Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the 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.

General Information

PIA Identifier: 417
System Name: e-Gov Travel - e2Solutions (eGT e2S)
CPO Approval Date: 3/27/2023
PIA Expiration Date: 3/26/2026

Information System Security Manager (ISSM) Approval

Arpan Patel

System Owner/Program Manager Approval

Rebecca Bond

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
e-Gov Travel - e2Solutions (eGT e2S)

B: System, application, or project includes information about:
Federal agency employee official travel details.

C: For the categories listed above, how many records are there for each?
1,033,142 active profiles excluding CWTSatoTravel support accounts as of today. We know some are invitational travelers, but we can assume all are federal employees.

D: System, application, or project includes these data elements:
Name Contact information SSN if required by agency financial system Credit Card/Payment Card Information, bank routing when required by agency financial system (DOS).

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate 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.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
Contracted Travel Services Program GSA/GOVT-4"

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
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.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: 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/

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
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.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 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. We have implemented a highly secure network configuration with managed firewalls and routers. We actively monitor 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.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
E2 Solutions TAVS does not monitor members of the public, GSA employees or contractors. We only track details as it relates to the travelers using the end to end system

3.5 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. 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

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
E2 Solutions TAVS does not de-identify any data.

4.0 Limits on Using and Sharing 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?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

4.2How: If so, how will GSA share the information?
CWTSatoTravel does not control how GSA shares information in support of our ETS2 Product E2 Solutions TAVS. We 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. The information stored in support of the E2 Solutions TAVS system is limited to the information needed to carry out the collection of data.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
E2 Solutions profile data is collected in one of three ways: During the onboarding process, a profile load file is compiled by the contracting Federal Agency to create user profiles in the system. 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. 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?
Yes

4.4WhoHow: If so, who and how?
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.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated 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.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
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 Open Web Application Security Project (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.

6.1b: 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 Open Web Application Security Project (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 a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
7/8/2023

6.3: How will the system or application be secured from a physical, technical, 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 and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: 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 monitor 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.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
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. Users who choose to opt out will not be able to login and receive travel service in the E2 Solutions TAVS Application.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
Users who choose to opt out will not be able to login and receive travel service in the E2 Solutions TAVS Application.

7.2: What are the procedures that 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?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

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

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to 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. Chronicle Backstory, Cisco AppDynamics, Splunk, , , and 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.