United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Go.gov		**System Owner: Adil Gulamali**	
Preparer: Andrew Lam		**Office: OFA/OCIO**	
Date: 06.30.26		**Phone: 202.564.2925**	
Reason for Submittal:			
New: ☐X	Revised:☐	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: X☐	
Operation & Maintenance: ☐	Rescindment/Decommission: ☐		

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

The GO.gov system is a multi-component System of Systems (SoS) designed to provide an integrated suite of travel, expense, integration, notification, and reporting services in support of Federal agencies. GO.gov's core purpose is to streamline and standardize federal travel and expense operations while maintaining compliance with federal security and privacy regulations. GO.gov integrates several commercial Software as-a-Service (SaaS) and Platform-as-a-Service (PaaS) offerings with secure hosting environments within AWS GovCloud (US) and AWS East/West commercial regions to provide

a unified, end-to-end business capability. Go.gov is replacing Concur.

Section 1. Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

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

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

GO.gov has a completed System Security Plan and a FedRAMP ATO. It expires on 05/06/2029. The Authorization To Use (ATU) date is still to be determined.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Go.gov information is not covered by the Paperwork Reduction Act. No ICR is required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FEDRAMP approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Go.gov data is maintained and stored in the Cloud. Go.gov is FedRAMP approved and is a SaaS.

Section 2. Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

- 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)

2.2 What are the sources of the information and how is the information collected for the system?

The information is collected by travel form and other sources, including Federal agency business systems such as Human Resource (HR) or Financial Management (FM) data (Employee Name, Address, Email, Phone).

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Cincinnati Finance staff ensure the data provided on the form is correct and enter it into the system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of

information included

Privacy Risk:

The privacy information provided by the travel requestor is inaccurate.

Mitigation:

Inaccurate information by the requestor will result in no payment being made. Cincinnati Finance staff must review the provided information thoroughly, validate for discrepancies, and request that the requestor make the necessary corrections.

Section 3. Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

The system has role-based access controls to prevent authorized users from accessing information they don't have a need to know. When multiple roles are used, each user is limited in the actions they can take and the information they can see while a payment is being processed.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Cincinnati finance center maintains Standard Operating Procedures (SOPs) that define the actions each role can perform.

3.3 Are there other components with assigned roles and responsibilities within the system?

The GO.gov system incorporates role-based access controls that limit users' rights based on the information they need to review or the activities they need to perform. The user's role is identified by the employee's supervisor, approved by regional/national system administrators, and then by the GO.gov system Security Administrator. There are no other users other than the authorized users.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

OFOM staff (Contractor), Cincinnati Finance Center (EPA Employee).

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule

number.

Records are maintained for 6 years and 3 months after final payment. They are deleted when no longer needed.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system

Privacy Risk:

The data stored in GO.gov is kept active in the system for longer than required.

Mitigation:

To mitigate the risk of over-retention in GO.gov, records are retained for up to 6 years and 3 months after final payment, then deleted.

Section 4. Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Information shared outside of the EPA is part of the normal agency operations. Ticketing records must be sent to the Travel Management Company (TMC). They use the profile information to issue tickets.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The original purpose of GO.gov was to book travel and make travel-related payments

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

MOUs and ISAs are reviewed by the Agency Information Security Office (ISO) with the approval of the Senior Information Official (SIO) and the Chief Information Officer (CIO).

4.4 Does the agreement place limitations on re-dissemination?

Yes. Data use is covered in the MOU between interconnecting systems.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Information shared outside of the agency may be compromised if handled inappropriately.

Mitigation:

MOU between EPA and outside agencies describes the PII within the information system and the purposes for its distribution and how the data should be protected. To mitigate the risk of information being shared inappropriately, EPA users must take the Security and Privacy Awareness Training to ensure that they understand EPA privacy responsibilities and procedures.

Section 5. Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

Individuals who have access to Go.gov agree to use the system solely for travel. All users are subject to the system's security controls and roles. They all have at least a Basic National Agency Check with Inquiries (NACI) background screening.

All EPA personnel with access to sensitive data are required to undergo a higher Level of background screening sponsored by the EPA. Go.gov employs role-based access and the principle of least privilege, granting users only the minimum rights needed to perform their tasks—no more and only for as long as necessary.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection

EPA personnel and contractors are required to complete an Information Security and Privacy Awareness and Training course annually. The training course instructs personnel not to disseminate PII to unauthorized individuals and to secure information using approved techniques, such as encryption.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

An unauthorized user accessing the system or a user who tries to access any data in GO.gov.

Mitigation:

The GO.gov system implements least-privilege access controls that limit users' rights to only what information they need to review or activities they need to perform. The GO.gov user's role is identified by the employee's supervisor, approved by regional/national system administrators, and then by the GO.gov system Security Administrator**.**

Section 6. Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

GO.gov uses the information to book travel and make payments for travel.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: X☐ No: ☐ If yes, what identifier(s) will be used.

A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.

Travel Management Company (TMC) Reservation & Ticketing, Voucher, Authorization.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

There is a standard operating procedure (SOP) that has been developed to enforce the sole use and purpose of collection. Individuals that have access to this system agree to use the system strictly for the purpose of collection.

All users are subject to security controls and roles in the system. They all have at least a basic National Agency Check with Inquiries (NACI) background screening. All EPA personnel with access to sensitive data are required to undergo a higher level of background screening sponsored by EPA. GO.gov employs role-based access and the principle of least privilege, granting users only the minimum rights needed to perform their tasks—no more and only for as long as necessary.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Users mishandle GO.gov PII.

Mitigation:

To reduce the likelihood of PII mishandling in GO.gov, Security and Privacy Awareness Training is provided to ensure personnel understand their privacy responsibilities and procedures. EPA personnel and contractors are required to complete an Information Security and Privacy Awareness Training course annually. The training course instructs personnel not to disseminate PII to unauthorized individuals, how to secure information using approved techniques such as encryption, and how to destroy and dispose of PII properly. Individuals with system access must undergo a security background check. Go.gov only grants access to users based on the principle of least privilege, which provides users with sufficient access to perform their jobs, no more than necessary to accomplish their organizational missions/business functions.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not

GO.gov provides notice via a posted privacy policy, on-page point-of-collection disclosures (including a Privacy Act Statement for any PII collected from users), and the authentication provider's privacy notice. For general visitors following shortened links, only standard web logs and permitted analytics are collected, as described in the policy.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of the collection or sharing of their information?

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 for which the related contested record was submitted. Complete EPA Privacy Act procedures are set out in 40 C.F.R. part 16.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information.

Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Notices may not provide enough information for users to understand the full uses of their information.

Mitigation:

There is a notification procedure outlined in the government-wide SORN, GSA/GOVT-4.

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and Freedom of Information Act (FOIA).

Privacy Risk:

Individuals' records could be provided to the incorrect requestor.

Mitigation:

EPA's Privacy Act request process ensures the requestor gives appropriate identification during a

Privacy Act and/or FOIA Request before EPA can share any records that EPA may maintain on that individual.

I attest as the Agency Privacy Officer that **GO.gov** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.07.10 12:54:57 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA