E-Gov Travel Service Next Generation (ETSNext) (branded GSA Implementation of GO.gov MiSaas)-PIA

Privacy Impact Assessment (PIA) - Guidance

POINT of CONTACT

privacy.office@gsa.gov

Version 1.6: 4-17-2025

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 8B059AABDAF1477...

GSA Information System Security Manager

Christine Courter, GSA Program Manager:

X DocuSigned by: Christine Courter 693864BCE7814B5...

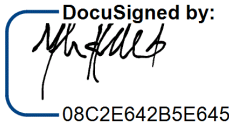
GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X DocuSigned by: Richard Speidel 171D5411183F40A...

GSA Chief Privacy Officer

Melvin Hubbard, GSA Contracting Officer Representative (COR):

X 

GSA Contracting Officer Representative

800-171 PIA Template Document Revision History

Version 1.6: 4-17-2025

Date	Description	Version of Template
12/2/2025	**Initial Draft of Non-Federal System PIA**	**1.6**
12/4/2025	**Final Draft**	**1.6**
12/9/2025	**Final Revisions**	**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:

E-Gov Travel Service Next Generation (ETSNext) (branded GSA Implementation of GO.gov MiSaas)

B. GSA Client:

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. System, application, or project includes information about:

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

[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."

- Place of birth
- Sex
- 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)

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

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.

The legal authority and/or agreements that allow GSA to collect, maintain, use, or disseminate the information are

United States Code (USC) 5 USC 5701-5739, and 31 U.S.C. §§ 3511, 3512, and 3523; Federal Travel Regulation CFR-title41.

For reference, here are the authority citations for that CFR entry: 5 U.S.C. 5707; 5 U.S.C. 5738; 5 U.S.C. 5741-5742; 30 U.S.C. 905(a); 31 U.S.C. 1353; 49 U.S.C. 40118; E.O. 11609, 3 CFR, 1971-1975 Comp., p. 586

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.

SECTION 2.0 DATA MINIMIZATION

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

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.

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

The system monitors GSA employees and contractors as well as other government employees.The system does collect unique identifiers on government employees to help track the users travel information such as bookings, expense, reimbursements along with being able to track where they will be scheduled to be based on their travel itineraries in case of emergencies.

The system however, does not monitor the public; individuals traveling on behalf of the government (invitational travelers/members of the public) are treated as federal employees when they are on TDY Travel.

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

The GO.gov (formerly ETSNext) system 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. Additional requirements for the "reporting service" include:

a) 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.

b) 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)

c) Delivery of 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)

d) Submission of 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 sources information 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.

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?

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.

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.

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. A Secure File Transfer Protocol Solution is utilized between GO.gov and the Financial Management (FM) System. The solution uses AWS Transfer Family to provide SFTP connectivity with FIPS-compliant, AWS-encrypted endpoints and TLS 1.2 securing all communications. Files are stored in Amazon S3, where they are protected with AES-256 encryption at rest. Authentication is performed using user accounts and certificates, with no passwords allowed. All data transferred through the platform is additionally protected with PGP encryption: inbound files to GO.gov are encrypted using GO.gov public key, while outbound files to the FM System are encrypted with a FM public key. At no point are files stored or transmitted in plain text.

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)?

Initially, information is collected directly from the Individual, 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).

Other sources include Federal agency business systems which may provide Financial Management (FM) data (Employee Name, Address, Email, Phone).

SECTION 4.0 DATA QUALITY AND INTEGRITY

4.1 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.

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?

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.

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.

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

Yes. GSA Implementation of Go.gov MiSaas(GIGM) CRM SSP pending ATO.

5.3 How will the system or application be secured from a physical, technical, and 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.

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?

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.

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.

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).

No they cannot opt-in or opt-out.

The Financial Management (FM) System 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.

6.2 What procedures allow individuals to access their information?

When logged into the system, the users are able to access their information in their Traveler Profile.

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

Yes.

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Requests must be submitted to the agency contact indicated on the initial document on which the related contested record was submitted. All information about

individuals within the system originates from either the agency's FM or HR systems. Therefore, amendments must be made through the individual's agency representative who has the authority to make the requested amendment and update information in the system.

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.

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.

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?

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 system employs 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.

Certificate Of Completion

Envelope Id: 20D1E65E-4698-4438-827F-AFDF5A62D3AA
Status: Completed
Subject: Complete with Docusign: E-Gov Travel Service (ETS) (branded GO.gov)-PIA.docx
Source Envelope:
Document Pages: 16
Signatures: 4
Certificate Pages: 2
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London

Envelope Originator:
Melvin Hubbard
1800F F St NW
Washington DC, DC 20405
melvin.hubbard@gsa.gov
IP Address: 136.226.20.100

Record Tracking

Status: Original
12/12/2025 1:41:42 PM
Holder: Melvin Hubbard
melvin.hubbard@gsa.gov
Location: DocuSign

Security Appliance Status: Connected
Pool: FedRamp

Storage Appliance Status: Connected
Pool: US General Services Administration
Location: Docusign

Signer Events	Signature	Timestamp
MELVIN HUBBARD melvin.hubbard@gsa.gov Program Specialist US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: 08C2E642B5E645A... Signature Adoption: Drawn on Device Using IP Address: 136.226.20.100	Sent: 12/12/2025 1:48:33 PM Viewed: 12/12/2025 1:48:44 PM Signed: 12/12/2025 1:48:58 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Arpan Patel arpan.patel@gsa.gov IT Specialist US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Arpan Patel 8B059AABDAF1477... Signature Adoption: Pre-selected Style Using IP Address: 173.79.167.15	Sent: 12/12/2025 1:49:00 PM Viewed: 12/12/2025 1:54:28 PM Signed: 12/12/2025 2:01:39 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Christine Courter christine.courter@gsa.gov Director, Office of Travel and Charge Card Services US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Christine Courter 693864BCE7814B5... Signature Adoption: Pre-selected Style Using IP Address: 136.226.21.41	Sent: 12/12/2025 2:01:40 PM Viewed: 12/12/2025 2:26:45 PM Signed: 12/12/2025 2:27:05 PM
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 171D5411183F40A... Signature Adoption: Pre-selected Style Using IP Address: 136.226.19.74	Sent: 12/12/2025 2:27:07 PM Viewed: 12/12/2025 2:38:59 PM Signed: 12/12/2025 2:39:15 PM
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
Erin Lush erin.lush@gsa.gov Contracting Officer U.S. General Services Administration (GSA) Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via Docusign	COPIED	Sent: 12/12/2025 2:39:18 PM Viewed: 12/12/2025 2:40:23 PM
Carolina McFaul carolina.mcfaul@gsa.gov Contracting Officer US General Services Administration Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via Docusign	COPIED	Sent: 12/12/2025 2:39:18 PM

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	12/12/2025 1:48:33 PM
Certified Delivered	Security Checked	12/12/2025 2:38:59 PM
Signing Complete	Security Checked	12/12/2025 2:39:15 PM
Completed	Security Checked	12/12/2025 2:39:18 PM

Payment Events	Status	Timestamps