uses the Privacy Impact Assessment (PIA) as a key tool in fulfilling these legal and regulatory obligations. By conducting PIAs, GSA ensures that:

- The information collected is used only for the intended purpose;
- The information is timely and accurate;
- The information is protected according to applicable laws and regulations while in GSA's possession;
- The impact of the information systems on individual privacy is fully addressed; and
- The public is aware of the information GSA collects and how the information is used.

Principle of Minimization: Federal agencies 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.

Collection of PII is required for E2 Solutions application in support of the ETS2 master contract. 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. Sensitive E2 Solutions 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 appropriate and authorized CWTSatoTravel and/or CWT personnel. Electronic media will be securely overwritten (at least six passes) or degaussed, or turned into CWTSatoTravel 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 "ETS2 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."

Principle of Individual Participation: In order to properly provide travel services to our customers and their travelers, CWTSatoTravel creates an electronic 'Traveler Profile' for each traveler. The personal data is entered through feeds from the customer's systems or by the traveler (or the authorized travel arranger). The personal data that we collect for each traveler may include: name, gender, date of birth, address, phone numbers, email addresses, credit card references/numbers, travel destinations, travel schedules, travel preferences (seat, meal, smoking, etc.), passport and visa details, as well as next of kin information. This 'Travel Profile' may be stored in the Global Distribution System used to make reservation or in the online booking tool

service provider used to provide online reservations. CWTSatoTravel collects personal data from users to its web sites through the use of online forms and when the user emails us his/her details. CWTSatoTravel forwards these user requests to the appropriate CWTSatoTravel team to respond to the user. CWTSatoTravel keeps personal data only as long as required to fulfill the services requested by the customers and/or in accordance with the appropriate data retention periods specified in the contract or in accordance with applicable retention periods specified in the Federal Acquisition Regulations.

Principle of Data Quality and Integrity: Accuracy of the data is maintained by the traveler or travel arranger to 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 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.

Privacy Risk: Access controls within E2 Solutions limit the functions and data available to a given user based on need-to-know and job responsibilities. The potential for sensitive data to be viewed, modified, or deleted by unauthorized personnel is minimized.

Mitigation: 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.

Designated Agency-wide System Administrators will have access for the purpose of adding or deleting users, resetting passwords, setting up individuals as travel arrangers to make travel reservations on another individual's behalf, or changing group profiles.

Procedural controls at the Agency level must be used to ensure that data is appropriately protected commensurate with its sensitivity. Application of these local policies 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 E2 Solutions 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 advice 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.

Section 3.0 Uses of the Information

The following questions require a clear description of the application's use of information.

3.1 Describe how and why the application uses the information.

Collection of PII is required for E2 Solutions application in support of the ETS2 master contract. 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 is 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.

3.2 Does the application use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how GSA plans to use such results.

Not applicable

3.3 Are there other components with assigned roles and responsibilities within the system?

ETS2 data is protected by the Privacy Act of 1974. Any disclosure of collected information to third parties is identified in the System of Record Notice (SORN) as published in the Federal Registry. The nature of the travel reservations business warrants that collected information be shared with multiple parties (i.e., airlines, auto-rental companies, etc.) to facilitate the end-to-end travel process. The CWTSatoTravel E2 Solutions information system is in complete compliance with the provisions of the Privacy Act. Compliance includes the displaying of all required warning banners; custom messages can be displayed at agency or government request per the E2 Solutions configurable message center.

An agency will neither share data nor have free access to another agency's data in E2 Solutions TAVS but data may be provided to other agencies in accordance with the "*Routine uses of records*…" section in System of Records, GSA/GOVT-4 "Contracted Travel Services."

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Procedural controls at the Agency level must be used to ensure that data is appropriately protected commensurate with its sensitivity.

Mitigation: Warning banners are displayed at login to all users to warn them that the E2 Solutions TAVS system is For Official Use Only and that it contains information the Privacy Act of 1974 covers. These warning banners must advise users of their obligations to protect the system and data it contains in accordance with Federal policy and must be acknowledged by the user prior to the user being granted system access. 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 System Administrator allows access on a need-to-know basis. The access lists are periodically reviewed and updated. Logs are audited for inappropriate or unauthorized activity.

Section 4.0 Notice

The following questions seek information about the application's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the application provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The information requested in E2 Solutions is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code for the purpose of recording travel information provided by the user to create travel itineraries, reserve any method or mode of travel accommodations, and claim entitlements and allowances prescribed in applicable Federal travel regulations. The purpose of the collection of this information is to establish a comprehensive travel services system which enables travel service providers under contract with the Federal Government to authorize, issue, and account for travel and travel reimbursements provided to individuals on

official Federal Government business. Routine uses which may be made of the collected information and other financial account information in the system(s) of record entitled "Contracted Travel Services Program GSA/GOVT-4". The full privacy act statement can be reviewed for E2 Solutions at https://e2.gov.cwtsatotravel.com

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the application?

ETS2 provides an electronic means for Federal travelers to accomplish their travel needs. All agency restrictions and controls apply to every user of the system. .ETS2 enables the government to further consolidate travel services, platforms, and channels, improves the leverage of government travel spending, increases transparency for improved accountability, and reduces waste. This directly aligns and supports the Office of Management and Budget Memo M-12-12 regarding *Promoting Efficient Spending to Support Agency Operations* with respect to travel. E2 Solutions TAVS provides an electronic means for Federal agencies and its travelers to accomplish their travel needs. Based on an agency mission and policy, use of the online TAVS application may not be acceptable for travelers to use. 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.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Travelers may not be aware of why the system is collecting their information and how it is being used and disseminated.

Mitigation: CWTSatoTravel adheres to privacy notice requirements per the ETS2 Master Contract citing contractor responsibilities. ETS2 data is protected by the Privacy Act of 1974. Any disclosure of collected information to third parties is identified in the System of Record Notice (SORN) as published in the Federal Registry. The nature of the travel reservations business warrants that collected information be shared with multiple parties (i.e., airlines, auto-rental companies, etc.) to facilitate the end-to-end travel process. The CWTSatoTravel E2 Solutions information system is designed to comply with the provisions of the Privacy Act. Compliance includes the displaying of all required warning banners; custom messages can be displayed at agency or government request per the E2 Solutions configurable message center.

Section 5.0 Data Retention by the application

The following questions are intended to outline how long the application retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

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. NARA guidelines regarding records disposition are to be followed. As specified in the contract, "ETS2 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. The contract stipulates "ETS2 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 is 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 GDS and PNR hold post-travel data for reporting purposes for 90 days.

5.2 Privacy Impact Analysis: Related to Retention

Principle of Minimization, Data Quality and Integrity: E2 Solutions information will be properly disposed of when no longer needed, however, retention/destruction must be in compliance with ETS2 master contract requirements. ETS2 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.

Privacy Risk: Collection of PII is required for E2 Solutions application in support of the ETS2 master contract.

Mitigation: 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 is 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. Sensitive E2 Solutions 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 appropriate and authorized CWTSatoTravel and/or CWT personnel. Electronic media will be securely overwritten (at least six passes) or degaussed, or turned into CWTSatoTravel 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 "ETS2 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.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the application information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of GSA as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

An agency will neither share data nor have free access to another agency's data in E2 Solutions 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.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

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.
p. To the National Archives and Records Administration (NARA) for record management.

6.3 Does the application place limitations on re-dissemination?

An agency will neither share data nor have free access to another agency's data in E2 Solutions TAVS 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.

6.4 Describe how the application maintains a record of any disclosures outside of the Agency.

CWT/CWTSatoTravel has implemented appropriate technical and organizational measures to protect the personal information obtained from clients' travelers against accidental or unlawful disclosure or destruction. E2 Solutions keeps personal information only as long as required to fulfill the services requested by its clients. CWTSatoTravel may need to keep certain information to comply with financial reporting laws or to inquiries from clients on past travel activities. CWTSatoTravel may be required by law to transfer information to governments and law enforcement agencies where required. CWTSatoTravel is required to adhere to applicable security requirements in those contracts and agreement with respect to the safeguarding of, access to, and processing of, any travel or traveler data. These security requirements may include the Privacy Act and/or adherence to data protection for information management systems in accordance with guidance issued by the National Institute of Standards & Technology or by the U.S. Office of Management & Budget, or specific agencies.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Can a traveler access another traveler's data? Can travel arrangers gain access all travelers' information?

Mitigation: E2 Solutions has no independent impact on Federal traveler privacy. Some of the data entered into the system by travel agencies under contract to the Government already collect and maintain, and some are currently maintained by authorization and voucher payment systems of agencies. Individuals are given various levels of access to the system. Only agency travel managers, the System Administrator(s), and the TMC through the GDS may access others' records in a manner that constitutes monitoring. In addition, there are policies in place such as the Rules of Behavior which help to prevent unauthorized monitoring.

CWTSatoTravel through ETS2 adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. The traveler has a right of access to his/her personal data. Access controls within the E2 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.

CWTSatoTravel Account and Security personnel jointly develop draft MOU, ISA and IA documents based on GSA ETS2 Master Contract requirements and agency input; these draft documents are then provided to the agency for review. In conjunction with the appropriate agency POCs, we verify that all required information is recorded prior to forwarding the documentation to GSA for approval.

The E2 Solutions Information System Security Officer (ISSO) has responsibility for assuring the access controls are in place within the E2 Solutions system through continuous monitoring activates. Agency management and Agency-wide System Administrators are responsible for assuring proper use of the data within the agency. Security and auditing controls are implemented to prevent or identify unauthorized access to data. Individuals are given various levels of access to the system. Only agency travel managers, the System Administrator, and the TMC through the GDS 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. Continuous monitoring and A&A activities are required to ensure continuity of operations is maintained across E2 Solution components.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Access controls within the E2 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.

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.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Traveler 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 Name Record (PNR). Accuracy of the data is maintained by the traveler or travel arranger to 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.

7.3 How does the application **notify individuals about the procedures for correcting their information?**

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 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 in E2 Solutions.

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's name as associated with his or her agency's business system is stored within the E2 Solutions profile, with a variety of other configurable permissions and settings associated with the user (including the traveler's ETS2 user ID). If the traveler's name changes, a system administrator or other user with the appropriate permissions can update that name in the appropriate record. Travelers may store and update an alternate name for reservation purposes to comply with security requirements. Any updates of the name used for reservations will be applied to subsequent reservations. Traveler name changes, whether associated to the agency's business system or for reservation purposes, do not require a change to the traveler's ETS2 user ID. The profile and reservation data will only be available to the servicing TMC on a need-to-know basis. The Travel Management Center (TMC) will have access to the profile and reservation data input by the traveler and can provide support to address corrections if required to traveler's inquiries. This access is necessary for the TMC to complete reservation and ticketing actions. The TMC does not have access to E2 Solutions.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: E2 Solutions TAVS has no independent impact on Federal traveler privacy. Some of the data entered into the system travel agencies under contract to the Government already collect and maintain, and some are currently maintained by authorization and voucher payment systems of agencies. Individuals are given various levels of access to the system. Only agency travel managers, the System Administrator, and the TMC through the GDS 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.

Mitigation: Accuracy of the data is maintained by the traveler or travel arranger to 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. Additionally, 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.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the application ensure that the information is used in accordance with stated practices in this PIA?

The CWTSatoTravel ISSO is the principal point of contact for information assurance activities for ETS2 for ensuring that management, operational, and technical controls for securing CUI are in place and are followed. This includes ensuring that appropriate steps are taken to implement information security requirements, including conducting the Privacy Impact Assessment (PIA) for the ETS2 information systems throughout their life cycle, from the requirements definition phase through disposal. Ensuring ETS2 information systems and the data each system processes have necessary security controls in place and are operating as intended and protected in accordance with GSA regulations, policies and standards. . E2 Solutions maintains continuous monitoring through annual FISMA compliance reviews and quarterly activity to assess security strengths and weaknesses. Plan of Action and Milestone (POA&M) Reports are developed to monitor privacy controls and internal privacy policy to ensure effective implementation. E2 Solutions is a FIPS 199 Moderate baseline, required contractually to maintain Authority to Operate (ATO).

CWT performs periodic internal and external audits on major client-facing products and services. These audits review compliance with information security and privacy policies, the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standard (PCI DSS) requirements. Any deficiencies that might be identified are recorded and escalated to the appropriate teams and management. Remediation plans are initiated and monitored to ensure progress.

Security and auditing controls are implemented to prevent or identify unauthorized access to data. Proactive monitoring of CWT client facing products, including E2 Solution is in place utilizing industry recognized logging/monitoring tools (e.g. Splunk, McAfee SIEM, Solarwinds, Gomez, ServiceNow). These tools provide a breadth of monitoring activity and are configured to send alerts for incident management.

Agency management and Agency-wide System Administrators are responsible for assuring proper use of the data within the agency.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the application?

CWTSatoTravel adheres to CWT's standard and policies on security and protection of data. CWT policies, standards and standard specifications are available on-line to employees. CWT provides annual Information Security training and awareness program developed using CWT Information Security global policies and standards, and what is expected from each employee/contractor. CWT Information Security/Data Privacy global policies and standards are communicated at time of hire and reiterated annually via required global Information Security/Data Privacy training programs to provide the purpose and use of sensitive information.

Procedural controls at the Agency level must be used to ensure that data is appropriately protected commensurate with its sensitivity. Warning banners are displayed at login to all users to warn them that the E2 Solutions TAVS 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 advice 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.

8.3 What procedures are in place to determine which users may access the information and how does the application determines who has access?

E2 Solutions provides an electronic means for Federal travelers to accomplish their travel needs. All agency restrictions and controls apply to every user of the system. Only authorized agency users will have access to the information system. A user profile is established for each traveler and each user must have a unique ID and password combination to access their travel information. Access controls within the E2 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.

8.4 How does the application review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within GSA and outside?

CWTSatoTravel Account and Security personnel jointly develop draft MOU, ISA and IA documents based on the ETS2 Master Contract requirements and agency input; these draft documents are then provided to the agency for review. In conjunction with the appropriate agency POCs, we verify that all required information is recorded prior to forwarding the documentation to GSA for approval.