CI Travel Back Office Enclave (CBOE) - 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 _____

GSA Information System Security Manager

Michael Salter, GSA Program Manager:

X _____

GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X _____

GSA Chief Privacy Officer

Jason Cross, GSA Contracting Officer Representative (COR):

X_____

GSA Contracting Officer Representative

800-171 PIA Template Document Revision History

Date	Description	Version of Template
1/30/2026	Initial Draft of Non-Federal System CI Travel Back Office Enclave (CBOE) PIA.	1.0
2/2/2026	Revisions to initial draft.	1.1
2/9/2026	Final Revisions.	

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:

This system and its supporting infrastructure boundary are referred to as the CI Travel Back Office Enclave (CBOE).

B. GSA Client:

CI Travel

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

CI Travel Back Office Enclave (CBOE) agents support customers by creating ticketed air/rail reservations and the associated lodging and rental car reservations. This data originates in the Global Distribution Systems (GDS) and then the Passenger Name Record (PNR) record is securely transferred to CBOE at CI Travel's headquarters location. CBOE leverages Passenger Name Record (PNR) data to invoice for the travel booked by CI Travel Back Office Enclave (CBOE) travel agents.

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

- *Name and other demographic information including date of birth and, Sex for Government Travelers booking Travel with CI Travel Back Office Enclave (CBOE);*
- *Contact information including telephone number and, email address for Government Travelers booking Travel with CI Travel Back Office Enclave (CBOE) and,*

[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."

- *Financial Information (credit card/Payment Card Information (PCI)) for Government Travelers booking Travel with CI Travel Back Office Enclave (CBOE).;*

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

CI Travel Back Office Enclave (CBOE) provides government services for arranging travel for government personnel. CI Travel Back Office Enclave (CBOE) leverages travel technology to orchestrate front office (e.g. reservations, invoice) and back office (e.g. accounting, collection, deposits) workflows.

CI Travel Back Office Enclave (CBOE) agents support customers by creating ticketed air/rail reservations and the associated lodging and rental car reservations. This data originates in the Global Distribution System (GDS) and then the Passenger Name Record (PNR) record is securely transferred to CBOE at CI Travel's headquarters location. CBOE leverages PNR data to invoice for the travel booked by CI Travel Back Office Enclave (CBOE) travel agents. The Passenger Name Record (PNR) record includes credit card numbers, gender, email address, name, and date of birth (DoB).

These front-office applications capture reservations, itineraries, and invoices. The data from these transactions are sent to the back office through the interface process eliminating the need to manually add sales into Trams back-office system. The Trams back-office system captures and stores the names and addresses of customers, the invoice numbers, amounts and travel dates, etc., to account for each sale. This data serves as the foundation for the enablement of decision support reporting. The common link between the front office and the back office is the invoice. The invoice is the product of the front office and the entry point of the back office. The Trams system is the primary processor of government customer information within the CI Travel Back Office Enclave (CBOE). The remainder of the CBOE environment is supporting infrastructure to process interfaces, run reports, and securely store data.

Trams is a commercial off the shelf (COTS) system and originally licensed by Tres Technologies. Based in Palos Verdes Peninsula, California, Tres is a Solution developer who specializes in the development of the original Trams system and the newer Tres systems which will replace Trams in the future. The system is installed at the CI Travel headquarters network location on a virtual machine. The virtual machine provides access to the software front end which communicates to the Trams database. The system can only be accessed by users on the CI Travel network or connected to the network through a VPN. Only domain users have access to the CI Travel VPN

client. This system and its supporting infrastructure boundary are hereby referred to as the CI Travel Back Office Enclave (CBOE)

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.

CBOE does not collect personal information from end users. Passenger Name Record (PNR) data is sent to CBOE via a secure, interface connection through a web service. This information originates in the Global Distribution System (GDS) system. For this effort, the Travelport + GDS system has their own, separate Privacy Policy that is posted by Travelport. To be able to book travel, users must give their information to the GDS or online booking tool authorizing the use of that data for travel related services, which includes the payment processing performed using CBOE. CI Travel Back Office Enclave (CBOE) does not manage these as we do not elicit the information from the end users. For example, the Privacy Policy for Travelport is located here: https://www.travelport.com/privacy

SECTION 2.0 DATA MINIMIZATION

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

CI Travel Back Office Enclave (CBOE) needs to collect the specific traveler information in order to invoice travel companies for the ticketed travel.

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

CI Travel Back Office Enclave (CBOE) does not monitor users. The Passenger Name Record (PNR) data is ingested after a booking or reservation is booked and/or invoiced. Travelers do not need to be logged into the Global Distribution System (GDS) or CBOE for travel to be booked.

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

User travel plans, or travel history is available inside CI Travel Back Office Enclave (CBOE). Reports in CBOE provide a passenger name with the payment card used to book the travel. There are no user summaries or reports providing a traveler's personal details as the system is used for accounting purposes and not to book or schedule travel.

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?

CI Travel Back Office Enclave (CBOE) leverages an external reporting tool called Grasp to build customer reports to meet contract requirements. Based in Dublin Ohio, Grasp is a Travel Management software solution provider for reporting. Currently, the data used in Grasp reporting does not include PII. The Activity Reports include masked Credit Card numbers (masks

and last four). Names are also available in these reports but without additional identifying information.

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?

CI Travel Back Office Enclave (CBOE) data is used for customer reporting. PII and PCI data are never used for marketing or business development. The total annualized values of travel spend by organization is used; however, specific user or payment data is never associated with metrics in aggregate. The use of the data for invoicing purposes is consistent with the Global Distribution System (GDS) privacy policy that states data obtained in collecting tickets is used for business purposes only.

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?

CI Travel Back Office Enclave (CBOE) data is used for customer reporting. Customer reports are developed internally and provide a summary of the amount of travel dollars booked and to which payment card. These reports can be broken down by individual activities within an agency, by location, by office and by date. This information is emailed to customers as specified by individual contracts. Primarily these reports are sent weekly and monthly as accounting summaries for CI Travel Back Office Enclave (CBOE) customers. If customer access is given for customer specific reports, the specific customer is only given access to their data which is controlled by row level security which implements security controls that only allow the organization that owns the data to access that row of data which is the point of storage. Today, these customer reports are emailed to the corresponding customers by CI Travel.

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)?

To be able to book travel, users provide their Personally Identifiable Information (PII) and payment information in the Travelport + GDS or online booking tools (such as ConcurGov or Go.Gov) authorizing the use of that data for travel related services, which includes the payment processing performed by CI Travel Back Office Enclave (CBOE). This information then flows through a secure channel to CI Travel Back Office Enclave (CBOE).

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

CI Travel Back Office Enclave (CBOE) uses profile data that is entered originally by end user organizations into the Global Distribution System (GDS) system. If this information is incorrect, then reservations or bookings made by CI Travel Back Office Enclave (CBOE) agents will not succeed. This information would need to be corrected in Go.Gov or Travelport + GDS to continue to process the booking. When that occurs a CI Travel Back Office Enclave (CBOE) agent will contact the end traveler or the customer initiator of the travel and confirm the incorrect data over the phone. CI Travel Back Office Enclave (CBOE) agents cannot log into the GDS on the customer's behalf and correct the information.

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?

Users are granted access to CI Travel Back Office Enclave (CBOE)under the following conditions.

1) *Successful screening process. CI Travel only hires individuals that have a successful background screening process initiated by Human Resources prior to employment.*
2) *Signed Non-Disclosure Agreement. CI Travel only grants individual access to customer data that have signed non-disclosure agreements specific to those programs.*
3) *New Hire Training. Every new hire is required to attend new hire training. This new hire training includes human resource policies and cybersecurity training.*
4) *Annual Cybersecurity Training. All CI Travel contract and supporting staff members must take annual cybersecurity training specified by contract requirements.*
5) *Need to Know. Only those individuals with a Need to Know are granted access to sensitive company information. For Trams, only personnel that are required to access financial information are granted access to the system.*
6) *Departmental Approval. Only those individuals with approval from the Chief Financial Officer (CFO) may have access to Trams.*
7) *Technology Safeguards. Only individuals that are seated within the network boundary, or have Virtual Private Network (VPN) access are permitted to access the system. SSPP*

There are three types of accounts.

1) *User. Users have base access to the system for accessing and performing transactional duties within the system.*
2) *Manager. Managers have the ability to add or delete financial records and access multiple programs.*
3) *Admin. Admin has additional permissions that allow for the management of users.*

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

The original review and approval of the SSPP was performed by the Defense Human Resources Activity Enterprise Operations Center (DEOC) DEOC Cybersecurity Team Assessment Report May 24, 2019. The SSPP has been updated and shared with DoD customers regularly. CI Travel has updated the CI Travel Back Office Enclave (CBOE) SSPP using the GSA provided template. Approval of that SSPP is pending GSA's review and assessment.

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

CI Travel Back Office Enclave (CBOE) leverages 24x7 by cipher locks and video surveillance to protect the physical entry to the office. The office includes video surveillance to monitor space access.CI Travel Back Office Enclave (CBOE) Firewall provides logical security by enforcing network perimeter security. CI Travel Back Office Enclave (CBOE) uses FortiGate Next Generation Firewall appliances to establish a network perimeter. The Corporate Technology Team uses the Auvik Network Monitoring system to identify real-time network activity across the company.

CI Travel uses the Arctic Wolf Managed Detection and Response (MDR) and Risk Management platforms to provide security incident and event management (SIEM). In the unlikely event that an unauthorized access attempt of CI Travel computing resources results in a breach, CI Travel holds breach insurance to ensure viability to continue to serve company customers and to ensure available resources to recover from the breach.

Personnel security approach is tiered to build knowledge through training to establish trusted protectors of sensitive customer data. CI Travel conducts background investigations to ensure that only verifiable US Citizens without criminal history and without financial risk join the organization. Every employee then receives introductory training to review the company's

privacy policies and how to secure customer data. This also includes cybersecurity topics of phishing, social engineering, malware, and device security.

CI Travel Back Office Enclave (CBOE) uses encryption at rest to encrypt PCI, PII and PHI stored on file servers, storage appliances and in databases. CI Travel stores data based on retention requirements of each customer. The system administrators configure retention rules with both operational and backup data stores. CI Travel staff destroys data securely in accordance with the Data Destruction Policy and includes secure shredding services for hard copy information and physical destruction for computing hard drives and peripherals.

System administrators have configured access to CI Travel's Microsoft Domain using Multi-Factor Authentication (MFA) to ensure there are two methods to prove users' identity. The Identity and Access Management policy defines user account management policies, password configuration, and MFA enrollment. This policy also describes the controls of system and data access based on a user's need to know to include a user's role and the CI Travel Department (Federal, Business and Leisure). Data Loss Prevention (DLP) software runs in the company's Microsoft tenant leveraging rules that analyze data structures and packets to ensure the encryption of PII and PCI data fields.

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?

CI Travel Back Office Enclave (CBOE) follows an Incident Response plan in the event of a data breach. If a breach is confirmed and involves customer Personally Identifiable Information (PII), CI Travel Back Office Enclave (CBOE) leverages its breach response in which includes the submission of security incident reporting forms to notify the proper authorities and cyber insurance company in accordance with its Incident Response plan and GSA contract instructions.

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.

Individual information is required to book travel. Thus in accordance with CI Travel (CIT) and Global Distribution System (GDS) privacy policies users may opt out by not choosing to provide

Personally Identifiable Information (PII) or Payment Card Information (PCI) for booking purposes. However, refraining from providing this information would render CIT unable to process a booking transaction as personal details are required for reservations and ticketing. Once the user provides details for the booking, traveler name and credit card number are required to remain in CI Travel Back Office Enclave (CBOE) for accounting purposes for 10 years for historic business, customer and contract financial reporting requirements. This information is shared with Airline Reporting Corporation (ARC), the non-profit company that provides ticket transaction settlement services between airlines and travel agencies (both traditional and online) and the travel management companies that sell their products in the United States.

6.2 What procedures allow individuals to access their information?

Travelport does document "Right to request access to your personal data – you have the right to request access to the GDS Personal Data we hold about you" within their privacy policy at this location. https://www.travelport.com/privacy

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

Travelport does document "Right of Rectification – you have the right to request correction of the GDS Personal Data that we hold about you where it is incomplete or inaccurate." within their privacy policy at this location. https://www.travelport.com/privacy

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 CI Travel new hires receive 2-hour of cybersecurity training and awareness from the Chief Information Officer (CIO) upon starting with CI Travel. This training includes the definition of Personally Identifiable Information (PII) or Payment Card Information (PCI) and requirements for securing that information, threat protection, acceptable use, and incident management. Each year the organization completes annual awareness training. Other awareness activities include phishing simulations, SharePoint posts and occasional emails to the 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?

Access to CI Travel Back Office Enclave (CBOE) is only provided with a Need to Know which is established by the Chief Financial Officer (CFO) at time of hire. The user's account is then provisioned with least privilege reserving the elevated privileges for administrators and managers of the accounting team. The Director of Accounting and CFO oversee the annual account reviews and annual password change process for the Trams system used to modify CBOE information. Non Disclosure Agreements (NDAs) are used as administrative controls to ensure that external reporting systems (Grasp) do not share data with third parties. Audit controls include the oversight of technical assets using Arctic Wolf's Managed Detection and Response (MDR) and Risk Management platforms. Agents reside on servers and workstations that prevent data exfiltration. The Risk Scanner performs scans of all servers which assist with ensuring operating system software is regularly patched. Penetration Testing occurs annually, internal audits are performed in years when a formal audit is not planned.