



Travel Incorporated - Travel Management Platform

Privacy Impact Assessment (PIA) - Guidance

POINT of CONTACT

privacy.office@gsa.gov

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 the 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 protections 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

6/23/2026 | 18:48:03 BST

8B059AABDAF1477...

GSA Information System Security Manager

Michael Salter, GSA Program Manager:

X

DocuSigned by:

Michael Salter

6/11/2026 | 13:05:12 BST

ABA02A5B3FBB446...

GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X

DocuSigned by:

Richard Speidel

6/9/2026 | 20:00:35 BST

171D5411183F40A...

GSA Chief Privacy Officer

Janelle Scribner, GSA Contracting Officer Representative (COR):

X

DocuSigned by:

JANELLE SCRIBNER

6/11/2026 | 11:16:52 BST

B587777B86134FE...

GSA Contracting Officer Representative

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
5/18/2026	Privacy Office review completed and updates requested	1.5
6/04/2024	Privacy Office final review completed	

Table of Contents

Document purpose	1
Overview	1
SECTION 1.0 OPENNESS AND TRANSPARENCY	3
SECTION 2.0 DATA MINIMIZATION	3
SECTION 3.0 LIMITS ON USING AND SHARING INFORMATION	4
SECTION 4.0 DATA QUALITY AND INTEGRITY	5
SECTION 5.0 SECURITY	6
SECTION 6.0 INDIVIDUAL PARTICIPATION	8
SECTION 7.0 AWARENESS AND TRAINING	8
SECTION 8.0 ACCOUNTABILITY AND AUDITING	9

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 information¹ 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:

Travel Incorporated - Travel Management Platform

B. GSA Client:

Travel Incorporated

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

Federal Employees and Contractors

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

Personally Identifiable Information (PII): name, contact information

Travel itinerary data: trip dates, destinations, accommodations, transportation

Financial data: payment method details, cost breakdowns

Agency-specific preferences and travel history

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."

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

Travel Incorporated-Travel Management Platform (TI-TMP) is used to book travel for Federal Employees and Contractors

1. Collection of PII:

User Profile Creation/Management: A traveler would create or have a profile within the system. This would involve collecting their name, contact information (email, phone), agency ID, and possibly travel preferences (frequent traveler numbers, seating preferences). This data is essential for identification and personalizing the travel experience.

2. Use of PII:

Travel Authorization:

When a travel request is initiated, the system will collect PII related to the trip, such as the traveler's name, purpose of travel, destination, and dates. This ensures the authorization is tied to a specific individual and trip.

Booking and Reservations:

To book flights, hotels, and rental cars, the system would need the traveler's name, contact information, and potentially date of birth (as required by some vendors). If using a government travel card within the system, the card details (likely tokenized or masked) would be involved. Travel preferences like frequent flyer numbers or hotel loyalty IDs would also be collected to apply them to the bookings.

Expense Reporting:

For expense reimbursement, the system would need to identify the traveler's name and potentially bank account details if direct deposit is used. Receipts containing PII (like name and purchase details) might be uploaded.

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.

Yes. Acknowledgements are required when first using the system. They are stored with the user profile.

See [Appendix A - Travel Incorporated Privacy Policy \(https://www.travelinc.com/privacy-policy/\)](https://www.travelinc.com/privacy-policy/)

SECTION 2.0 DATA MINIMIZATION

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

PII is required to book travel for Federal Employees and Contractors

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

No

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

Agency travel Managers can report on travel activities by employees and contractors that are within their agency.

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?

If the Agency requests anonymized reporting, Travel Incorporated Travel-Management Platform (TI-TMP) provides reports either with identifiable data elements included or with data de-identified, based on the Agency's stated reporting requirement and business purpose.

De-identification and anonymization methods used (as applicable to the report type and data set).

- Aggregation by default when individual-level detail is not required, for example totals, counts, rates, and trends by time period, organization, location, service category, or other approved dimensions.

- Removal of direct identifiers from report outputs, for example name, email address, phone number, government identifiers, traveler profile identifiers, and free text fields that may contain identifiers.
- Masking, truncation, or tokenization for fields that must retain a realistic structure but do not require real values, for example masking all but the last 4 digits, truncating dates to month and year, or replacing internal identifiers with non-identifying tokens.
- Generalization, for example replacing exact timestamps with date buckets, replacing exact locations with broader geographic buckets, and replacing exact itinerary details with categories where feasible.
- Small-cell suppression to reduce re-identification risk in sparse populations, for example suppressing or rolling up categories when a group size is below an Agency-approved threshold.
- Data minimization in the report extract, limiting the data set to the minimum number of records and minimum set of fields necessary to satisfy the reporting objective.
- Controlled handling for exceptions, if the Agency requires identifiable reporting, the report content is limited to the minimum necessary fields, access is restricted to approved recipients, and distribution is controlled per the Agency's direction.

Agency direction.

The Agency can specify whether reports must be anonymized or must contain PII as needed for their specific business purposes. Travel Incorporated-Travel Management Platform (TI-TMP) will implement the above approaches accordingly.

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?

Data collected by the system will only be used for the purpose of booking travel.

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?

The information will not be shared with other individuals, federal and/or state agencies, private-sector organizations, foreign governments and/ other entities, except as required by law.

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)?

The data will be collected directly from the individual or an agency travel manager authorized to book travel on their behalf..

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

Data accuracy will be verified using the following methods:

1. User Validation:

Users maintain their own travel profile. Before finalizing a booking, present a summary of all the entered information for the user to review and confirm its accuracy.

2. Real-time Feedback: Provide immediate feedback to the user if they enter invalid data, guiding them to correct it before submission.

3. Backend Validation :

- Format Checks: Ensure data matches the expected format (e.g., email address format, phone number format, date format).
- Required Fields: Verify that all mandatory fields have been filled.
- Data Type Checks: Confirm that the entered data is of the correct type (e.g., numbers in a "quantity" field, text in a "name" field).
- Range Checks: Ensure numerical values fall within acceptable ranges (e.g., number of travelers must be a positive integer).
- Consistency Checks: If multiple related fields are entered, ensure they are consistent with each other (e.g., the departure city and arrival city are different).

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?

Employees, contractors, managers, and program staff.

Access will be specified by the project design documentation.

Travel Incorporated-Travel Management Platform (TI-TMP)'s agents assisting with travel booking.

Access will be specified by role, and controlled/audited by Travel Incorporated Human Resources Department

Travel Incorporated-Travel Management Platform (TI-TMP)'s backoffice associates responsible for invoices, billing, reporting, etc.

Access will be specified by role, and controlled/audited by Travel Incorporated Human Resources Department

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

The SSPP (Rev 3, Version 2) was submitted May 14, 2026. Approval is expected no later than June 30, 2026

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

Physical Controls:

Perimeter Security: Fences, security guards, surveillance cameras

Access Control: Key cards, locked doors, visitor management systems.

Surveillance: CCTV cameras monitoring critical areas, motion sensor lights and alarm systems.

Environmental Controls: Temperature and humidity controls for servers, fire detection and suppression systems, and uninterrupted power supplies.

Secure Disposal: Secure data destruction for hard drives and other media.

Technical Controls: Identification and Authentication systems, intrusion detection and prevention systems, Security Information and Event Management (SIEM), data encryption, data integrity controls data loss prevention systems, vulnerability management, patch management

Administrative Controls:

Policy and Standards: Policies and standards that govern various aspects, such as access management, data security, and acceptable user behavior.

Procedure and Guidelines: Procedure and guidelines for covering various areas such as onboarding/offboarding, change management, and data backup.

Risk Management: Risk assessments, incident response plan, business continuity plan, and disaster recovery plan.

Security Awareness and Training Program: Train employees on phishing, social engineering, malware and other security issues. Additionally, send out regular security awareness communications.

Personnel Security: Background checks for new hires, secure hiring processes, and separation of duties.

Governance and Compliance: Establish roles and responsibilities for cybersecurity. Additionally, develop and maintain controls for NIST SP 800-171

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?

Travel Incorporated-Travel Management Platform (TI-TMP)'s incident response plan provides procedures for effectively responding to security incidents, including defining the scope, outlining roles and responsibilities, and detailing the necessary response steps.

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.

In order to use the system the individual must accept our terms and conditions. The terms and conditions cover all the necessary uses of the information. Individuals can opt-out of information collection by deleting their account.

6.2 What procedures allow individuals to access their information?

Individuals can obtain a copy of their personal data by submitting a Data Access Request Form. Specific travel information will be provided to individuals on their travel itinerary.

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

Individuals can amend information about themselves by contacting a Travel Incorporated-Travel Management Platform (TI-TMP)'s Agent.

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.

All staff undergo privacy and security training upon joining the organization and annually. Security awareness communications are distributed monthly. Compliance is ensured through tracking the completion of training modules, which requires a signed acknowledgement from all staff.

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?

To ensure information is only being used in accordance to the stated practices in this PIA:

- Policies have been created governing the proper usage of information.
- Technical controls have been implemented to protect the information, monitor the usage of the information, and enforce the proper handling of information
- Regular audits are conducted to validate compliance with agency guidelines, NIST 800-171 guidance, and Travel Incorporated-Travel Management Platform (TI-TMP)'s policy

Certificate Of Completion

Envelope Id: 1A065E74-79B6-8F6C-8005-CD2EEF40E0BE

Status: Completed

Subject: Complete with Docusign: Travel Inc - Privacy-Impact-Assessment-(PIA).pdf

Source Envelope:

Document Pages: 15

Signatures: 4

Envelope Originator:

Certificate Pages: 2

Initials: 0

Tiwalade Adebajo

AutoNav: Enabled

1800F F St NW

Envelopeld Stamping: Enabled

Washington DC, DC 20405

Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London

tiwalade.adebajo@gsa.gov

IP Address: 136.226.21.19

Record Tracking

Status: Original

Holder: Tiwalade Adebajo

Location: DocuSign

6/9/2026 7:20:30 PM

tiwalade.adebajo@gsa.gov

Security Appliance Status: Connected

Pool: FedRamp

Signer Events

Arpan Patel

arpan.patel@gsa.gov

IT Specialist

US General Services Administration

Security Level: Email, Account Authentication
(None)

Signature

DocuSigned by:

Arpan Patel
8B059AABDAF1477...

Timestamp

Sent: 6/9/2026 7:26:54 PM

Viewed: 6/23/2026 6:47:58 PM

Signed: 6/23/2026 6:48:03 PM

Signature Adoption: Pre-selected Style

Using IP Address: 136.226.18.209

Electronic Record and Signature Disclosure:

Not Offered via Docusign

JANELLE SCRIBNER

janelle.scribner@gsa.gov

Program Analyst

US General Services Administration

Security Level: Email, Account Authentication
(None)

DocuSigned by:

JANELLE SCRIBNER
B587777B86134FE...

Sent: 6/9/2026 7:26:56 PM

Viewed: 6/11/2026 11:16:14 AM

Signed: 6/11/2026 11:16:52 AM

Signature Adoption: Pre-selected Style

Using IP Address: 136.226.19.83

Electronic Record and Signature Disclosure:

Not Offered via Docusign

Michael Salter

michael.salter@gsa.gov

Program Analyst

US General Services Administration

Security Level: Email, Account Authentication
(None)

DocuSigned by:

Michael Salter
ABA02A5B3FBB446...

Sent: 6/9/2026 7:26:54 PM

Viewed: 6/11/2026 1:04:55 PM

Signed: 6/11/2026 1:05:12 PM

Signature Adoption: Pre-selected Style

Using IP Address: 136.226.18.201

Electronic Record and Signature Disclosure:

Not Offered via Docusign

Richard Speidel

richard.speidel@gsa.gov

Chief Privacy Officer

US General Services Administration

Security Level: Email, Account Authentication
(None)

DocuSigned by:

Richard Speidel
171D541183F40A...

Sent: 6/9/2026 7:26:55 PM

Viewed: 6/9/2026 8:00:27 PM

Signed: 6/9/2026 8:00:35 PM

Signature Adoption: Pre-selected Style

Using IP Address: 136.226.18.91

Electronic Record and Signature Disclosure:

Not Offered via Docusign

In Person Signer Events

Signature

Timestamp

Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	6/9/2026 7:26:56 PM
Certified Delivered	Security Checked	6/9/2026 8:00:27 PM
Signing Complete	Security Checked	6/9/2026 8:00:35 PM
Completed	Security Checked	6/23/2026 6:48:03 PM
Payment Events	Status	Timestamps