Duluth Travel Network (DTN) - PIA

Privacy Impact Assessment (PIA) - Guidance

POINT of CONTACT

privacy.office@gsa.gov

Version 1.4: 5-27-2022

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, of GSA Information System Security Manager (ISSM):

X DocuSigned by: Arpan Patel 8B059AABDAF1477... 5/5/2026 | 18:35:11 BST

GSA Information System Security Manager

Michael Salter, of GSA Program Manager:

X DocuSigned by: Michael Salter ABA02A5B3FBB446... 5/5/2026 | 18:42:01 BST

GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X DocuSigned by: Richard Speidel 171D5411183F40A... 5/5/2026 | 18:56:31 BST

GSA Chief Privacy Officer

Janelle Scribner, of GSA Contracting Officer Representative (COR):

X DocuSigned by: JANELLE SCRIBNER B587777B86134FE... 5/6/2026 | 15:17:41 BST

GSA Contracting Officer Representative

800-171 PIA Template Document Revision History

Date	Description	Version of Template
06/10/2020	Initial Draft of Non-Federal System PIA	1.0
08/05/2020	Version for rideshare vendors	1.1
10/20/2020	General updates for broader template usage	1.2
08/03/2021	Formatting and made 508 compliant	1.3
5/27/2022	Formatting and editing	1.4
4/29/2026	Privacy Office review and updates requested	1.5
5/04/2026	Privacy Office final revision	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:

Duluth Travel Network (DTN)

B. GSA Client:

Duluth Travel

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

The Duluth Travel Network maintains information on government employees using DTN services for business travel.

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

The Duluth Travel Network maintains traveler names, travel information, and financial information necessary for charging for travel. A more detailed list of maintained formation includes the following:

- Name and other biographic, demographic, or biometric information (e.g., date of birth, age, gender, race, height, fingerprints, photos, or video);
- Contact information (e.g., address, telephone number, email address);

[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."

- Social Security Number (SSN), Driver's license number, passport number, or other government-issued identifiers or images of documents, etc.;
- Financial Information (credit card/Payment Card Information (PCI), bank routing, tax identification number (TIN), etc.);
- Other Information - disability status and any specific medical or dietary needs.

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

The Duluth Travel Network (DTN) provides advanced and reliable travel management services for government clients. The DTN, in coordination with the government's ETSNext (now Go.gov) travel program and related information systems, maintains information on reservations, fees/fares, accounting, travel history, and similar travel information.

The DTN maintains personal contact and demographic information on travelers. Travel data is transferred from the government's ETSNext (now Go.gov) program, and maintained using secure storage, transmission, and processing controls. Sensitive information is used solely by Duluth for travel scheduling, billing, and related purposes. Data is retained and disposed of in accordance with approved data retention guidelines.

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.

Duluth mainly receives information from the government's ETSNext (now Go.gov) system, and to a much lesser extent, directly from travelers. Duluth relies on and supports the privacy notices of government systems, and the notices provided to travelers by the government for notifying users of data collection. Duluth also maintains a privacy policy, posted on the Duluth website at https://duluthtravel.com/privacy-policy/, which covers subject sensitive data collection, use, and maintenance.

SECTION 2.0 DATA MINIMIZATION

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

The collection of PII is necessary to facilitate travel reservations and services for those requesting the services. Collection also assists in maintaining visibility into the locations and travel status of traveling individuals, and assists with supporting emergency services.

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

Yes. The Duluth Travel Network features strong duty of care tracking processes which allow Duluth and authorized individuals to verify the travel status and safety of travelers. This is a commonly provided function in the travel industry.

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

Reports include individual and organization-based summary reports on various aspects of travel and billing information. Additionally, Duluth offers duty of care tracking processes to verify the safety and travel status of individual travelers, available only to authorized personnel.

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?

Duluth generally does not de-identify data for reporting purposes, but will offer summary and detailed reports to authorized client representatives as needed for billing, accountability, and travel status purposes. Most reporting is used to support and improve internal processes, and is not shared outside of Duluth.

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?

Sensitive information is provided to Duluth from the government's ETSNext (now Go.gov) travel program as needed to support active requests for travel reservations. Where needed, the provided information is augmented via phone conversations with travelers to complete the requested reservations. Transferred and collected sensitive information is available only to travel agents on an as-needed and minimum necessary basis in order to complete the requested reservations, or to provide related services. Access rights to sensitive information are always restricted on a business-need-to-know basis.

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?

Travel information is always available to the travelers who are the information subjects. Federal agencies are provided summary and detailed reporting on travel for the agency's employees for the purpose of billing for travel services. Duty of care information is provided to authorized persons when required. The government's ETSNext (now Go.gov) travel program has full access to all sensitive information. Duluth internal and external auditors may have supervised access to sensitive information for the purposes of confirming compliance with program or security requirements. Other than what is described in this paragraph, no other organizations, governments, or individuals are granted access to Duluth sensitive data.

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)?

Duluth transfers sensitive information from the government's ETSNext (now Go.gov) program, and to a lesser extent also collects information from the data subjects.

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

The source of most sensitive information has been discussed above. Travel data is created by agents who enter or change travel information to complete traveler requests. Travel information

is verified by receiving travel agents, by travel company verification processes, and by quality control processes within Duluth.

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?

Only authorized Duluth travel agents and managers will have access to sensitive information in the Duluth Travel Network. Agents have direct access to sensitive information for travel reservation scheduling and maintenance purposes. Managers have access to travel information for management, verification, and agent performance evaluation purposes. Some automated processes are used to transfer information to and from the government's ETSNext (now Go.gov) program information systems. Duluth employees are screened with background checks, and authorized by management to access job-relevant data. Periodic access control reviews are used to verify only authorized personnel are granted access to the Duluth Travel Network. There is a review and approval process used for establishing sharing or system links, which must be justified to be needed for valid business purposes. Access to sensitive data is promptly terminated when employees leave Duluth, transfer away from relevant job responsibilities, or are judged to no longer meet Duluth security and/or ethics standards.

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

The SSPP (Rev 3, Version 2) was submitted to GSA in February 2026. The final version was provided on May 4 2026.

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

Physical security for production infrastructure is inherited from Microsoft Azure data center controls, which maintain SOC 2 Type II certification. The Duluth administrative office in Duluth, Georgia uses key-controlled access. Technical controls include: identity and access management through Microsoft Entra ID with conditional access policies requiring multi-factor authentication; endpoint management and compliance enforcement through Microsoft Intune; 24/7 security monitoring via Barracuda XDR Security Operations Center; endpoint detection and response through SentinelOne on all managed workstations and servers; vulnerability scanning

via Qualys; encrypted backup through Cove Data Protection (TRAMS/Azure) and Barracuda (Microsoft 365); and TLS 1.2/1.3 encryption for all external service connections. Access to the TRAMS back-office accounting system requires Azure VPN connectivity with Entra ID MFA at the identity layer. From a management perspective, the VP of Operations and Product and the CTO of the managed service provider (Genesis) regularly review the effectiveness of technical and administrative security controls and report to executive leadership.

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?

Duluth Travel maintains a formal Incident Response Policy and Plan (Version 26.0, approved 22 January 2026) that defines roles, responsibilities, escalation procedures, and coordination protocols for security incidents affecting the authorization boundary. The Incident Commander (VP of Operations and Product) has authority to declare incidents, authorize containment actions, and approve external notifications including to GSA and Contracting Officers. The managed service provider (Genesis) executes technical response actions under Incident Commander authority, supported by 24/7 monitoring from the Barracuda Security Operations Center and SentinelOne endpoint detection. The plan was validated through a tabletop exercise conducted on 30 January 2026, which simulated an email account compromise involving potential unauthorized access to CUI. Anti-malware protection, intrusion prevention, and automated alerting are maintained across all managed endpoints. The incident response plan integrates with the Business Continuity Plan and Disaster Recovery Plan. Post-incident reviews are conducted for all significant incidents, with lessons learned documented and corrective actions tracked through the Plan of Action and Milestones process.

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.

Government agency travelers may refuse to provide information to Duluth or to the government's ETSNext (now Go.gov) program information systems. However, if key information is not provided, travel services may be refused.

6.2 What procedures allow individuals to access their information?

Travelers and agencies may request details on information being maintained by Duluth. Such requests are evaluated for appropriateness, and where requests are legal and appropriate,

Duluth provides access to the requested information. Information on what data is collected and how that data is used may also be found in the Duluth privacy policy, posted on our website.

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

Individuals may amend information about themselves. Where Duluth has collected the information, or for select information on individual travel requests, modifications are made by Duluth. Where information is kept by the government's ETSNext (now Go.gov) program information systems, the customer is referred to their travel profile to make the appropriate modifications.

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.

Duluth staff are provided annual and periodic privacy and security awareness training. Privacy training covers:

- Recognizing sensitive information.
- Rules on who may access sensitive information and under what circumstances,
- Understanding how to protect sensitive information.
- Identifying sensitive information data breaches and reporting those breaches to the correct Duluth representative.
- Notice of Duluth monitoring and accountability processes for sensitive data usage.

Training completions are both required and documented, and employees verify annually that they understand and will follow the sensitive data protection requirements as a condition of employment with Duluth.

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?

Users are restricted to accessing only data necessary to complete their job responsibilities. Supervision and training are used as a primary means of ensuring correct sensitive data handling. Data monitoring and user monitoring are used to verify compliance with policies on data use and protection. Periodic audits are used to verify control measures are appropriate and sufficient for their intended purposes. Separation of duties is used for key functions to ensure one individual cannot act independently to negatively impact security functions. External audits are periodically provided by qualified third party auditors specializing in data protection and cybersecurity controls. Internal audits are periodically conducted by management and supervisors who are trained in company policy and data protection practices.

Certificate Of Completion

Envelope Id: 119554DA-6023-89C0-8382-4836EAF72074
Status: Completed
Subject: Complete with Docusign: Duluth-PIA.pdf
Source Envelope:
Document Pages: 14
Signatures: 4
Certificate Pages: 2
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London

Envelope Originator:
Tiwalade Adebanjo
1800F F St NW
Washington DC, DC 20405
tiwalade.adebanjo@gsa.gov
IP Address: 136.226.21.19

Record Tracking

Status: Original
5/5/2026 6:28:09 PM
Security Appliance Status: Connected

Holder: Tiwalade Adebanjo
tiwalade.adebanjo@gsa.gov
Pool: FedRamp

Location: DocuSign

Signer Events	Signature	Timestamp
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: 136.226.19.87	Sent: 5/5/2026 6:33:00 PM Viewed: 5/5/2026 6:35:03 PM Signed: 5/5/2026 6:35:11 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
JANELLE SCRIBNER janelle.scribner@gsa.gov Program Analyst US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: JANELLE SCRIBNER B587777B86134FE... Signature Adoption: Pre-selected Style Using IP Address: 136.226.19.88	Sent: 5/5/2026 6:33:01 PM Viewed: 5/6/2026 3:17:02 PM Signed: 5/6/2026 3:17:41 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Michael Salter michael.salter@gsa.gov Program Analyst US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Michael Salter ABA02A5B3FBB446... Signature Adoption: Pre-selected Style Using IP Address: 136.226.20.178	Sent: 5/5/2026 6:33:00 PM Viewed: 5/5/2026 6:41:50 PM Signed: 5/5/2026 6:42:01 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: 136.226.18.206	Sent: 5/5/2026 6:33:01 PM Viewed: 5/5/2026 6:56:04 PM Signed: 5/5/2026 6:56:31 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

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/5/2026 6:33:02 PM
Certified Delivered	Security Checked	5/5/2026 6:56:04 PM
Signing Complete	Security Checked	5/5/2026 6:56:31 PM
Completed	Security Checked	5/6/2026 3:17:41 PM

Payment Events	Status	Timestamps