U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary of Transportation (OST)

Office of Financial Management (B-30)

Delphi

Responsible Official

Daniel King
Deputy Chief Financial Officer (OST B1)
Email: daniel.king@dot.gov

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Department of Transportation (DOT) Office of Financial Management (B-30) is responsible for managing, accounting, and reporting financial transactions across DOT. To fulfill these responsibilities, B-30 uses Delphi, its core financial management system, which supports accounting and financial reporting for DOT and other federal agencies on a fee-for-service basis**.**

This Privacy Impact Assessment (PIA) is conducted in accordance with the e-Government Act of 2002**,** as Delphi collects Personally Identifiable Information (PII) from members of the public and federal employees during its operations.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

Delphi is the DOT's implementation of the Oracle Enterprise Business Suite (EBS) Commercial Off-The-Shelf (COTS) software. It is a financial management system that provides its users with the ability to enter, search, browse, maintain, share, classify, register, and standardize financial transactions through a web-based application.

Delphi is the backbone of the Department's financial system and supports the agency's business objectives of paying vendors, receiving payments from or providing payments to state and local organizations, and completing payroll accounting. It reduces program exposure to various sources of risk and automates, streamlines, and standardizes financial processes, providing accurate financial results. Use of Delphi promotes Departmental efficiency and effectiveness by providing:

- One system and 14 sets of financial records shared by all DOT Operating Administrations (OAs), regions, centers, and headquarters.
- Ability to share and extract information and data from a common source.
- Improved financial statements and reports enhanced credibility so that Department's financial information is viewed as more trustworthy, reliable, and professionally produced by key oversight bodies — specifically Congress, OMB, and Treasury.
- Streamlined business processes.
- More accurate and timely information available to management for decision-making.
- More flexibility for program and accounting managers to report financial information.
- Clear lines of responsibility and accountability on projects that improve the Department's ability to measure program effectiveness.
- Accurate cost and lifecycle asset valuations.
- Financial statements produced directly from system.

External non-DOT Federal agencies also use Delphi on a fee-for-service basis. It provides financial management and accounting functions to include obligations, payables, inventory, general ledger, financial reporting, budgeting, project costing, billing, and customer and asset management. The non-DOT agencies are customers of the Delphi solution; each OA and non-DOT Federal organization has its own segregated set of financial records within Delphi. By placing the system on the Federal Aviation Administration (FAA)

Telecommunication Infrastructure (FTI) network and by supporting Internet connectivity, Delphi enables DOT OAs and other users with a browser-enabled workstation to remotely access the full range of system capabilities. Delphi is hosted and maintained by DOT's shared services provider, the Federal Aviation Administration (FAA) Enterprise Services Center (ESC), located in Oklahoma City, OK.

In managing accounting functions for the department's customers Delphi may contain PII of customers, employees, contractors and vendors including:

- **Personal and professional Contact Information:** name, address, phone/cell/fax number, email address is used to facilitate communication with individuals who may be users of the system, or the subject of a transaction managed by the system.
- **Financial Information:** banking numbers such as government credit cards and individual/vendor checking account number, tax identifiers including Employer Identification number (EIN) or Tax Identifier Number (TIN) are used to perform financial management and accounting functions to include procurement, payables, billing.

In addition to the PII collection noted above, the Department's use of Delphi may also include the following PII:

- **Personal Identifiers:** Date of Birth, Social Security Number (SSN) use to support employee payments including payroll and reimbursement and vendor payments associated with entities established as an Individual.

PII may be collected for purposes such as:

- Processing payments to and from vendors, contractors, individuals, and other entities
- Managing financial transactions with state and local governments
- Supporting payroll, benefit, travel, and accounting functions for federal employees

Delphi interfaces with human resources systems to access necessary employee data for accurate payroll processing. It also collects vendor contact and banking information to ensure timely and accurate payments. PII is collected only when required to establish and maintain an accounting relationship with DOT.

Access for each user organization is restricted to its own financial data on the Delphi system. Each user organization is required, on a semi-annual basis, to approve its active user list and the access rights and privileges assigned to each user.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a

framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Employee and individual records in Delphi are retrieved by unique identifier linked to an individual and are protected under the Privacy Act. General accounting records stored in Delphi are linked via system identifiers based on transaction type. All forms used to collect information stored in Delphi are approved by the Office of Management and Budget (OMB) and include appropriate Privacy Act notices. The Department has published a Privacy Act system of records notice (SORN) DOT/ALL 7 - DOT Financial Management Records (90 FR 55335, December 2, 2025) for the records maintained in the system exclusively for the purposes of executing Department's financial activities and its responsibilities as a Federal Shared Service Provider (FSSP).

The records associated with individual access and use of the Delphi system, including those of the department's customers are managed in accordance with DOT/ALL 13 - Internet/Intranet Activity and Access Records (67 FR 30757, May 7, 2002).

The Department's FSSP customers are responsible for issuing their own Privacy Act notices for their information maintained in Delphi and for providing copies of those notices to the Department to support use and access to their records.

The publication of this PIA further demonstrates DOT's commitment to providing appropriate transparency into Delphi. Individual's wishing to inquire about the PII or understanding DOT's personal information handling practices or contact privacy officials to address privacy concerns can visit the Department's privacy office website at https://www.transportation.gov/privacy.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Subject to the limitations of the Privacy Act, individuals may request access to information about themselves contained in a DOT system of records through Department's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of Delphi to determine if any records have been added that may pertain to them. The Privacy Act applies to information that is maintained in a "system of records." A system of records is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying information assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DOT extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of Department by complying with Department Privacy Act regulations, 49 CFR part 10.

The Department will review all Privacy Act requests on an individual basis and may as appropriate, waive applicable exemptions if the release of information to the individual would not detrimentally impact on the law enforcement or national security purposes for which the information was originally collected or subsequently being used. Privacy Act requests for access to an individual record must be in writing. Department policy requires in the inquiry, the name of the individual, mailing address, phone number or email address, and a description of the records sought, and if possible, the location of the records. Requests should be submitted for the attention of the official responsible for the record at the address below:

Privacy Act requests may be addressed to:

Office of Financial Management
Delphi System Owner
1200 New Jersey Ave., SE
Washington, DC 20590
Email: privacy@dot.gov

Your request must be in writing and include the following information:

- Provide your name, address and telephone number. Also, if you have an e-mail address, please provide it, so that we can contact you if we have questions about your request.
- Specify whether you are making a Freedom of Information Act (FOIA) or Privacy Act (PA) request.
- Provide as much detail as possible about the records you seek.
- Indicate whether you are requesting the information in a form or format other than paper.
- State your willingness to pay any fees, and how much you are willing to pay as advance authorization Privacy Act requests for records covered by system of records notices not published by the Department will be coordinated with the appropriate customer privacy official and acted upon accordingly.

Individuals may also submit a request online via the DOT Public Access Link (PAL) at https://pal.dot.gov/. Requests submitted through these electronic channels must include a digital certification of identity.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

The Department must manage its finances and account for those financial transactions undertaken in support of its mission. In addition to managing its own accounting of financial transactions, the Department provides accounting services to other Federal agencies, as authorized by the U.S. Department of Treasury's Office of Financial Innovation and Transformation and OMB Memorandum M-18-08, *Improving Financial Systems Through Shared Services*. The Department uses Delphi to control and facilitate the accounting and reporting of financial transactions for the Department and its Federal agency customers.

Data Minimization & Retention

DOT should collect, use, and maintain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

The primary basis of information collection in Delphi is OMB authorized government-wide forms used to support federal financial activities.[4] Categorized into Payments and

[4] See Appendix A for the forms most commonly used in Delphi transactions.

Receivables[5] these forms have been reviewed by OMB and the information collection deemed necessary for the execution of the activity for which they were created.

Unless otherwise authorized by customer specific records retention schedules, records in Delphi are retained in accordance with the following National Archives and Records Administration (NARA).

Item	Records Description	Disposition Instruction	Disposition Authority
General Records Schedule (GRS) 1.1: Financial Management and Reporting Records			
001	**Financial management and reporting administrative records.** Records related to managing financial activities and reporting. Records include: • correspondence • subject files • feeder reports • workload management and assignment records	**Temporary.** Destroy when 3 years old, but longer retention is authorized if needed for business use.	DAA-GRS-2016-0013-0001
010	**Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.** Many records included in this item are maintained by accountable officers to account for the availability and status of public funds, and are retained to enable GAO, Office of Inspector General, or other authority audit. Financial transaction records include those created in the course of procuring goods and services, paying bills, collecting debts, and accounting for all finance activity, per the following definitions.	**Temporary**. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.	DAA-GRS-2013-0003-0001

[5] Payments includes reimbursements of federal funds, via a variety of mechanisms, to federal and private individuals, federal agencies, state, local and international governments, and the private sector, to effect payment for goods and services. Or distribute entitlements, benefits, grants, subsides, or claims [to include medical]. Receivables include (including **c**ollections and receivables include deposits, fund transfers, and receipts for sales or service, as well records documenting events, associated with collections and receivables activities as described in the U.S. Government ledger Account Transaction Categories.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

Delphi access is strictly limited to authorized personnel, including DOT employees and contractors, and non-DOT agency employees and contractors, based on approved agreements. Access is provisioned based on role-based authentication and a verified need-to-know to perform financial management or reporting functions to support business operations. DOT enforces strict policies, including user responsibilities for handling information and validating need-to-know, to prevent unauthorized access or disclosure.

PII within Delphi is processed solely for the purposes for which it was collected. Secondary sharing or use of Delphi data is prohibited.

The Department discloses Delphi records to external parties only in accordance with Privacy Act authorizations and the system of records notice titled, DOT/ALL-7- DOT Financial Management Records (90 FR 55335), December 2, 2025:

- Disclosure of information to the U.S. Department of Treasury relevant to review payment and award eligibility through the Do Not Pay Working System for purposes of identifying, preventing, or recouping improper payments.
- Disclosure of data to external systems must be approved through an authorized data sharing agreement.
- Additional routine uses for this system can be found in the published notice.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s)

All Delphi system components are COTS software which are furnished with data quality controls. System monitoring controls are in place at the network and application tiers to detect and notify if malicious activity has been detected. The system utilizes system audit controls to check the integrity of files to ensure that there has not been any malicious activity by means of installing or altering files. In the event of malicious code detection, the applicable code/file is quarantined, and an administrator is notified. PII in Delphi may be information provided on invoices, forms or other documents, authorized users submitting PII into Delphi are responsible for ensuring the accuracy and completeness of submitted

information. In addition, Delphi performs data validation on information stored in the system.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for Federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53 Rev. 5, Recommended Security Controls for Federal Information Systems and Organizations, dated September 2020. The Department has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII.
- Protect against unauthorized access to or use of PII.

Delphi records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls are implemented to minimize the risk of compromising the information that is being stored. Access to the computer systems containing the records in Delphi is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. Delphi is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

Logical access to the system is guided by the principles of least privilege and need to know. Role-based user accounts are created with specific job functions allowing only authorized access that are necessary to accomplish assigned tasks in accordance with operational needs and business functions of the system. Any changes to user roles require approval of the FSSP customer Access Control Officer (ACO) and the user's manager.

The Department maintains an auditing function that tracks all user activities in relation to data including access and modification. Technical security controls include firewalls,

intrusion detection, encryption, access control lists, and other security methods. Department personnel and contractors supporting the system are required to attend security and privacy awareness training and role-based training offered by the Department. No access will be allowed to Delphi prior to receiving the necessary clearances and security and privacy training as required by the Department. All users must agree to and accept the Standard Federal Warning Banner before gaining access to the Delphi system. The DOT federal users are required to read/acknowledge and electronically sign annual Rules of Behavior (ROB). A ROB for non-DOT users is handled by each external user agency based on their established protocol for accessing IT Systems.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

The Department follows the Fair Information Principles as best practices for the protection of information associated with Delphi. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees will be given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance will be provided in the form of mandatory annual Security and Privacy Awareness training as well as acknowledging the Rules of Behavior. The Department Chief Privacy Officer will conduct regular periodic security and privacy compliance reviews of Delphi consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 5a.1) a) i, ii, Managing Information as a Strategic Resource.

Responsible Official

Daniel King
Deputy Chief Financial Officer (OST B1)
daniel.king@dot.gov

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.07.13 13:54:34 -04'00'

Appendix A – Delphi Forms

The following forms are typical information collection instruments used to collect data maintained in Delphi.

- FS (Fiscal Service) Form 7600A US Government Inter-Agency Agreement
- FS Form 7600B US Government Order Form
- GSA (General Services Administration) 276 Supplemental Lease Agreement
- GSA 3557-13 Relocation Income Tax Allowance (RITA) Claim & Tax Status Certification
- GSA 3626 U.S. Government Lease for Real Property Short Form
- OF (Optional Form) 1164 Claim for Reimbursement for Expenditures on Official Business
- OF 347 Order for Supplies and Services
- OF 1012 Travel Voucher
- SF (Standard Form) 1012 Travel Voucher
- SF 1034 Public Voucher for Purchases and Services Other Than Personal
- SF 1038 Advance of Funds Application and Account Award
- SF 1047 Public Voucher for Refunds Award
- SF 1080 Voucher for Transfer Between Appropriations and/or Funds Award
- SF 1081 Voucher and Schedule of Withdrawals and Credits Award
- SF 1103 U. S. Government Bill of Lading
- SF 1113/A Public Voucher for Transportation Charges Award
- SF 1145 Voucher for Payment Under Federal Tort Claims Act Award
- SF 1154 Public Voucher for Unpaid Compensation Due a Deceased Civilian Employee Award
- SF 1156 Public Voucher for Fees and Mileage Award
- SF 1164 Claim for Reimbursement for Expenditures on Official Business Award
- SF 1199A Direct Deposit Sign-Up Form
- SF 1449 Solicitation/Contract/Order for Commercial Items
- SF 182 Authorization, Agreement and Certification of Training
- SF 26 Awards/Contracts
- SF 270 Request for Advance or Reimbursement

- SF 271 Outlay Report and Request for Reimbursement for Construction Programs
- SF 30 Amendment of Solicitation/Modification of Contract
- SF 95 Claim for Damage, Injury, or Death