



U.S. Department of Transportation
Privacy Impact Assessment
Office of the Secretary of Transportation (OST)
Office of Financial Management (B-30)
Delphi

Responsible Official

David Rivait
DOT Deputy Chief Financial Officer
Office of Financial Management
202-493-0476

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

12/29/2014

X Claire W. Barrett

Claire W. Barrett
Departmental Chief Privacy & Information Ass...
Signed by: CLAIRE W BARRETT



Executive Summary

In response to the Office of Management and Budget's (OMB) Memorandum M-13-08, *Improving Financial Systems Through Shared Services*, the Treasury Department's Office of Financial Innovation and Transformation (FIT) has partnered with the Department of Transportation (Department) to facilitate government agencies' use of shared services for financial management. As a Federal Shared Service Provider (FSSP) the Department's Office of the Secretary/Office of Financial Management has engaged the Federal Aviation Administration's (FAA) Enterprise Services Center (ESC) and Delphi service offering. This Privacy Impact Assessment (PIA) was conducted because the financial transaction information may include personally identifiable information, for purposes such as paying vendors, receiving payments from or providing payments to state and local organizations, and completing payroll accounting activities. Delphi also interfaces with HR systems, to gather information necessary to record employee pay appropriately. Likewise, Delphi collects contact and payment information from vendors in order to appropriately process payments. The Delphi system collects PII only when an individual requires an accounting relationship with DOT. The Delphi system is supported by the ESC Enterprise Service System (ESS), the PIA for which may be found the Department's privacy program website – www.dot.gov/privacy.

Introduction & System Overview

OMB's Memorandum M-13-08 directs agencies to: move from agency-specific financial systems to FSSPs, consolidate financial management systems use existing FSSP operations and maintenance teams to support systems and infrastructures. The Office of the Secretary's (OST) Office of Financial Management (B-30) owns and the FAA's Enterprise Service Center (ESC) provisions the Delphi environment that provides financial services to aid the Department and its FSSP customers in meeting current and future financial mission requirements.

Delphi is a financial management and data repository system that provides its users with the ability to search, browse, maintain, share, classify, register and standardize financially administered items through a web-based application. A single database instance supports all of Delphi's customers.

The core of Delphi is the Oracle Federal Financials Commercial Off-The-Shelf (COTS) consisting of the following modules; General Ledger, Accounts Receivable, Accounts Payable, Purchasing, Fixed Assets, Assets, Projects, Payments, Sub Ledger, iSupplier Portal, Federal Financials (including the Budget Execution Module and Federal Administrator modules), and Federal Financial Statements.

In addition DOT makes the following Oracle applications and modules available to its customers;

- **Discoverer** - An ad-hoc querying, reporting, analysis tool of the Delphi data.
- **Web Reports** - Provides custom-developed reports that provide Delphi users with financial information.
- **MarkView** - Allows users to view and use electronic images of any size or type on their computer.
- **Tutor** - Serves as the online Delphi user's guide.
- **ESC PRISM** - Supports the complexities of federal acquisition by tracking the progress of acquisitions through the stages of procurement and providing reporting capability of critical data for internal and external requirements.
- **Oracle Business Intelligence Enterprise Edition (OBIEE)** - users are limited to creating predefined and programmed custom reports. Reports are read only.

- **iSupplier** - an electronic invoicing system replacing the manual submission of paper invoices for payment requests for grants with an automated, on-line solution.
- **Governance, Risk, and Compliance (GRC)** - enforces segregation of duties, reduces fraud, prevents information spillage, provides configuration management, and enforces the principles of least privilege and functionality throughout Delphi's Oracle Federal Financials.

In managing accounting functions for the Department's customers Delphi may contain personally identifiable information (PII) of customer employees, contractor and vendors

- **Personal and Professional Contact Information:** (name, address, phone/cell/fax number, email address) is used to facilitate communications with individuals who may be users of the system, or the subject of a transaction managed by the system.
- **Financial Information:** (banking numbers [e.g., credit card, checking account number], tax identifiers [Employer Identification number (EIN), Tax Identifier Number (TIN)]) used to perform financial management and accounting functions to include procurement, payables, billing

Department of Transportation Use of Delphi

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, automates, streamlines, and standardizes financial processes, and provides accurate financial results. Use of Delphi promotes Departmental efficiency and effectiveness by providing;¹

- One system and 14 sets of books 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 (Congress, Office of Management and Budget (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 which will improve the Department's ability to measure program effectiveness.
- Accurate cost and lifecycle asset valuations.
- Financial statements produced directly from system.

¹ In order to achieve these outcomes the Department leverages the following Oracle Financial System modules within Delphi: Accounts Payable, Accounts Receivable, Budget Execution, Fixed Assets, General Ledger, Project Accounting, Purchasing, and Federal Financials

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 Numbers [SSN]) used to support employee payments including payroll and reimbursement.

Fair Information Practice Principles (FIPPs) Analysis

This DOT PIA template 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) v3², 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 Organizations³.

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.

Records in Delphi are retrieved by personal identifier linked to an individual and are protected under the Privacy Act. 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 - Departmental Accounting and Financial Information System \(DAFIS\) and Delphi Accounting System](#) (65 FR 19481, April 11, 2000) for the records maintained in the system exclusively for the purposes of executing Department's financial activities and its responsibilities as a FSSP. The SORN is being updated by the Chief Privacy Officer to more completely address the records maintained in the system. The updated SORN will be published in the Federal Register and on the Department's privacy program website, www.dot.gov/privacy.

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 provide 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 www.dot.gov/privacy.

² <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

³ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Individual Participation and Redress

DOT should provide 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 be provided 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 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 to the attention of the official responsible for the record at the address below:

Privacy Act requests may be addressed to:

Claire W. Barrett
Departmental Privacy Officer
1200 New Jersey Ave., SE
E31-312
Washington, DC 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

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 Public Access (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.

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 its collects, uses, maintains, or disseminates PII.

The Department must manage its finances and account for those financial transactions undertaken in support of support 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 retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The primary bases of information collection in Delphi are OMB authorized government-wide forms used to support federal financial activities.⁴ Categorized into Payments and Receivables⁵ 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 NARA published General Records Schedule (GRS) – [1.1 Financial Management and Reporting Records](#). This schedule covers records created by Federal agencies in carrying out the work of financial management: procuring goods and services, paying bills, collecting debts, accounting for all financial transactions, and monitoring agencies' net worth. Records are typically destroyed between 2 and 6 years after the completion of the specific activity for which the record was created.

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.

The Department discloses Delphi records to external parties accordance with applicable Privacy Act authorizations and notices including to 'consumer reporting agencies' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1982 (31 U.S.C. 3701(a)(3)).

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

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, subsidies, or claims [to include medical]. Receivables includes (including collections 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.

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 Commercially Off the Shelf (COTS) software which are furnished with quality control and accountability. System Administrators are notified if malicious activity has been detected. The system utilizes an audit device 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 a proposal, invoice, or other document and 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 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. 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009. 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 have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system 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 accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the system. Any changes to user roles required approval of the FSSP customer and the System 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 list, 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 at the federal and state level are made aware of the Rules of Behavior (ROB) for IT Systems prior to being assigned a user identifier and password and prior to being allowed access to Delphi.

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.

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to Department privacy and security policies and regulations. The Department will follow 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 Acceptable 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 8b(3), Securing Agency Information Systems.

Responsible Official

David Rivait
DOT Deputy Chief Financial Officer, B-2
202-493-0476
david.rivait@dot.gov

Approval

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

Appendix A – Delphi Forms

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

- [SF 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 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](#)

Appendix B – Internal Department Sharing

In support of the Department's own use of Delphi to manage its financial obligation Department data in Delphi may be shared with the following internal systems;

- **OST WCF RRDD** - Office of the Secretary of Transportation, Working Capital Fund, Resource Requirement Decision Data; a financial management system used to document budget formulation and develop the Working Capital Fund (WCF) budget and related operational plans during the federal fiscal cycle.
- **CASTLE/IR** - Consolidated Automation System for Time and Labor Entry and the Interface Repository; collects standard interface files plus additional data elements needed to satisfy DOT interfacing application requirements.
- **FAA PRISM** – Portable Reusable Integrated Software Modules; uses Delphi financial information to automate data quality assurance checks and to validate accounting information as well as to ensure funds are available before contracts are awarded.
- **NHTSA GTS** - National Highway Traffic Safety Administration, Grants Tracking System; used to track obligations and reimbursements for traffic safety grants from all United States.
- **FTA FMS** - Federal Transit Administration (FTA) Financial Management System (FMS), interface provides for the daily transmittal of financial data to and from Delphi and the FTA's feeder systems.
- **FHWA DIMS** - Federal Highway Administration, Delphi Interface Management System; interface provides accounts payable and obligations file transfers for processing.
- **Volpe FDM** - Financial Data Mart; populated by extracts of the Delphi system for reviewing and analyzing financial status of projects and tasks on a scheduled and ad hoc basis.