Privacy Impact Assessment for

DELPHI

October 23, 2025

Contact Point
Office of the Chief Financial Officer (OCFO)
Erick Borda
System Owner

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

Abstract

The United States Office of Personnel Management's (OPM) DELPHI system is a multi-tier, distributed financial management system supporting dynamic interoperability with other federal systems. DELPHI provides OPM financial and procurement management functions and is designated as the core financial management system for Salaries and Expenses and Revolving Fund business processes. DELPHI is used to create and maintain records of each commitment, obligation, expense, travel reimbursement, and accounts receivable issued and managed by the agency. This Privacy Impact Assessment is being conducted because DELPHI contains personally identifiable information about OPM employees, vendors, and customers who engage in OPM business operations.

Overview

DELPHI is the Office of Personnel Management's (OPM) core financial management system supporting all financial functions for OPM's Salaries and Expense and Revolving Fund business operations. It is a multi-tier, distributed financial management system supporting dynamic interoperability with other federal systems and resides in the Federal Aviation Administration (FAA) infrastructure.

FAA is the owner of the DELPHI system and is responsible for managing the DELPHI system. DELPHI resides in the FAA Enterprise Services Center (ESC), and ESC provides shared services to federal agencies.

DELPHI provides agency compliance with Federal proprietary and budgetary accounting and financial reporting requirements and is a comprehensive source of financial, budget, and performance information to OPM program offices. DELPHI records purchasing, accounts payable, accounts receivable, disbursements, and other integrated budget activities so the transactions, when processed, can update budgets, financial plans, and the general

ledger. DELPHI also performs Revolving Funds billing and collection, project costing, and funds control and offers the functions needed to consolidate financial reports and controls. Some personally identifiable information (PII) is required within DELPHI to support its primary business functions of recording and processing financial accounting records for the collection and payment of financial obligations made on behalf of OPM.

DELPHI includes two Commercial-Off-the-Shelf products that support OPM's core financial management operations. These are Oracle's Enterprise Business Suite (EBS) for Federal Financials and Unison PRISM.

EBS is a web-based Enterprise Resource Planning (ERP) system used by OPM to manage its core financial business processes for Salaries and Expense and Revolving Funds business operations on single integrated information architecture. The Oracle EBS modules used by OPM, and their purpose are described below:

- *Accounts Payable:* Tracks all information needed to record the expenditure and liquidation of agency funds properly.
- *Accounts Receivable:* Records, monitors, and controls all activities in the client's billing and collection process.
- *Automated Disbursements:* Allows OPM to disburse funds through the United States Treasury.
- *Budget Execution:* Automates the budget execution process by recording numerous budgetary-control levels and validates budgetary financial activity.
- *General Ledger:* Provides all the necessary financial postings for all transactions across all sub ledgers and provides a complete audit trail of transactions processed in DELPHI.

- *Project Cost Accounting:* Allows OPM to track project costs incurred, record reimbursable agreements, and distribute project costs to the agreements which are funding the projects, bill customers based upon terms of the agreement, and track billing and collection activity against agreements and projects.

- *Purchasing:* Supports the procurement process by tracking a purchase's financial and descriptive information from pre-commitment to funds to a vendor invoice.

- *Fixed Assets:* Allows OPM to track capitalized and accountable property from acquisition to disposal, including asset depreciation.

- *Travel Accounting:* Allows OPM to track and account for travel obligations (based on travel orders) and expenditure.

Unison ESC PRISM is a web-based application that supports the acquisition management lifecycle, from requisitioning through source selection, award, post-award management, and closeout. The PRISM components used by OPM are:

- Contract Solicitations

- Requisitions

- Contract Awards

- Delivery/Task Orders

- Multiple Award Schedules (i.e., IDIQ's)

- Blanket Purchase Agreement (BPA) and BPA Calls

- Interagency Agreements

- Contract Modifications

- Receiving/Inspection/Acceptance
- Contract Closeout

DELPHI Business Processes

OPM uses DELPHI to execute three financial business processes: *Procure to Pay, Order to Cash, Plan to Report and Acquire to Retire*. The *Procure to Pay* process is the end-to-end process that begins with the requisition, includes contracting/purchase of goods and services, and ends with payment for those goods and services. This area includes activities associated with contracting, purchasing, invoicing, disbursements, and vendor management and contains disbursements for payroll and travel/expense reimbursements. Data generated from this business process include contract award data, requisition data, purchase order data, invoice data, credit card data, disbursement/payment data, travel reimbursement data, payroll data, workflow data, and vendor data.

The Order to Cash Process is the end-to-end process that addresses activities from initial order receipt and credit authorization to revenue recognition, receivables, and collections. This area includes activities associated with reimbursable agreements, billing, collections, adjustments, customer management, and receivable management. Data generated from this business process includes reimbursable agreement data, billing and collections data, customer data, project management data, project contract data, and project cost data.

The Plan to Report Process is the end-to-end process that begins with planning the budget includes recording financial activity to the general ledger and execution of operating plans and ends with creating accounting, management, and performance reports. This area includes activities associated with planning and executing budgets, validating, and reconciling accounts, closing the books on a monthly and yearly basis, and creating financial reports. Data generated from this business process include budget

data, general ledger accounting data, cost allocation data, month-end close data, year-end close data, and reporting data.

The Acquire to Retire Process includes Asset Additions, Transfers, Disposals, Reclassifications, Financial Adjustments, Reinstatement, and Recording of periodic depreciation. The Assets module is integrated with Payables and General Ledger modules.

DELPHI Interfaces

DELPHI supports various interfaces with external to obtain its financial data and information. These interfaces use batch-file transfer technology that is a machine based in its authentication and authorization mechanism, as well as technology that masks sensitive information and ensures that it is communicated securely.

DELPHI interfaces with six systems that are external to OPM. The Department of Treasury's Intergovernmental Payment and Collection (IPAC) System provides a standardized process for interagency funds and expenditure transfer mechanism for Federal agencies daily. It facilitates intra-governmental federal e-commerce by transferring funds with related descriptive data, between OPM and other federal agencies. DELPHI also has interfaces daily with Treasury's Secure Payment System (SPS) to generate payment requests for the payment on delivery of goods and services to vendors and travel reimbursement to Federal employees.

DELPHI also receives data from the General Service Administration (GSA) systems. GSA's Electronic Time and Attendance HRLinks System provides OPM with labor cost data by pay cycle based on OPM timekeepers' information. This files' time and labor data is used to record direct labor costs for projects defined in DELPHI. GSA's System for Award Management (SAM) is a government-wide portal that OPM uses to obtain primary vendor data to support OPM's contract acquisition and internal agreement processes.

The remaining two external systems with which DELPHI interfaces are the Carlson Wagonlit Sato Travel (CWGT) E2 Solutions System, an electronic travel system that includes travel authorizations, travel vouchers, and miscellaneous reimbursements (including local travel) that it converts into DELPHI format for obligations and expenditure invoices; and the Citibank system, from which DELPHI obtains credit card purchases and payments information.

Authorities and Other Requirements

What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Several statutes and other authorities support collecting the information contained in DELPHI. These include 31 U.S.C., Subtitle II, which defines the budget process and describes the method for establishing and accounting for an agency's Federal budget; and 31 U.S.C., Subtitle III that describes the Federal financial management requirements and responsibilities to record accounting activities related to debt, deposits, collections, payments, and claims and to ensure effective control over, and accountability for, assets for which the agency is responsible.

Several other Federal financial mandates and legal authorities that govern financial management systems also support the collection of the information in DELPHI. These include The Chief Financial Officers Act of 1990, Public Law 101-576, and the Federal Financial Management Improvement Act (FFMIA) of 1996, Public Law 104-208, as well as guidance issued by the Office of Management and Budget: OMB Circular A-123, Management's Responsibility for Internal Control; OMB Memorandum 16-11, Improving Administrative Functions Through Shared Services (May 2016); and OMB Memorandum 13-08, Improving Financial Systems Through Shared Services.

What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The applicable SORNs are OPM/Govt-1, General Personnel Records, OPM/Internal 5, Pay, Leave, and Travel Records and OPM/Internal 23, Financial Management Records.

Has a system security plan been completed for the information system(s) supporting the project?

Yes. The DOT completed a system security plan for DELPHI in July 2025. In addition, a full Security Assessment and Authorization review of DELPHI was conducted to ensure proper security controls and protocols were in place. The DOT granted an Authority to Operate (ATO) to DELPHI in July 2025, expiring July 2028.

Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. The applicable records schedule is General Records Schedule 1.1. The schedule calls for the records to be destroyed six years after final payment or cancellation, but longer retention is authorized if business use requires.

If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information contained in DELPHI that pertains to OPM employees and vendors is not subject to the requirements of the PRA because the information is not collected directly from the public. DELPHI collects information from Federal agency financial management systems representing federal and commercial companies.

Characterization of the Information

Identify the information the project collects, uses, disseminates, or maintains.

DELPHI collects, uses, disseminates, and maintains information about OPM employees, vendors, customers, and members of the public. Specifically, the DELPHI application contains the following information:

- **Vendor Data:** This is limited to vendors or contractors conducting business with OPM and includes company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, tax identification number (TIN) (which may be a Social Security number in the case of sole proprietors set up as individuals), and DUNS number.

- **Employee Data:** This is limited to OPM employees and includes employee name, employee 'E' Number (used for travel reimbursement identification), and bank account information.

- **Customer Data:** This is limited to Federal agencies and entities with which OPM has an interagency agreement and includes customer name, treasury account symbol, agency location code, and trading partner.

- **Financial and other Banking Data:** This includes bank routing transit number, bank account number, and credit card number for all OPM purchase cards, travel cards, and fleet card holders.

DELPHI also supports external and internal financial reporting requirements, for example, tax and unpaid debt collection purposes. Both routinely and on an ad hoc basis, DELPHI generates standard financial reports such as for the status of funds, open obligations and commitments, aged receivables, vendor payments, and the status of a specific financial transaction.

What are the sources of the information and how is the information collected for the project?

The information maintained in DELPHI is primarily received from other systems via direct, automated system interfaces. Those systems, as explained in the Overview, include the Department of Treasury's Intergovernmental Payment and Collection (IPAC) System and Treasury's Secure Payment System (SPS), the General Service Administration (GSA)Electronic Time and Attendance HRLinks System and GSA's System for Award Management (SAM), the Carlson Wagonlit Sato Travel (CWGT) E2 Solutions System, and the Citibank system.

Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

While DELPHI does not integrate publicly available information from commercial sources, it does receive data from commercial sources available to the public. For example, the SAM portal is used by OPM's acquisition organization staff to manually search and gather contractor/vendor information. The SAM database is available for the public to search; however, acquisition professionals have privileged access to SAM in order to gather additional contractor/vendor information that is not made available to the public (e.g., DUNS number, TIN, or information not made public by the vendor). OPM's acquisition staff also uses SAM to verify that the contractor/vendor is in good standing with the Federal Government. The contractor/vendor information is interfaced daily to DELPHI to add new or updated vendor information to support OPM contract awards, obligations, and expenditures for contractors/vendors that provide services to OPM. This information is used when generating payments for services rendered and transmitting required information to Treasury for tax purposes.

Discuss how accuracy of the data is ensured.

The information maintained in DELPHI is primarily received from other systems. These source systems generally gather information directly from

agencies, vendors, and other commercial providers and as such, are accurate. In addition, DELPHI has various internal controls and procedures to ensure data accuracy. For instance, the majority of data in DELPHI is received through automated system interfaces; the built-in system edits and configuration increase data accuracy by minimizing data entry errors. Before uploading to DELPHI, the source data is also automatically evaluated for errors (e.g., file format, duplicate records, incorrect financial data), and if errors are found, DELPHI will not accept the record(s) and will generate an error log that must be reviewed and reconciled by a user in consultation with the source system or provider. Once reconciled, the record is re-submitted to DELPHI as part of the next automated transmission.

DELPHI embeds role-based access controls to ensure end-user roles and access levels are established following the separation of roles and duties principle, which inherently creates accuracy checks in the DELPHI when processing transactions. These controls also ensure that no one user can create and approve a single financial transaction. With each layer of review and approval, information in DELPHI is checked for accuracy, and errors are returned to the originating user for correction. Furthermore, when making corrections, users validate the information against the source data, which increases the data accuracy.

Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that PII will be unnecessarily collected and maintained in DELPHI.

Mitigation: DELPHI has mitigated this risk by establishing effective policies to avoid the unnecessary collection of PII and to redact PII if it is collected inadvertently. In addition, the Social Security number and bank account number are masked and transmitted via secure VPN connections to limit its exposure.

Privacy Risk: There is a risk that the information in DELPHI is inaccurate.

Mitigation: This risk is mitigated by the detailed procedures DELPHI has in place, described in Section 2.4, to ensure that the information is as accurate as possible.

Uses of the Information

Describe how and why the project uses the information.

DELPHI uses the information identified in Question 2.1 for the following purposes:

- **Payments/Disbursements**

Employees: DELPHI uses employee information such as name and banking information to process employee reimbursement for temporary duty travel and local travel vouchers.

SSNs are only used by the Treasury Offset Program (TOP). Reimbursements and payments for travel expenses are eligible for the TOP. For the payments to be offset at Treasury, Treasury verifies whether the name and SSN (or TIN in the case of Vendors) match. If they are a match, and there has been a debt filed with the TOP, the payments are intercepted and sent to the creditor who holds the debt.

Vendor/Contractors: DELPHI uses business-related information such as company name, address, TIN/DUNS, and banking information to generate payment for services rendered. DELPHI also use this information, including the TIN, to submit information about the contractor/vendor to the IRS for tax purposes.

- **Contract Awards/Modifications**

DELPHI uses business-related information (interfaced from SAM) such as company name, address, DUNS number, point of contact, and contract number to generate contract awards, commitments, and obligations.

- **Billing/Collections**

DELPHI uses business-related and financial information for Federal agencies name, address, treasury account symbol, trading partner number, and point of contact to generate billing invoices, and collections for debts owed to OPM for services provided to customer agencies.

- **Reporting**

  - DELPHI uses the information to generate regulatory, routine, and ad hoc reports. Such reporting also includes sharing the categories of information with other Federal agencies such as GSA for payroll information and Treasury for payment disbursements.

  - DELPHI uses information from PRISM to generate a public report containing information on contracts awarded with a value of $10,000 or more. This report is submitted to the Federal Procurement Data System - Next Generation (FPDS-NG), as required by the Federal Funding Accountability and Transparency Act (FFATA) of 2006 which is accessible to the public Also, the FPDS-NG information is shared with USA Spending as part of Digital Accountability and Transparency Act of 2014.

Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

DELPHI end-users have the ability to query and analyze information within the financial system. A variety of standard financial reports are available to monitor and detect differences or anomalies.

Are there other programs or offices with assigned roles and responsibilities within the system?

Yes. OPM program offices that use DELPHI have access to the discrete functionality that supports their organization with assigned user roles and responsibilities. There are approximately 350 DELPHI end-users across all Program Offices within OPM.

Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse of the information through unauthorized access to the information and a related risk that information within DELPHI may be used in a manner that is inconsistent with the purpose for which it is being collected and maintained in DELPHI.

Mitigation: This risk is mitigated using Role Based Access Controls (RBAC) comprised of user provisioning, permissions management, and access controls. More specifically, user access is also mapped to organizational duties performed to ensure that users are only processing data specific to their authorized functions. DELPHI has functionality built to track and identify what has been accessed by an individual end user using the RBAC. Additionally, all users receive training regarding the proper use of DELPHI and agree to Rules of Behavior prior to being granted access to the system. Additionally, all users receive training regarding the proper use of DELPHI and agree to Rules of Behavior prior to being granted access to the system.

Privacy Risk: There is a risk that the PII in DELPHI will be inappropriately exposed in the system, leading to unauthorized use.

Mitigation: This risk is mitigated by the proper implementation of security controls. In addition, OPM regularly reviews its DELPHI users to confirm that everyone who has access should have access and removes access for those who no longer have a need for it.

Notice

How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DELPHI does not generally collect information directly from individuals and, therefore, does not provide notice directly to individuals. Rather, DELPHI compiles information from several other sources that may collect information directly from individuals. Those systems that collect information directly from individuals are responsible for providing notice at the time of collection. While DELPHI does not provide notice directly to individuals to inform them of the collection, maintenance, and use of their information, notice is provided through this PIA.

What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Since information in DELPHI is primarily received from other sources, individuals do not have the option to consent to particular uses of their information once transmitted to DELPHI. Once collected, their information is used for the purposes described in this PIA. If consent is required, notification of use of PII was previously established in external/interface source system and distributed the individual.

Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware that DELPHI collects and uses their information.

Mitigation: This risk is mitigated through the publication of this PIA and indirectly via the relevant SORNs and notice provided at the points of collection by other systems that have direct contact with individuals.

Data Retention by the Project

Explain how long and for what reason the information is retained.

Pursuant to the applicable records schedule, the information in DELPHI is maintained for seven years. Retention of the information for this amount of time is necessary in order to apply any additional expenditure, adjust payments and account balances, and for auditing purposes.

Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in DELPHI will be retained for longer than is necessary to meet the business needs for which it was originally collected.

Mitigation: This risk is mitigated by adhering to the applicable records schedule, which addresses the business need to retain the information. When records are scheduled for destruction based on the retention schedule, OPM notifies FAA to implement the records schedule.

Information Sharing

Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. OPM shares information maintained in DELPHI outside of OPM with the Department of Treasury, the General Services Administration, and certain financial institutions.

DELPHI shares information with the Department of Treasury Financial Management Service (FMS) to facilitate payment disbursements to contractors/vendor, employees, and other Federal customers. Information shared with FMS is transmitted electronically via a direct upload to Treasury's SPS system. Transmission of data to Treasury via SPS is encrypted. Treasury uses the information provided to issue federal payments on behalf of OPM in the form of a paper check or EFT transaction. An

Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) allow OPM to conduct data exchanges in support of these financial management transactions.

As required on an annual basis, OPM shares financial information maintained in DELPHI with the Internal Revenue Service (IRS) to report payments issued to vendors/contractors for services rendered to OPM. This includes interest payments distributed to obligors (IRS Form 1099). This information is shared with the IRS to support the federal income tax processing and in accordance with the Internal Revenue Code and IRS regulations.

DELPHI also shares information on debts with Treasury pursuant to the Debt Collection Improvement Act of 1996. OPM accounting staff prepares data files that are sent electronically to Treasury via an encrypted transmission to the Treasury Cross-Servicing Program and/or Treasury Offset Program for appropriate processing, including sending out debt collection letters, establishing repayment agreements, withholding wages, and other debt collection activities.

DELPHI also shares bank account and routing information with external financial institution for merchant card processing, and other credit card processes and payments.

Describe how the external sharing noted in 6.1 is compatible with the SORNs noted in 1.2.

The sharing described above is compatible with the original purpose for which the information was collected, namely, to perform financial management functions to support OPM business operations and is shared pursuant to appropriate routine uses in the applicable SORNs.

Does the project place limitations on re-dissemination?

Yes, re-dissemination of DELPHI information is subject to the terms in stated and signed contracts and interagency agreements.

Describe how the project maintains a record of any disclosures outside of OPM.

Records of information disclosed outside of DELPHI are maintained through interface logs upon integration with the systems identified in this PIA. For example, OPM uses the payment schedule dates from when batch payment files are transmitted to the Treasury to track disclosures of DELPHI data (including PII). DELPHI records the disclosure of the associated records and data by recording the payment schedule date from the batch file.

Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information from DELPHI may be inappropriately disclosed outside of OPM.

Mitigation: This risk is mitigated by only sharing information about individuals as permitted by the applicable SORN.

Privacy Risk: There is a risk that information, once shared appropriately, will be further shared, or used in a manner that is inconsistent with the original purpose for which it was collected and shared.

Mitigation: This risk is mitigated by ensuring that the sharing is subject to written agreements that define the purposes for which the information is shared, prohibits other uses, and appropriately limit any onward sharing with third parties.

Redress

What are the procedures that allow individuals to access their information?

Individuals do not have direct access to DELPHI. However, they may request access to records about themselves that are included in the relevant systems of records by following the procedures outlined in the relevant SORNs referenced in 1.2.

What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals who access their records contained in relevant systems of records may request correction of any inaccurate or erroneous information by submitting a request to correct the data via the procedures outlined in the relevant SORNs referenced in 1.2.

How does the project notify individuals about the procedures for correcting their information?

The procedures for submitting a request to correct information are outlined in the applicable SORNs.

Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to access information about them that is contained in DELPHI nor be afforded adequate opportunity to correct that information.

Mitigation: This risk is mitigated by providing individuals with an appropriate opportunity to request access to and amendment of their records as outlined in the applicable SORNs.

Auditing and Accountability

How does the project ensure that the information is used in accordance with stated practices in the PIA?

DELPHI uses auditing to capture information associated with any viewing, creating, updating, or deleting of records and the user that performed the activity at the database level. DELPHI audit trails provide adequate information to facilitate an understanding of transactional events if compromise or malfunction occurs. The audit trail discloses actions such as unauthorized access, modification, and destruction of data. While the information is contained within the FAA systems, FAA will work with OPM to review the data as needed.

FAA has imposed appropriate controls to minimize the risk of compromising stored information.

Additionally, the TINs and DUNs maintained in DELPHI for OPM vendors are visible only to those authorized users with a need to know based on their user access and prescribed official duties.

Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM and FAA employees and contractors complete annual mandatory Security and Privacy Awareness Training. In addition, end-users are provided access to applicable DELPHI content training specific to work responsibilities once the DELPHI access is granted.

What procedures are in place to determine which users may access the information and how does the project determine who has access?

Each user account is assigned specific roles with a defined set of privileges to ensure overall system integrity. DELPHI system administrators can elect to assign all the privileges for a given role or can select only certain privileges to assign. Access is limited to OPM employees who have a need to access the system based on their roles in support of financial administration and management operations at OPM. Users are also provided access to system-specific user training once the user access has been granted. The roles and privileges assigned to a particular user are predetermined depending on the user's function.

How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

DELPHI program managers coordinate with relevant OPM stakeholders, including the Chief Financial Officer, Chief Privacy Officer, and Chief Information Security Officer, to review and assess new uses of information.

Additionally, DELPHI program managers, the CPO, and CISO will review information sharing agreements, including interconnection service agreements (ISA) and Memoranda of Understanding (MOUs) to ensure that appropriate privacy and security provisions are included to safeguard PII.

Responsible Officials

Minh Le
Acting Associate Chief Financial Officer

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy