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: 532
System Name: Go.gov
CPO Approval Date: 5/14/2026
PIA Expiration Date: 5/13/2029

Information System Security Manager (ISSM) Approval

Arpan Patel

System Owner/Program Manager Approval

Lauren Concklin

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Go.gov

B: System, application, or project includes information about:
Individuals covered by the system are Federal employees authorized to perform official travel, Federal employees authorized to manage travel, Federal employees authorized

to approve travel/reimbursement, and individuals being provided travel by the Federal Government (aka invitational travelers).

C: For the categories listed above, how many records are there for each?
There will be about 19 million reservations and 40 million vouchers when the system is in full operating capacity and all civilian federal agencies have migrated onto the platform.

D: System, application, or project includes these data elements:
● Full name of individual (traveler/employee)
● Employee ID information
● Travel personnel role
● Date of birth
● Place of birth
● Gender
● Accessibility requirements
● Medical alerts
● Dietary restrictions/preferences
● Passport information (number, country, expiration, etc.)
● Immigration information (green card, issued visas, etc.)
● Traveler redress ID number
● Home address
● Work address
● Email address (work and/or personal)
● Telephone number (work and/or personal)
● Emergency contact information
● Federal agency (employer)
● Business unit (department, division, etc.)
● Manager name and contact information
● Travel arranger/delegate name and contact information
● Trip purpose
● Government credit card information (number, expiration, etc.)

● Account information for fund transfers
● Travel vendor information (name, address, contact information)
● Travel booking preferences (airline seat type, car type, room type, etc.)
● Traveler loyalty program information (frequent flyer, hotels, car rental, etc.)
● Known traveler number (passenger number DHS utilizes to facilitate passenger clearance e.g. TSA Pre-Check, Global Entry)
● Redress number
● Passenger name record (PNR reference for bookings)
● Travel itinerary (dates, locations, mode of transportation)
● Expense details (type, lines of accounting, costs, advances, etc.)
● System roles (traveler, manager, approver, auditor, etc.)
● System ID (login ID, username)

Overview:

The General Services Administration (GSA) Federal Acquisition Service (FAS) has acquired a configurable, commercial Travel and Expense (T&E) technology managed service for deployment and centralized management across all government agencies. This development, known as GO.gov, is the third generation of the electronic government travel services (ETS). The T&E managed service includes capabilities for planning, authorizing, booking, and vouchering T&E expenses, along with audit and reporting functions to ensure compliance with travel regulations. Additionally, GO.gov offers essential services such as security, data integration, program management, training, help desk support, and change management. These services are delivered under a fully managed shared services model, ensuring seamless operations and effective transition support.

1.0 Purpose of Collection

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

5 USC 5701-5739,. 31 U.S.C. §§ 3511, 3512, and 3523; Federal Travel Regulation CFR-Title 41

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?
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.
GO.gov records are managed under the General Record Schedule 1.1, item 010
Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. The records created under this schedule are retained for 6 fiscal years after completion of the transaction and all payments made on travel or arrangements. The detailed schedule can be found at:
https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
PII is necessary to this system because it allows for user authentication, support services, updating them regarding their upcoming/current travel along with regulatory compliance such as financial transactions, identity verification and fraud prevention. The information collected is used to meet TSA/FAA requirements for travel purposes.

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?
The protections that exist to protect the system are implementing security and privacy controls required for FedRAMP Moderate security categorization. Role-based access controls are implemented for this application and only authorized users have access to the application. Agencies leverage single sign-on and identity provider solutions to facilitate multifactor authentication to grant access.

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

GSA Employees

3.4 Explain: Please elaborate as needed.
Yes, the system monitors GSA employees and contractors as well as other government employees. The system does not monitor the public.

3.5 What kinds of report(s) can be produced on individuals?
The GO.gov (formerly ETSNext) requires a “Data and Reporting Requirements Management Plan to address the “Required coverage to include activities and processes to transfer, store, cleanse, normalize and report on Authorization, Pre-Ticket Reservation (PNR), Post-Ticket Reservation (Back Office), Voucher, T&E Credit Card Charges, Reshopping, and User Experience to make available to agency customers and GSA via API interface. In addition, it requires the following for the “reporting service”.

This includes a comprehensive data set of reservation (both pre- and post-ticket),voucher, authorization, credit card, reshopping, and user experience data elements, as defined in the Data and Reporting Requirements Management Plan.

The Contractor shall provide designated users the ability to retrieve data sets consisting of a specified set of fields for each travel category (TMC Reservation & Ticketing, Voucher, Authorization, etc.) in a timely manner as defined in the Data and Reporting Requirements Management Plan. (DR-3)

Deliver a data storage, deletion, and retrieval plan consisting of documentation of its process for storing and retrieving a baseline of 6 years of ETSNext T&E data (and additional years if the specific agency requires it) to the Government within 21 days after contract award. (DR-4)

Submit a list of high impact fields for each T&E data category that traditionally cause challenges in Government analytics and reporting (e.g., valid Hotel Rate Codes, Lowest Fare, Vendor Names & Cities, etc.) and create an ongoing scorecard to evaluate these fields on a regular basis, as defined in the Data Cleansing and Normalization Plan. (DR-5)

The Requirements Traceability Matrix (RTM) has the following requirements for Reporting:

Requirement Description:

Capture information parameters (e g , reporting period, department/agency/office, trip begin/end dates) consistent with FTR.

Develop and document travel information (e g , number of reservations by type of service, payment for services unnecessary or unjustified, collection of outstanding travel advances) consistent with FTR.

Provide travel information (e g , reporting period, number of reservations by type of service, payment for services unnecessary or unjustified, collection of outstanding travel advances) consistent with FTR.

Develop and document travel trends and patterns analysis content (i e , structure and information), including government-designated source of record information consistent with FTR.

Provide travel trends and patterns analysis content (i e , structure and information), including government-designated source of record information consistent with FTR.

Provide reporting information from multiple government-designated information sources consistent with FTR.

Provide real-time access to a report builder tool that enables users to query, drag, drop, and filter data elements of interest and export results in Excel, CSV, and PDF formats.

Provide agencies with data visualization capabilities to slice and dice data from each data category.

Provide agency benchmark reporting to reveal behaviors or prices paid in context with other agencies and uncover opportunities for improvement.

Provide access to help desk reports and statistics, in a reasonable timeframe, by agency and type of issue, to better understand what challenges users are having in the system.

Provide ongoing reports to GSA and agencies regarding response time of reports and ad-hoc queries run.

Provide agencies with a comprehensive standard report set for each source of data (Authorization, Reservation, Back Office, Voucher, T&E Charge Card, UX, Reshopping) that can be scheduled or pulled for specific date ranges.

Provide a way to pull an extract of records that had a change in any of the report fields in a given day (authorization, reservation, voucher).

Provide the ability to schedule, extract, and distribute reports in the vendor's report set or ad-hoc reports to agency-specified lists of users.

Provide the ability to take a canned report and then filter it for a specific sub-agency, destination, date, etc. before exporting.

Generate standard reports of local authorizations as described by Agencies.

Demonstrate any pre-defined templates for standard reports such as Expense Summary, Travel Compliance, Approvals, etc. such as authorizations pending approval.

Demonstrate how the system enables users to select specific fields and filters to generate ad hoc reports tailored to the user's needs. Show how the system generates ad hoc reports in real-time, pulling the latest available data.

Show how the system provides various data visualization formats like charts, graphs, and heat maps to provide analytical insights for expense and travel data.

The system shall produce regular and normalized data extracts at the trip, air ticket, air segment, hotel, car, and voucher level so that agency stakeholders can feed the data into an internal dashboard or pivot with ease.

The system shall report on adoption rate to track the number of transactions not assisted by the TMC travel agent with the purpose to improve the adoption rate percentage and provide cost savings to the government.

The system shall provide reports on conference trip information to improve conference travel management.

The system shall record and make available the lowest available airfare brought back based on search parameters for reporting and data extracts.

Various pro forma reports as well as ad hoc reports can be run from a predefined set of data elements permitted for reporting. Many of the reports will be on government employee travel data, which include work travel activities to and from locations, travel documents used and travel expenses.

These reports may have identifying information like employee names, agency identifier, and email address, but would not have sensitive PII (e.g. passport number, full credit card info, DOB, etc.). Some non-sensitive identifying information is necessary for agencies to identify their own employees to manage travel expenditure budgets and detect fraud/abuse.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
Some reports will require individual identification. Agencies must be able to identify their own employees to manage travel expenditure budgets and detect fraud/abuse. Reports

not requiring identification will leave individual identifiers off the report or will utilize aggregation/summary by travel categories, periods, and/or groups of travelers.

3.6 Why Not: Why will the data not be de-identified?

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?
The GO.gov Solution utilizes Application Programming Interfaces (APIs) as well as flat files to integrate and transfer data between and among internal and external components.
The federal agencies will begin transmitting data to the GO.gov API Gateway to load and update master data (human resources and lines of accounting) using the GSA-specified GO.gov Financial Management Standard API. In turn, the GO.gov API Gateway will send data back to the agencies for processing advances, funds checks, obligations, and vouchers using the same standard API.
The GO.gov API Gateway will also push data to Travel and Expense (T&E) Technology Services processing advances, funds checks, obligations, vouchers, and master data using standard T&E Expense Technology APIs and file formats. Conversely, T&E Technology Services will send funds check, obligation, and voucher data back to the GO.gov API Gateway via standard T&E Expense Technology APIs.
T&E Data Services will transfer unused ticket data to T&E Technology Services in standard T&E Expense Technology file formats. Meanwhile, T&E Technology Services will send data to T&E Data Services processing reservations, authorizations, and vouchers for reporting, following T&E Expense Technology APIs and file formats.
The GO.gov API Gateway will send data to the bank payment gateway to collect Service Access Fees from agencies once a voucher is finalized, using the standard bank payment gateway API.
For travel-related services, T&E Expense Technology Services will push booking data to Direct Connect Travel Suppliers (e.g. train and airlines using supplier APIs). These suppliers will return e-receipt data via standard T&E Expense Technology.
GSA SmartPay Card Providers (i.e. banks) will send credit card transaction data to T&E Expense Technology Services in payment card file formats.
The Global Distribution System (GDS) will provide PNR data to T&E Data Services via standard GDS APIs and deliver travel inventory (air, car, hotel) to T&E Technology Services through the same APIs.
Surge Blanket Travel (i.e. group travel booking vendor) will pull employee details and reservations from T&E Expense Technology Services to organize Surge Blanket Travel events using standard T&E Expense. The vendor will also create travel authorizations within T&E Expense Technology through the same APIs.
GO.gov will authenticate travelers, administrators, and process owners via integration with agency SSO solutions for secure access to T&E Technology Services across mobile, tablet, and desktop devices.
Finally, the GO.gov API Gateway will update the help desk software platform with user profile data whenever changes occur in the T&E Expense Technology.

In addition, GSA may share certain government-wide de-identified reports as required for government reporting (e.g. OMB, OGP, government-wide acquisition teams, etc.), but these reporting requirements are still under development.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
Federal agency business systems may provide Human Resource (HR) or Financial Management (FM) data (Employee Name, Address, Email, Phone)

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?
The GO.gov Solution utilizes Application Programming Interfaces (APIs) as well as flat files to integrate and transfer data between and among internal and external components.
The federal agencies will begin transmitting data to the GO.gov API Gateway to load and update master data (human resources and lines of accounting) using the GSA-specified GO.gov Financial Management Standard API. In turn, the GO.gov API Gateway will send data back to the agencies for processing advances, funds checks, obligations, and vouchers using the same standard API.
The GO.gov API Gateway will also push data to Travel and Expense (T&E) Technology Services processing advances, funds checks, obligations, vouchers, and master data using standard T&E Expense Technology APIs and file formats. Conversely, T&E Technology Services will send funds check, obligation, and voucher data back to the GO.gov API Gateway via standard T&E Expense Technology APIs.
T&E Data Services will transfer unused ticket data to T&E Technology Services in standard T&E Expense Technology file formats. Meanwhile, T&E Technology Services will send data to T&E Data Services processing reservations, authorizations, and vouchers for reporting, following T&E Expense Technology APIs and file formats.
The GO.gov API Gateway will send data to the bank payment gateway to collect Service Access Fees from agencies once a voucher is finalized, using the standard bank payment gateway API.
For travel-related services, T&E Expense Technology Services will push booking data to Direct Connect Travel Suppliers (e.g. train and airlines using supplier APIs). These suppliers will return e-receipt data via standard T&E Expense Technology.
GSA SmartPay Card Providers (i.e. banks) will send credit card transaction data to T&E Expense Technology Services in payment card file formats.
The Global Distribution System (GDS) will provide PNR data to T&E Data Services via standard GDS APIs and deliver travel inventory (air, car, hotel) to T&E Technology Services through the same APIs.
Surge Blanket Travel (i.e. group travel booking vendor) will pull employee details and reservations from T&E Expense Technology Services to organize Surge Blanket Travel events using standard T&E Expense. The vendor will also create travel authorizations within T&E Expense Technology through the same APIs.
GO.gov will authenticate travelers, administrators, and process owners via integration with agency SSO solutions for secure access to T&E Technology Services across mobile, tablet, and desktop devices.
Finally, the GO.gov API Gateway will update the help desk software platform with user profile data whenever changes occur in the T&E Expense Technology.

In addition, GSA may share certain government-wide de-identified reports as required for government reporting (e.g. OMB, OGP, government-wide acquisition teams, etc.), but these reporting requirements are still under development.
4.3: How is the information collected:
Initially, information is collected directly from the Individual, agency Human Resource (HR) or Financial Management (FM) systems, to develop the Traveler Profile. Travel Requests (Authorizations) and Expense Reports (Vouchers are created by the Traveler or Travel preparer for each individual trip. Data is provided by the Travel Management Company (TMC), which generates the reservations (itinerary) for the trip.and is updated from the travel providers (e.g. TMCs, GDS, airlines, hotels, etc.)

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?
It is the customer agency and user's joint responsibility to make sure that the information inputted into the system is accurate. The system also verifies the required sections are completed and filled out. Depending on the data field it verifies if the data has been filled out if required and where sources are available they are checked to determine if the data entered is valid e.g. zip code.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
The contracted service providers have access to the system along with the agency supplied identity providers which have a direct system integration to facilitate authentication and/or single sign-on functions. . Authorized agency users have access to the data within the system after successfully authenticating. For example, administrators, process owners, and traveler/users have access to the system.

6.1b: What is the authorization process to gain access?
GO.gov works with each customer agency to establish appropriate user roles with correct permissions and then assigns the correct user roles through a profile data import for each Federal employee to grant access to GO.gov. Federal Agency Travel Administrators (FATAs) with defined access maintain the user profiles after implementation. Federal agency business systems interface with GO.gov for proper recording of authorizations and vouchers. Data is exchanged between systems and is documented in IAA and/or Memorandum of Understanding (MOU). The agency business systems do not have direct access to GO.gov databases.

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.
12/17/2025

6.3: How will the system or application be secured from a physical, technical, and managerial perspective? managerial perspective?
This system has the ability to track individual user actions within the system. The audit and accountability controls are based on NIST and GSA standards, which in turn are based on applicable laws and regulations. The controls assist in detecting security

violations or other issues in the system. Access to this system is restricted to authorized government employees and contractors who require access for official business purposes. Users are classified into different roles and common access and usage rights are established for each role. User roles are used to delineate between the different types of access requirements such that users are restricted to information that is required in the performance of their duties. Periodic audits and reviews are conducted to determine whether users still require access and have the appropriate roles.

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?
The procedures for handling security incidents are documented in the GO.gov incident response plan. Any security incidents suspected or confirmed involving GO.gov system as a whole or any subcomponents (e.g. SaaS, PaaS, IaaS, etc.) hosted by other vendors handling GO.gov data is reported up to GSA Incident Response (IR) team by the contracted service provider. The GSA IR team is notified in the event of an incident, and they work with the service provider and affected vendors to resolve any potential breach.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Opportunities are provided to individuals to consent to the use of the information system or application through the Privacy Act notice at login. Any individual who declines to provide information is denied access. If the user agrees to the Privacy Act Statement and logs in, the user may be asked to review their profile and, in some cases, to populate their airline seat preferences, their passport number, their frequent flier numbers, and other flight preferences. They can decline and not enter this information, but not providing certain information may prevent the individual from being able to complete their travel booking (some information is optional while others are not).

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
The HR/FM data is master data owned by the agency, provided to GO.gov and imported into GO.gov. Individuals may review the information, complete additional required fields and add optional fields like frequent flyer numbers for example. If an individual would like to decline use of the system, the individual would need to contact the GO.gov help desk to request to be removed from the system, which would trigger a notification to the agency business process owner to remove the individual from GO.gov.

7.2: What are the procedures that allow individuals to access their information?
When logged into the system the users are able to access their information in their Traveler Profile.

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.

Each respective agency is responsible for providing general privacy training in accordance with applicable laws and guidance. GO.gov managed service provider gives system specific training for certain user roles that may have privileged access to data with privacy implications.

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?

This Privacy Impact Assessment is included in the package of materials required for information security reviews. GSA periodically facilitates third-party assessments to review all information security artifacts for compliance with the requirements, including the use of information in accordance with the PIA. GO.gov has implemented the required security and privacy controls according to GSA. The systems employ a variety of security measures defined in the System Security and Privacy Plan (SSPP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, identification and authentication, incident response, planning, personnel security, system and communications protection. Finally, role-based access control has been implemented to allow access only to users based on job functions or roles.