U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Financial Services (ABA)
Delphi Transaction File (DTF)

Responsible Official

William Lampiris
william.lampiris@faa.gov

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Office of Finance and Management (AFN) Office of Financial Services (ABA) Delphi Transaction File (DTF) serves as a centralized repository for the historical financial information used by other FAA's "downstream systems." The purpose of the system is to provide a single source of financial data to downstream systems so that they can perform budget, financial, and performance management functions. DTF maintains historical financial information in the event of requests or audits and interprets, validates, and stages this data so that other FAA downstream systems do not need to perform these tasks. DTF is authorized under 5 United States Code (U.S.C.) § 301.

The FAA is publishing this Privacy Impact Assessment (PIA) for DTF in accordance with Section 208 of the E-Government Act of 2002 because the system processes Personally Identifiable Information (PII) from members of the public who are businesses, vendors, and customers that do business with the FAA. There have been updates to the DTF system and the FAA is publishing this update to the DTF PIA.

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:

[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).

DOT Privacy Office Approved - 09/26/2024

- *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*
- *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.

DOT Privacy Office: Approved: 03/26/2024

Introduction & System Overview

Before the implementation of the Department of Transportation's (DOT) core accounting system, Delphi, the FAA allowed the transfer of accounting data to FAA Lines of Business (LOBs) systems independently. Upon receiving the account data from each LOB, the system owner had to build and apply account rules to the data before reporting was possible. What FAA experienced with this mode of data dissemination was that accounting rules were applied inconsistently across FAA systems causing financial reporting to be out of balance with the core accounting system, Delphi. This inconsistency with each LOB's financial reporting caused an undue burden on the FAA Office of Accounting, resulting in considerable time and effort in reconciling budgets and financial reports from each of FAA LOB's systems to Delphi.

To reduce the undue burden to the FAA Accounting Office, the FAA decided to centralize the distribution of Delphi financial data. This was accomplished by creating DTF where Delphi financial data would be transformed by applying consistent business and accounting rules that would balance back to the Delphi General Ledger. DTF was then offered to the LOBs as a single source of Delphi data.

DTF serves as a centralized repository of historical budget, financial, and performance management information for the FAA. The information is extracted from the DOT core accounting system, Delphi. While Delphi retains information for all the agencies in the DOT, FAA's DTF contains only financial information specific to the FAA. The FAA Office of Information Technology (AIT), Solution Delivery Systems Integration Division (ADE-300) operates DTF to store and provide a historical extract of budget, financial, and performance management data for the FAA. The overall objective of the DTF is to reduce the uncontrolled proliferation, processing, and storage of budget, financial, and performance data.

DTF financial data is offered to downstream systems that have a business need for the data. Access to DTF is provided via a service account for each system upon completion of a signed service agreement with the DTF System Owner. Only DTF system administrators have direct access to the DTF system and database. All other access is provided by a service account that has access to data based on what is authorized via the service agreement.

DTF contains PII from the following types of individuals (all PII comes from multiple system-to-system data exchanges[2] and is not collected directly from individuals):

Members of the Public (Businesses/Vendors/Customers that do business with the FAA):

- Business name/Point of Contact (POC) Name
- Business address
- Business phone number
- Financial account information (e.g., bank account number/routing number)

FAA Employees and Contractors (To manage the system, travel reimbursement, and FAA-issued Purchase Card (P-Card) use):

- Name/Card holder name
- Home address
- FAA or personal phone number
- Financial account information (e.g., bank account number/routing number)
- Last six digits of government-issued credit card number
- Delphi User ID

FAA Employee and Contract Workforce (for account access):

- Username
- Password
- FAA Email address

PII data enters DTF via a system-to-system transaction with Delphi and is the sole source of the PII data that is transferred and stored in DTF. Delphi provides an extract of the prior day's financial transactions every morning to DTF. DTF loads the financial transactions into the DTF database. The downstream FAA systems, with authorized access, have a system-to-system connection that automatically logs into DTF, obtains only the authorized data for that system, and automatically downloads the data to the downstream system.

DOT Privacy Office - Approved - 03/26/2024

[2] DTF has valid PII Data Sharing Agreements or MOUs covering these data exchanges.

DTF sends, receives, or exchanges data with the following downstream systems, i.e., "data subscribers":

- Cost Accounting System (CAS)
- Office of Information Technology Services Enterprise Data Repository (AIT
- EDR)
- Asset Inventory Tracking System[3] (AITS)
- Capitalization (CAP)
- Platform for Unified Reports for the Enterprise (PURE)
- System of Airports Reporting (SOAR)

Daily, DTF receives zipped files containing various extracts of DOT Delphi's financial data that include the following information:

- **Accounting** consists of financial information, such as general ledger transaction data and Ledger setups, Project Accounting, purchasing, and accounts receivable/payable.

- **Assets and Liability Management** consists of data about FAA assets, such as project number, project type, task, and asset location (state, city, and country). Asset data reflects the depreciation, retirement, transfer, adjustment, or reclassification of FAA assets and liabilities.

- **Budget Formulation** consists of accounting data, such as obligation balances, obligation status, and balance reports.

- **Collections and Receivables** consist of detailed accounting data, such as purchase orders, requisition numbers, invoice amount, receipt number, payment status, and method of payment. Accounts Payable transactions paid with a government credit card list the government cardholder's name and the last six (6) digits of the card. Accounts Payable transactions list the bank routing and account number of the vendor that is paid.

- **Cost Accounting/Performance Management** consists of accounting data, such as project number, project name, project status, and project type.

- **Funds Control** consists of financial information, such as transaction check number, date, payment method, Purchase Order (PO) number, expense amount, invoice number, payment number, amount remaining, pay status, requisition number, and authorization.

- **Payments** consist of payment records, such as non-payroll-related expenses, payment records for payroll made offline, and labor cost records.

DOT Privacy Office - Approved - 03/28/2024

[3] AITS is being replaced by FAA Real Estate and Asset Management Enterprise System (FRAMES).

- **User Fee Collection** consists of PII data, such as contact and banking information of those businesses, which could include the name of a point of contact for that business, that pay money directly to the FAA for services received. In addition, account name, location, payment method, expense category/type, terms of payment, invoice amount, and date comprise this category.

DTF provides access only to the above FAA systems that have a pre-arranged Provider Agreement. As a part of this Provider Agreement, the FAA systems set up what DTF data they require to access their system. PII sharing agreements cover these data exchanges. Policies, procedures, and practices for information storage, data use, access, notification, retention, and disposal are described here in this PIA.

DOT Privacy Office Approval: 03/26/2021

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,[4] 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.

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.

DTF is a privacy-sensitive system because it maintains, uses, disseminates, and retains PII from members of the public who are businesses, vendors, or customers that do business with the FAA and members of the FAA employee workforce for travel reimbursements and FAA-issued P Card activity. FAA downstream systems must sign a service agreement with

[4] https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

the DTF to receive the DTF data. Additionally, there are PII Data Sharing Agreements or Memorandums of Understanding (MOU) that cover these data exchanges.

All PII maintained in DTF, except the access and authentication data, comes from other systems and is not collected from the individual by DTF. All consent mechanisms, including Privacy Act Statements (PAS), are handled by the systems that collect the information.

DTF is not a system of records subject to the Privacy Act because it is not designed to be searchable by name, address, phone number, or any other PII field. Although those fields exist in the database, the system is designed to be searched by date. Additionally, substantive records are not retrieved by an identifier linked to an individual, and the records are not about individuals, and are therefore not subject to the Privacy Act. Additionally, a System of Records Notice (SORN) is not required because the system is not retrievable by PII. Records for login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the DTF program and/or manage the system are covered by SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

Lastly, the publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the DTF system and provides notice to the public as to the information management policies and practices related to this system.

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 reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

As previously discussed, DTF is a copy of the Delphi accounting system data for the FAA financial transactions. Information is transferred from Delphi and loaded into DTF as an automated electronic data feed. No data is entered into the system by any user. Individuals wanting to obtain redress should follow the procedure outlined in the Delphi system, which is detailed in the Delphi PIA located at URL https://www.transportation.gov/individuals/privacy/pia-delphi.

Additionally, DTF does not collect PII from any individual directly. FAA downstream systems must sign a service agreement with the DTF to receive the DTF data. There are no individual users of DTF.

DOT Privacy Office- Approved- 05/25/2024

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.

Congress has authorized the FAA Administrator to develop systems and/or tools that perform budget analysis, financial, and performance management functions. DTF addresses the unique demands of the FAA's workforce and operates under 5 U.S.C. 301. DTF maintains the information below, which is all from data exchange with Delphi, except system access and authentication PII, to support other downstream FAA financial systems. The data is used by the other systems interconnected with DTF, to perform analysis of budget, financial, and performance management functions. The purpose of DTF is to create a single source of financial data for FAA downstream systems. A key function of the DTF is the balancing back to the Delphi General Ledger to ensure consistency and accuracy in the financial data. The other objective of DTF is to reduce the number of system connections and MOU with Delphi.

DTF maintains the following PII from FAA employees and contractors for account access:

- Username
- Password

DTF maintains the following PII from Members of the Public (Businesses, vendors, and customers that do business with the FAA):

- Business name
- Business address
- Business phone number
- Financial account information (e.g., bank account number/routing number)

DTF maintains the following PII from FAA employees for travel reimbursements and FAA-issued P-Card purchases:

- Name
- Home address
- Work or personal phone number
- Financial account information (e.g., bank account number/routing number)
- Card holder name
- Last six digits of government-issued credit card number
- Delphi User ID
- Email address

DOT Privacy Office- Approved- 05/20/2024

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.

DTF maintains the minimum amount of information from individuals to support FAA's budget analysis, financial, and performance management programs. Information in DTF for the primary purpose of the system is covered under the National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.1, *Common Office Records*, July 2017, Item 20: Non-recordkeeping copies of electronic records. These records are temporary and should be destroyed immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.

General technology records are covered under NARA GRS 3.1, General Technology Management Records, November 2019, Item 20, *Information Technology Operations and Maintenance Records.* These records are temporary and should be destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

Information in DTF such as login credentials, audit trails, and security monitoring are retained until business use ceases in accordance with NARA GRS 3.2, *Information Systems Security Records, System Access Records*.

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 PII from members of the public (i.e., businesses, vendors, and customers that do business with the FAA) such as name, address, and phone number may be used by DTF in the performance of budget analysis, financial, and performance management. FAA employees' PII (name, address, phone number) is used for travel reimbursements and FAA-issued Purchase Card activity. The FAA does not use the PII for any other purpose.

The FAA/DOT limits the scope of information maintained in DTF to support the budget analysis, financial, and performance management functions. The DTF system controls access to data for each system through data views. Those data views are assigned to the service account. A system that enters into DTF via a service account only get access to the data via the data views assigned to them via the DTF agreement.

DOT Privacy Office - Approved 09/26/2024

The system does not retrieve records using a personal identifier. Access and authentication records within DTF are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

Finally, the FAA periodically reviews the collection, use, and disclosure of PII through its periodic review of this PIA and a Privacy Threshold Analysis (PTA).

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).

The DTF system is a copy of the Delphi accounting system data for the FAA financial transactions. Information is transferred from Delphi and loaded into DTF as an automated electronic data feed. No data is entered into DTF by any user. As such, data in DTF is assumed accurate when it is transferred from Delphi. As a part of the DTF automated data feed, the data is checked to ensure it is loaded properly from the source files. No verification is done regarding the accuracy of the data values in the source file other than what is provided by the Delphi accounting 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.

The FAA protects PII with 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 Security 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020 (includes updates as of Dec. 10, 2020).

In addition, DTF takes appropriate security measures to safeguard PII and other sensitive data including:

DOT Privacy Office - Approved - 03/26/2024

- DTF utilizes an Oracle database that encrypts the login process and stores the account passwords in an encrypted format.
- DTF utilizes Oracle to encrypt data at rest.
- AMI employs automated tools on the AMC Domain to identify technical vulnerabilities and manage system patches.
- Symantec Antivirus Corporate Edition (SAV CE), with the latest virus pattern signatures, protects the DTF's data and program integrity from problems introduced by malicious code.

The FAA Enterprise Network (ENET) security services defend against external threats (those originating from the Internet) thereby protecting the FAA internal network infrastructure. This significantly reduces the potential risks introduced by intentional human threats and malicious code threats originating from outside of the FAA's network. Implementation of various operational and technical controls assures user accountability, including annual user security awareness training, user acknowledgment and adherence to the Rules of Behavior, interconnection agreement, PII Data Sharing agreements, or MOUs with downstream systems, and the system administrators regularly reviewing the system/application logs for anomalous activity. There have been no known violations that would require disciplinary action to date.

In addition to the requirements of the FISMA, a security assessment was completed for DTF. The assessment process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years. All relevant policies, procedures, and guidelines, including NIST Special Publication 800-53, have been followed to ensure the security of the system and the information it contains.

DOT Privacy Office - Approved - 03/26/2024

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 DOT/FAA implements 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. Access to DTF PII is limited according to job function.

FAA Order 1370.121B, *FAA Information Security and Privacy Program & Policy*, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act),

the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, the FAA will implement additional policies and procedures as needed as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with DTF are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training, as well as FAA Order 1370.121B. The FAA conducts periodic privacy compliance reviews of DTF as related to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource.*

Responsible Official

William Lampiris
System Owner
IT Project Manager, Office of Information Technology, Solution Delivery, Information System Services

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2024.03.26 15:17:16 -04'00'

DOT Privacy Office - Approved - 03/26/2024