



# **E2 Solutions Travel and Authorization Voucher System**

*Privacy Impact Assessment*

November 5, 2019

**POINT of CONTACT**

**Richard Speidel**

*Chief Privacy Officer*  
GSA IT  
1800 F Street NW  
Washington, DC 20405

## **Instructions for GSA employees and contractors:**

This template is designed to assist GSA employees and contractors in complying with the [E-Government Act of 2002, Section 208](#), which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with [1878.2A CIO P - Conducting Privacy Impact Assessments](#); is designed to align with GSA businesses processes; and can cover all of the systems, applications or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers and Developers as they assess potential privacy risks during the [early stages of development and throughout the system, application or project's life cycle](#). The completed PIA demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are made available to the public at [gsa.gov/privacy](http://gsa.gov/privacy) (<https://www.gsa.gov/portal/content/102237>).

Each section of the template begins with a statement of GSA's commitment to the [Fair Information Practice Principles \("FIPPs"\)](#), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. For example:

This document contains important details about E2 Solutions TAVS. *GSA office* may, in the course of ETS2, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:

<https://www.gsa.gov/portal/getMediaData?mediaId=167954>

**Please send any completed PIAs or questions to [gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov).**

# Stakeholders

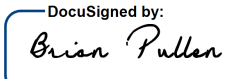
Name & Email of Information System Security Manager (ISSM):

- Brian Pullen
- [brian.pullen@gsa.gov](mailto:brian.pullen@gsa.gov)

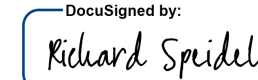
Name & Email of Program Manager/System Owner:

- Bob McCauley
- [bmccauley@cwtsatotravel.com](mailto:bmccauley@cwtsatotravel.com)

# Signature Page

X   
21CA83CF4EB94DA...  
Brian Pullen  
ISSM

X   
4FA31362FD6E4CC...  
Bob McCauley  
E2 Solutions System Owner/Program Manager

X   
171D6414183F40A...  
Richard Speidel  
Chief Privacy Officer

## Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third party services and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding “Information Collection Requests”	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard’s email address	2.3
<b>11/28/2018</b>	<b>Added new Stakeholders section to streamline process when seeking signatures &amp; specified that completed PIAs should be sent to <a href="mailto:gsa.privacyact@gsa.gov">gsa.privacyact@gsa.gov</a></b>	<b>2.4</b>

# Table of contents

## SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 Why is GSA collecting the information?
- 1.2 What legal authority and/or agreements allow GSA to collect the information?
- 1.3 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 1.4 Has any information collection request (ICR) been submitted to or approved by OMB? If yes, provide the relevant names, OMB control numbers, and expiration dates.
- 1.5 Has a records retention schedule been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.
- 1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

## SECTION 2.0 OPENNESS AND TRANSPARENCY

- 2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about them? If not, please explain.
- 2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

## SECTION 3.0 DATA MINIMIZATION

- 3.1 Whose information is included in the system?
- 3.2 What PII will the system include?
- 3.3 Why is the collection and use of the PII necessary to the project or system?
- 3.4 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.5 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.6 Will the system monitor members of the public, GSA employees or contractors?
- 3.7 What kinds of report(s) can be produced on individuals?
- 3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?
- 3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

## SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

- 4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

## **SECTION 5.0 DATA QUALITY AND INTEGRITY**

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

## **SECTION 6.0 SECURITY**

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

## **SECTION 7.0 INDIVIDUAL PARTICIPATION**

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

## **SECTION 8.0 AWARENESS AND TRAINING**

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

## **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

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

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

## Document purpose

E2 Solutions is the end-to-end travel and expense management tool that provides a convenient, user-friendly way to manage all aspects of travel for organizations that follow federal travel regulations. Create and track travel authorizations, book reservations, get approvals, submit expense reports, and receive reimbursements – all in one streamlined system. E2 Solutions is a proven product for travel program managers who want to effectively track compliance, manage costs, integrate with core business systems, and provide travelers with a simplified experience.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA’s [privacy policy](#) and [program goals](#). The sections also align to the Fair Information Practice Principles (“FIPPs”), a set of eight precepts that are codified in the Privacy Act of 1974.<sup>[2]</sup>

## System, Application or Project

*E2 Solutions Travel and Authorization and Voucher System (TAVS)*

## System, application or project includes information about

*Federal agency employee travel details.*

## System, application or project includes

- Customer Travel details

### 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 EGov 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 travel management service. This streamlined service delivers a transparent and accountable service 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 (<https://e2.gov.cwtsatotravel.com>) 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. If there is a situation in which trips/data are deleted from the active database, this information will be stored in the archival files. A user that has no system activity then the National Archives and Records Administration ("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 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 PURPOSE OF COLLECTION

*GSA states its purpose and legal authority before collecting PII.*

## 1.1 Why is GSA collecting the information?

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.

## 1.2 What legal authority and/or agreements allow GSA to collect the information?

The GSA Privacy Program (ID) is responsible for determining and documenting the legal authority permitting the handling of GSA U.S Federal Government “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.

## 1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

E2 Solutions customer’s personal identifier data is searchable within the E2 Solutions TAVS environment based on a need to know. Management of System-level accounts used by CWTSatoTravel support personnel is strictly controlled on a need-to-know basis and uses the principle of least privilege. System-level accounts are created and assigned only after management approval. The agency will determine the access level based on this need-to-know.

The agency 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.

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.

**1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.**

No ICR request has been submitted to OMB. National Archives and Records Administration (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 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 CWTSatoTravel 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. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.**

National Archives and Records Administration (NARA) guidelines regarding records disposition has been approved for ETS2 and should 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 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 CWTSatoTravel 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."

## **1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?**

Privacy Risk: There are privacy risks to the collection of personal data, but the potential for sensitive data to be viewed, modified, or deleted by unauthorized personnel is minimal. Access controls within E2 Solutions limit the functions and data available to a given user based on need-to-know and job responsibilities.

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 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.

## **SECTION 2.0 OPENNESS AND TRANSPARENCY**

*GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.*

### **2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.**

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>

## 2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

There are no known Privacy risk for E2 Solutions TAVS system.

## SECTION 3.0 DATA MINIMIZATION

*GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.*

### 3.1 Whose information is included in the system, application or project?

E2 Solutions TAVS Profile information and GetThere Online Booking Tool information.

#### Reference details:

**Online Booking Engines (GetThere).** Provides the capability for E2 Solutions TAVS users to book air, car, and hotels as part of their designated travel. Multiple booking engines can be supported to meet broad customer requirements and demand.

### 3.2 What PII will the system, application or project include?

As a travel & expense provider, E2 Solutions must store and transmit pertinent information on a traveler to complete the travel planning and reimbursement processes. This information can include traveler name, telephone numbers, address, credit card information, passport numbers, travel plans and frequent flyer numbers.

E2 Solutions Profile	GetThere Online Booking Tool
<ul style="list-style-type: none"> <li>● Name (first, last, middle, suffix, title)</li> <li>● Position Title (optional)</li> <li>● Employee ID or SSN</li> <li>● Homesite Location</li> <li>● Address Information</li> <li>● Phone Numbers</li> <li>● Email Information</li> <li>● Credit Card Information</li> </ul>	<ul style="list-style-type: none"> <li>● Name (first, last, middle, suffix, title)</li> <li>● Position Title (optional)</li> <li>● Address Information</li> <li>● Phone Numbers</li> <li>● Email Information</li> <li>● TSA Information (gender, date of birth, redress, known traveler number)</li> <li>● Emergency contact information (optional)</li> </ul>

E2 Solutions Profile	GetThere Online Booking Tool
<ul style="list-style-type: none"> <li>• Banking Data (per agency)</li> <li>• Travel Profile ID</li> <li>• Emergency Contact Information (optional)</li> </ul>	<ul style="list-style-type: none"> <li>• Traveler preference; frequency program numbers (optional)</li> <li>• Credit Card Information</li> <li>• Passport (optional)</li> <li>• Travel Visa (optional)</li> </ul>

**3.3 Why is the collection and use of the PII necessary to the system, application or project?**

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.

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.

**3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?**

The E2 Solutions TAVS system does not create or aggregate new data.

**3.5 What protections exist to protect the consolidated data and prevent unauthorized access?**

CWTSatoTravel monitors and scans the networks to detect the presence of unauthorized hardware, software and firmware components. CWTSatoTravel have implemented a highly secure network configuration with managed firewalls and routers. CWTSatoTravel actively monitors intrusion detection and protection systems to detect and secure against unauthorized access attempts. Hardware and software assets must not be removed from on-site facilities without the proper authorization. CCTVs and guards at the data centers and major call centers help deter unauthorized removal.

**3.6 Will the system monitor the public, GSA employees or contractors?**

E2 Solutions TAVS does not monitor members of the public, GSA employees or contractors. CWTSatoTravel only track details as it relates to the traveler's using the end to end system.

**3.7 What kinds of report(s) can be produced on individuals?**

A set of standard reports regarding travel are available to assist our client agencies with all aspects of travel analysis, including analysis of NFS travel. The report function is available to all users; individual reports are available to users based on user role and access level, as designated by the client agency.

Travel Administrators with the appropriate permissions have access to the User Configuration History (HIS002I) report which provides information about configuration changes by change category and configuration setting. This report can be used to monitor or research changes made to user settings, including:

- Specific setting changes
- Values (changed from / to). Traveler PII data is masked on the report.
- Changed by information
- When the change was made

Ad Hoc reporting capabilities are also offered to users with designated permissions. The Ad Hoc reporting domain includes a standard set of traveler information that can be incorporated with data inquiries. Access to information is restricted to the users reporting permissions. Traveler domain data includes; E2 user ID, employee ID, employee name and employee email address.

### **3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?**

E2 Solutions TAVS does not de-identify any data.

### **3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?**

There are no known risk as it relates to data minimization.

## **SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION**

*GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.*

### **4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?**

Yes, the information stored in support of the E2 Solutions TAVS system is limited to the information needed to carry out the collection of data.

#### **4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?**

CWTSatoTravel does not control how GSA shares information in support of its ETS2 Product E2 Solutions TAVS. CWTSatoTravel would not share information with other individuals, state agencies or private sector organizations or other federal agencies unless the sharing with other federal agencies would be limited to exceptions expressed in Executive Order 9397 or in Chapter 57, Title 5 United States Code.

#### **4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?**

E2 Solutions profile data is collected in one of three ways:

1. During the onboarding process, a profile load file is compiled by the contracting Federal Agency to create user profiles in the system.
2. System administrators have the ability to add or updated user profile information. CWTSatoTravel administrators act only on the advice of authorized Federal Agency personnel. Agency Administrators follow their own agency's policies and procedures for adding or updating user information.
3. Federal Agencies may alternately choose to provide a formatted file to E2 Solutions for automated upload and update of user information into the system.

#### **4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?**

Yes, E2 Solutions TAVS system does interact with ETS2 client agency financial systems as documented in the agency Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) documentation.

#### **4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?**

Yes, there are no known Privacy Risk for E2 Solutions TAVS system.

## **SECTION 5.0 DATA QUALITY AND INTEGRITY**

*GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.*

#### **5.1 How will the information collected be verified for accuracy and completeness?**

E2 Solutions employs field validation to ensure the integrity of data entered into the system. Field level validation includes format requirements, field length and alpha/numeric character restrictions. The accuracy of the data content is the responsibility of the agency system administrator.

## **5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?**

There are no known Privacy risk for any individuals who's information is collected in support of the E2 Solutions Application.

## **SECTION 6.0 SECURITY**

*GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

### **6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?**

There are various layers of security controls in place to protect and access data. Policies, standards and standard specifications have been implemented that are designed and aligned with the ISO 27001/2, Payment Card Industry Data Security Standards (PCI DSS) and NIST 800-53 frameworks. Controls for physical / environmental security, access, operations, organization, network, system security (masking, encryption, secure coding practices and vulnerability management), incident response, Disaster Recovery / Business Continuity and compliance add levels of security. A “defense in depth” strategy is employed, applying multiple levels of security controls that ensure the confidentiality, integrity and availability of personal data. These include:

Data Security – personal information is protected in transit outside of CWT networks using secure encryption protocols. E2 Solutions TAVS is developed and maintained per CWT's secure coding standards which are based upon OWASP Top 10.

Comprehensive Access Controls - access to data, applications and systems is granted only once it is approved and based on minimum necessary privilege.

### **6.2 Has GSA completed a system security plan for the information system(s) or application?**

In support of the E2 Solutions TAVS system CWTsatoTravel creates and maintains the System Security Plan.

### **6.3 How will the system or application be secured from a physical, technological, and managerial perspective?**

Physical access to the data centers and corporate offices is monitored using closed circuit TV cameras (CCTV) and perimeter contact alarms. Closed circuit camera feeds terminate at guard positions which are staffed 24 hours per day, 365 days per year, Facilities are monitored real-time through CCTV. CCTV Cameras are located at all perimeter ingress/egress locations, on the generator farm, and loading dock areas. All internal areas leading into secured and protected space within the facility have CCTV cameras at door entrances/exits.



Switch monitors physical access to detect and respond to physical security incidents; In the event incident appropriate CWT/CWTSatoTravel personnel will be contacted. Switch reviews physical access logs on a daily basis; and coordinates results of reviews and investigations with the organization's incident response capability. Switch maintains dedicated support for customers 24 hours per day via the network operations center (NOC). NOC representatives monitor customer inquiries, support issues and incidents on a real-time basis. Issues are documented in the Switch Engineering Response (SEER) ticketing system and tracked to resolution.

Additionally, CWT has multiple levels of controls in place to protect and manage its networks including a secure network management process, implemented security configurations, access controls, managed firewalls and routers, implementation of Intrusion Detection and Intrusion Protection Systems, secured remote access connections, and secured wireless connections. CWT's networks are periodically reviewed against its network security requirements to ensure compliance and to remediate any potential security risks. Security service levels and management requirements for all CWT networks have been identified and are documented in various supporting documentation, standards and processes. Contracts with service providers providing network services also include these requirements. Unnecessary ports and services are removed or disabled.

#### **6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?**

CWT workers are informed to use CWT's incident reporting tool, iRespond, to report security related incidents. CWT clients and vendors should report incidents through the appropriate CWT regional help desk or their CWT Program Management Team. Communication channels for reporting of security incidents by clients and vendors are identified within the client/ vendor contracts. CWT complies with all applicable data privacy laws and has robust privacy and information security controls in place to process and remediate any incidents in accordance with contractual or regulatory requirements.

Additionally we monitoring is implemented for Outbound and Inbound communications. CWT deploys SEP (Symantec Enterprise Protection) on the webservers and inbound active content from webservers, Internet-facing perimeter systems, mail servers, application servers, desktops, workstations and laptops. CWT performs ongoing 24 x 7 monitoring of all intrusion detection sensors and firewall log monitoring within the web hosting and browsing environments.

#### **6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?**

There are no known Privacy Risk in the E2 Solutions TAVS application.

## **SECTION 7.0 INDIVIDUAL PARTICIPATION**

*GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.*

### **7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.**

E2 Solutions TAVS displays the terms of use and a comprehensive Privacy Act notification before login and requires the user to acknowledge those provisions and assent to the terms of use and data protection responsibilities before gaining access to the system.

### **7.2 What procedures allow individuals to access their information?**

Security within the ETS2 E2 Solutions TAVS information systems application is controlled through role and hierarchical system configurations to ensure only personnel who have a need-to-know are strictly enforced. These roles (e.g. traveler, travel arranger, system administrator, approver and auditor) are authorized upon entry into the E2 Solutions TAVS information systems; portal and application user interface components are only visible and accessible if the user has been granted the associated privileges.

Authentication to E2 Solutions TAVS is performed with a unique login ID and strong password, which cannot be bypassed by a user or system administrator. All users will be able to access the E2 Solutions TAVS from non-government (non-SSO) locations using a User ID/Password. The client's Windows User ID can be assigned as the E2 Login ID. For multi-factor authentication, E2 Solutions TAVS supports Security Assertion Markup Language (SAML) 2.0 to federate with the client's authentication and policy servers. CWTSatoTravel utilizes Ping Identity as its single sign-on technology platform.

### **7.3 Can individuals amend information about themselves? If so, how?**

E2 Solutions TAVS uses a traveler's profile to store a range of configurable data that can be maintained online, from any location via use of a compatible Web browser, by the traveler or other users with appropriate permissions based on configurable agency business rules and travel policy. Traveler profiles are available for all ETS2 users, including non-federal invitational travelers. They are created online either through the agency on-boarding/implementation process, or manually online by a system administrator. While all users have the ability to maintain their own profiles online, use is subject to user access and specific data element permissions only designated travel arrangers and system administrators with the correct access permissions can view and maintain traveler profile data for other users. Customer agencies are responsible for the quality assurance of traveler profile data entered by the traveler via Web browser.

### **7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?**

E2 Solutions TAVS has no known identified privacy risks.

## **SECTION 8.0 AWARENESS AND TRAINING**

*GSA trains its personnel to handle and protect PII properly.*

### **8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.**

As part of the company induction program outlined within CWT's Global Human Resource policies, a new recruit must take the Security Awareness Training module on the Human Resource Learning portal on the company Intranet within 2 weeks of starting the job. This training module includes training on Data Protection (Includes PII Topics) and other emerging Security topics. The HR Learning Portal will automatically send warning messages if the new recruit hasn't completed the training module on time and the line manager will also check that the new recruit has completed the mandatory training using an Induction Checklist as part of the induction process. After introduction annual Security Awareness training is required for all employees annually.

### **8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?**

No, there are no known Privacy Risks as it relates to awareness and training.

## **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

*GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.*

### **9.1 How does the system, application or project ensure that the information is used in accordance with the 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 TAVS 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 TAVS 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.

## **9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?**

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.

---

[1] OMB Memorandum [Preparing for and Responding to a Breach of Personally Identifiable Information](#) (OMB M-17-12) defines PII as: “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” The memorandum notes that “because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.”

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.