CWTSatoTravel

Privacy Impact Assessment (PIA) - Guidance

POINT of CONTACT

privacy.office@gsa.gov

Version 1.4: 5-27-2022

Instructions for GSA vendors:

This guidance is designed for nonfederal systems described in the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" and NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A supplement to NIST Special Publication 800-171". General Services Administration (GSA) requires vendors to conduct privacy impact assessments (PIAs) for electronic information systems and collections in accordance with GSA Order CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. PIAs offer an opportunity for vendors to highlight data protection, privacy by design, data minimization and similar principles that their services may employ.

Vendors may use this or their own templates/forms to meet the requirement. If vendors use their own template, GSA requires that vendors order their sections/responses consistent with the below questions for the benefit of GSA's customer agencies and for simplicity during the review process. The vendor must demonstrate how it collects, stores, protects, shares, and manages personally identifiable information (PII). The purpose of a PIA is to demonstrate that nonfederal system owners and developers have incorporated privacy protection throughout the entire life cycle of a system. GSA will publish the final product on its public website https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia. Please review all questions and the bracketed guidance, then develop your response.

GSA Stakeholders

The GSA representatives listed below have reviewed the information provided by the vendor for completeness.

Arpan Patel, GSA Information System Security Manager (ISSM):

X DocuSigned by: Arpan Patel 8B059AABDAF1477... 9/15/2026 | 19:18:46 BST

GSA Information System Security Manager

Micheal Salter, GSA Program Manager (PM):

X DocuSigned by: Michael Salter ABA02A5B3FBB446... 9/15/2026 | 19:17:10 BST

GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X DocuSigned by: Richard Speidel 171D5411183F40A... 9/15/2026 | 19:17:49 BST

GSA Chief Privacy Officer

Erin Lush, GSA Contracting Officer (CO):

X DocuSigned by: Erin Lush 86A60220FEBE415... 9/15/2026 | 14:16:01 EDT

GSA Contracting Officer

800-171 PIA Template Document Revision History

Date	Description	Version of Template
06/10/2020	Initial Draft of Non-Federal System PIA	1.0
08/05/2020	Version for rideshare vendors	1.1
10/20/2020	General updates for broader template usage	1.2
08/03/2021	Formatting and made 508 compliant	1.3
5/27/2022	Formatting and editing	1.4
10/15/2025	CW Government Travel Inc. Document creation	1.5
09/10/2026	Privacy Office updates requested	1.6
09/14/2026	Privacy Office final revision approved	1.6

Table of Contents

Document purpose

This document contains guidance for vendors that maintain and operate nonfederal systems. To provide the requested service, the vendor collects, maintains and/or disseminates 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.

Vendors should use this PIA guidance to explain how and why they collect, maintain, disseminate, use, secure, and destroy information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals.

Overview

A. System, Application, or Project Name:

CW Government Travel Inc. dba **CWTSatoTravel**

B. GSA Client:

The Federal Acquisition Service, within the Travel and Expense Services Division under the Travel Management Company (TMC) Program Management Office (PMO).

C. System, application, or project includes information about:

Go.gov provides official travel services for federal travelers. Services include booking travel (air, hotel, rental car), processing travel claims, and facilitating reimbursement. Reservations are fulfilled through a GSA-provided booking tool integrated with Global Distribution Systems (Sabre) and supported by CWTSatoTravel's call centers and applications.

Categories of Individuals:

- Federal employees on official travel
- Invitational travelers authorized under agency policy

D. System, application, or project includes these data elements:

[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."

The system processes Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII), including:

- Full name, date of birth, gender
- Contact details (home/office phone, email, address)
- Passport/visa details, SSN (if required for travel/finance)
- Credit card and bank account details (for EFT reimbursement)
- Frequent traveler numbers, travel preferences
- Emergency contact information
- Travel authorization and claim data
- TSA Secure Flight Data (name, DOB, gender, redress/known traveler number)

E. The purpose of the system, application, or project is:

The PII is collected to create itineraries, authorize travel, book accommodation, process payments, reporting and ensure compliance with Federal Travel Regulations. The TMC services/systems support federal mission requirements for official travel.

SECTION 1.0 OPENNESS AND TRANSPARENCY

1.1 Are individuals given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Individuals are notified via system login banners, privacy notices, and consent at account creation. https://cwtsatotravel.com/PrivacyPolicy.aspx

Privacy Act Statements are provided where applicable, referencing GSA/GOVT-4 (Contracted Travel Services Program) SORN.

SECTION 2.0 DATA MINIMIZATION

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

The collection of PII is necessary for Go.gov to manage official federal travel services. Traveler information such as name, date of birth, contact details, passport/visa details, payment card, and banking information is required to:

- Authenticate and verify traveler identity in compliance with TSA Secure Flight and other federal requirements.
- Reserve and issue tickets for air, hotel, and rental accommodations via the Global Distribution System (GDS).

- Facilitate accurate billing and settlement, including centrally billed accounts and electronic funds transfers.

Without this PII, Go.gov could not provide core travel services, nor support the federal mission to ensure secure, accountable, and efficient travel.

2.2 Will the system monitor the public, GSA employees, or contractors?

No. CWTSatoTravel does not monitor members of the public, GSA employees, or contractors. CWTSatoTravel systems monitoring is limited to technical and administrative activities necessary for securing the environment, ensuring service availability, and preventing unauthorized access

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

CWTSatoTravel generates reports related to travel services, including:

- Travel history and itinerary reports
- First class and business class transportation reporting
- Traveler location for safety & security

Reports are role-based, and access is restricted to authorized agency administrators and designated personnel. While some PII (e.g., traveler name, employee ID) may appear in reports, sensitive fields are masked where feasible.

2.4 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?

Traveler PII in reports may be masked, but data is not fully de-identified due to record retention and contractual requirements. De-identification is not applied because agencies require identifiable data for auditing, reimbursement, and compliance with NARA retention schedules (six years).

SECTION 3.0 LIMITS ON USING AND SHARING INFORMATION

3.1 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. CWTSatoTravel collects only the minimum PII and CUI necessary to support official federal travel. This includes traveler identity details (name, date of birth, gender), contact information, payment information, travel preferences, and government-issued identifiers where required. These data elements directly support identity verification, booking, reimbursement, and compliance with federal regulations. No superfluous data is collected

3.2 Will the information be shared with other individuals, federal and/or state agencies, private-sector organizations, foreign governments and/ other entities (e.g., nonprofits, trade associations)? If so, how will the vendor share the information?

Yes. Information may be shared with:

- **Federal agencies** – to validate travel authorizations, process reimbursements, and support financial reconciliation.
- **Private-sector service providers** – such as airlines, hotels, rental car companies, and financial institutions, solely for booking, payment, and fulfillment purposes.
- **System vendors/partners** – e.g., Sabre (Global Distribution System), CWTSatoTravel support systems, and payment processors.

Sharing is performed securely through encrypted connections (TLS, VPN, SFTP) and is strictly limited to the data elements necessary to complete the specific travel transaction.
CWTSatoTravel does not share traveler information with foreign governments, trade associations, or unrelated third parties unless required by law or regulation.

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

CWTSatoTravel will collect Traveler information in the following ways:
Direct entry by the individual – Travelers provide PII during profile creation, booking, or reimbursement submission via the Go.gov authorized booking tool.
Agency-provided profile uploads – Federal agencies may compile user profile files (containing traveler details) and provide them to Go.gov for automated upload and updates.

System administrators may update records only under the direction of authorized agency officials. Data collection and updates follow agency policies and are aligned with contractual obligations.

SECTION 4.0 DATA QUALITY AND INTEGRITY

4.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

Go.gov uses multiple controls to ensure the accuracy and completeness of traveler information:

- **Field validation at entry** – System input fields enforce formatting rules (e.g., name, date of birth, phone number, credit card details) to reduce errors during data entry.

- **Automated reconciliation** – Tools such as CCRecon match centrally billed credit card transactions with corresponding travel bookings to ensure financial data consistency.
- **Agency oversight** – Federal agency system administrators are responsible for reviewing and maintaining traveler profile information, ensuring that updates (e.g., contact details, travel preferences) are accurate and current.
- **Vendor controls** – CWTSatoTravel and system vendors monitor data flows between internal applications (e.g., booking, reporting, invoicing) and external systems (e.g., Sabre, merchant payment systems) to prevent mismatches or incomplete records.
- **Auditing and reporting** – Regular audits and reports help agencies identify discrepancies, with corrective measures applied promptly.

These measures collectively help ensure that the data used for travel booking, authorization, reimbursement, and compliance reporting is accurate, complete, and reliable.

SECTION 5.0 SECURITY

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

Access to Go.gov data is strictly role-based and limited to:

- **CWTSatoTravel personnel** – System administrators, security staff, and support teams who manage the infrastructure and travel systems.
- **Federal agencies** – Authorized agency system administrators and designated users responsible for managing traveler profiles, authorizations, and reporting.
- **Travel service providers** – Select partners such as Sabre (Global Distribution System) and merchant payment processors, who require access to limited data to complete travel transactions.

Access is granted on a need-to-know basis and follows documented approval workflows. Privileged access requires management authorization, multi-factor authentication (MFA), and is continuously monitored. Non-privileged and administrative roles are separated to prevent unauthorized escalation of privileges.

5.2 Has a System Security and Privacy Plan (SSPP) been completed for the information system(s) or application?

Yes. A System Security and Privacy Plan (SSPP) for Go.gov has been drafted. The SSPP categorizes the system as **FIPS 199 – Moderate** for confidentiality, integrity, and availability

5.3 How will the system or application be secured from a physical, technical, and managerial perspective?

Physical Security

- CWTSatoTravel support systems are hosted at Switch SuperNAP (Las Vegas, NV) and Equinix (Ashburn, VA) data centers, both of which provide armed 24/7/365 security, biometric access controls, CCTV, and mantrap entry.
- Facilities have redundant power (diesel generators, UPS), advanced fire suppression, and proprietary cooling systems ensuring >99.9999% uptime.

Technical Security

- Encryption in transit and at rest using TLS, VPN, and SFTP.
- MFA enforced for remote access (RSA SecurID, Citrix Secure Access VPN).
- Session timeouts after 15 minutes of inactivity with automatic termination.
- Logging and monitoring of privileged activities; alerts generated for anomalous behavior.
- Intrusion detection, firewalls, and vulnerability management processes in place.

Managerial/Administrative Security

- Policies aligned with NIST SP 800-171, 800-172, and 800-53 GSA selected requirements.
- Annual security and privacy training for personnel, with additional secure coding training for developers.
- Separation of duties between developers, operations, and security/audit staff to prevent collusion.
- Continuous auditing of logs, access approvals, and system changes to maintain accountability.

5.4 What mechanisms are in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

CWTSatoTravel's has established incident response procedures, which include:

- Centralized monitoring of system and security logs.
- Automated alerts for anomalous or unauthorized activity.
- Immediate containment and remediation processes.
- Notification to GSA and affected agencies in line with federal breach reporting requirements.
- Periodic exercises and phishing campaigns to test staff readiness

SECTION 6.0 INDIVIDUAL PARTICIPATION

6.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Travelers provide PII at the time of account creation and when booking or claiming reimbursement. Providing information is required to enable travel services and ensure compliance with Federal Travel Regulations and TSA Secure Flight requirements. Individuals cannot fully opt out of providing mandatory fields (e.g., name, date of birth, gender, government ID, payment information), as this would prevent booking and reimbursement. However, some optional information (e.g., travel preferences, frequent flyer numbers) may be provided at the traveler's discretion.

6.2 What procedures allow individuals to access their information?

Travelers can access their personal information through:

- The Go.gov authorized booking tool, which allows them to view itineraries, profile data, and stored preferences.
- The CWTSato To Go mobile app, which provides access to trip details, alerts, and travel services.

6.3 Can individuals amend information about themselves? If so, how?

Yes. Travelers may update personal information (e.g., contact details, payment cards, preferences) directly through the authorized Go.gov authorized systems. In addition, updates can be made through contracting the CWTSatoTravel Travel Experience agents.

SECTION 7.0 AWARENESS AND TRAINING

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

CWTSatoTravel personal supporting the Go.gov contract or having access to data are required to complete mandatory training programs that include:

General Privacy & Security Awareness Training – New personnel must complete privacy and security awareness training within 90 days of onboarding and annually thereafter. Training covers handling of PII, data minimization, and reporting of suspected incidents.

Developer Training – Developers and technical staff must complete secure coding training aligned to OWASP Top 10 practices and CWT's secure development methodology.

SECTION 8.0 ACCOUNTABILITY AND AUDITING

8.1 How does the system owner ensure that the information is only being used according to the stated practices in this PIA?

CWTSatoTravel employs multiple layers of accountability and auditing to ensure compliance with privacy and security requirements:

- **Audit Logging** – Significant user and administrator actions (e.g., creation of authorizations, bookings, claims, configuration changes) are logged with time stamps, user IDs, and before/after values.
- **Monitoring & Alerts** – Security, firewall, and server logs are monitored daily. Automated alerts are generated for unauthorized access attempts or anomalous activity.
- **Access Reviews** – Role-based access is reviewed periodically to confirm that only authorized personnel retain system privileges, with prompt revocation when access is no longer needed.
- **Audit Trails for Privileged Users** – Privileged operations are captured in centralized audit logs and reviewed regularly to ensure accountability of system administrators and prevent unauthorized activity.

Together, these measures ensure transparency, support oversight, and demonstrate compliance with federal privacy requirements.