U.S. Department of Transportation

Office of the Secretary (OST)

# Privacy Impact Assessment

## Enterprise Services Center Purchase Request Information System (ESC PRISM)

### Responsible Official

Laura Herz
Email: laura.herz@dot.gov
Phone Number: 202-366-9948

### Reviewing Official

Karyn Gorman
Acting 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) was established under 49 CFR 1.33, Chief Financial Officer and Assistant Secretary for Budget and Programs for the purpose of controlling and facilitating the accounting and reporting of financial transactions for the Department of Transportation  (DOT). To assist in completion of these duties, the Office of Financial Management uses Enterprise Services Center Procurement Request Information System Management (ESC PRISM), which is a customized Commercial Off-The-Shelf (COTS) procurement system. ESC PRISM enables acquisition professionals to efficiently and effectively complete federal acquisition tasks in a compliant way from planning through closeout.

This Privacy Impact Assessment (PIA) is required under the eGovernment Act of 2002 because the system collects personally identifiable information (PII) from members of the public.

## 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

ESC PRISM is a COTS procurement system created by and supported by Unison. ESC PRISM offers a holistic online acquisition lifecycle management and contract writing system for federal agencies. It enables acquisition professionals to efficiently and effectively complete federal acquisition tasks, in a compliant manner, from planning through closeout. Extensive audit trails track the progress of acquisitions throughout every stage of procurement and PRISM's comprehensive reporting capability captures critical data for internal and external reporting requirements.

ESC PRISM collects, stores, and manages contact information for individuals associated with vendors who work with DOT. Information includes the vendor's name, address, and contact phone number. Social Security Numbers (SSN) or Taxpayer Identification Numbers (TIN) are not collected in the system. ESC PRISM collects the PII to effectively manage procurement actions and increase productivity across the procurement processes from requisitioning to closeout, minimize data entry, and maximize efficiency through electronic routing, workflow, and workload management. Email is the most common method of communication with the customers/vendors. Access to the data in the system is limited to the Financial Management division staff members that have a need to know and managed through user roles. Members of the public cannot access the system.

ESC PRISM is integrated with DOT Delphi[2]. ESC PRISM's integration with the DOT DELPHI system allows invoices to be approved in ESC PRISM and electronically sent to DOT DELPHI for payment. Once payment is made, ESC PRISM receives an update from DOT DELPHI reflecting that the payment has been

Processed.

ESC PRISM also takes advantage of the FedRamp FedConnect® system which is a Federal acquisition and grants portal where grant applicants/awardees can find opportunities for federal contracts, grants, and other types of assistance funding. It was developed to bridge the gap between government agencies and their grant applicant/recipient communities to streamline the process of doing business with the government. Through the FedConnect® portal, Federal Government representatives can issue opportunity requests and make awards via the internet. Company representatives can review opportunities, submit bids or proposals,

[2] 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.

and receive awards. FedConnect® provides an open channel of communication between ESC PRISM and the contracting bid/awardee that is both secure and auditable.

## 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[3], 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[4].*

## 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 the system retrieved by personal identifier are subject to the provisions of the Privacy Act. Records are maintained in accordance with the Department's published System of Records Notice (SORN), DOT/ALL-7, Departmental Accounting and Financial Systems (DAFIS) and Delphi Accounting System, 65, FR 19481, April 11, 2000. There are no exemptions claimed for the system.

Username, password (encrypted and hashed), email, activities while accessing the system (audit records) from vendors, individuals, and entities that resulted from procurement actions is collected to control and facilitate the accounting and reporting of financial transactions for DOT. User activity logs are covered by DOT/ALL 13 - Internet/Intranet Activity and Access Records – (67 FR 30757 - May 7, 2002).

The publication of this PIA further demonstrates the Office of Financial Management commitment to provide the appropriate transparency into ESC PRISM. This PIA is available to the public at: http://www.transportation.gov/privacy

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

## 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.*

Authorized users employ ESC-PRISM for entering award information and performing subsequent transactions, such as award status change, and closeout of procurement actions. Selected recipient data is programmatically interfaced from the Delphi information system to ESC-PRISM and is available for selection on various award documents. PII is collected and used to process and approve vendor invoices in ESC PRISM and to electronically submit outstanding obligations to DOT Delphi for payments. ESC PRISM collects contact information associated with vendors including name, username, password, (encrypted and hashed) and email address. Social Security Numbers and TINs are not collected in the system. Records in the system retrieved by personal identifier are subject to the provisions of the Privacy Act. Records are maintained in accordance with the Department's published System of Records Notice (SORN), DOT/ALL-7, Departmental Accounting and Financial Systems (DAFIS) and Delphi Accounting System, 65, FR 19481, April 11, 2000. There are no exemptions claimed for the system. Under the provision of DOT Privacy Act/ Freedom of Information Act (FOIA) procedures, individuals may request searches of ESC PRISM to determine if any records may have been added or pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing to:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Individuals should include in their requests the following information:

- Name and title of the system of records from which you are requesting the search.
- Name of individual
- Mailing address
- Phone number or email address; and
- Description of the records sought, and if possible, location of records.

Individuals wishing to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for and why the records should be corrected. Requests should be submitted to the attention of the OST Official responsible for the record at the address below:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

## 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 PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.*

ESC PRISM collects PII to effectively manage procurement actions, increase productivity across the procurement process from requisitioning to closeout, minimize data entry, and maximize efficiency through electronic routing, workflow, and workload management. The following PII is collected and maintained in the system: name, address, phone number, username, password (encrypted and hashed) and email activities while accessing the system (audit records) from vendors, individuals, and entities resulting from procurement actions. Social Security Numbers and TINs are not collected in the system.

ESC PRISM has the authority to collect PII in its system under 49 CFR 1.33, Chief Financial Officer and Assistant Secretary for Budget and Programs. These records are protected under the Privacy Act System of Records, DOT/ALL-7 – Departmental Accounting and Financial Systems (DAFIS) and Delphi Accounting System.

## 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 as long as necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record disposition schedule.*

Only relevant and necessary PII is collected in the system in ESC PRISM. The name of the vendor and the address is collected and used to process and approve vendor invoices and to electronically submit outstanding obligations to DOT Delphi for payment.

FedConnect® collects only PII that is relevant and necessary. The FedConnect® portal is only accessible by Federal Government representatives who issue opportunity requests and make awards from the internet.

Records in ESC PRISM are retained in accordance with NARA's General Records Schedule (GRS) 1.1, Financial Management and Reporting Records,

- GRS 1.1, Item 10 Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting: DAA-GRS-2013-0003-0001. Temporary. Destroy 6 years after payment or cancellation, but longer retention is authorized if required for business use.
- GRS 1.1, Item 11, Procuring goods and services. DAA-GRS-2013-0003-0002. Temporary destroy when business use ceases.

## 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.*

ESC PRISM, as well as data collected from FedConnect® contains contact information for individuals associated with vendors. The collected information is used to print the vendor name and address on the awards. Information used, collected, and maintained on DOT and Non-DOT Federal/Contract workforce includes username, password (encrypted and hashed), email, and activities while accessing the system. Extensive audit trails track the progress of acquisitions throughout every stage of procurement and PRISM's comprehensive reporting capability captures critical data for internal and external reporting requirements. Only the Financial Division staff members can access the data in the system.

Records in the system are covered under DOT/ALL-7, Departmental Accounting and Financial Systems (DAFIS) and Delphi Accounting System, 65, FR 19481, April 11, 2000, and may be disclosed outside of DOT as a routine use pursuant to 5. U.S.C. 552a(b)(12):

- Disclosures may be made from this system to "consumer reporting agencies" as defined in the Fair Crediting Reporting Act, 15 U.S.C. 1681a(f) or the Federal Claims Collection Act of 1982, 31 U.S.C.3701(a)(3).

- 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).*

ESC PRISM employs the data accuracy checks in its database software to ensure data validity and accuracy. The system is reviewed to ensure, to the greatest extent possible, the information is accurate, relevant, timely, and complete via security testing and evaluation.

The customers/vendors are responsible for ensuring the accuracy and quality of the data provided for processing. Information is entered manually by the service desk agent upon receipt from the agencies, who are customers of the ESC PRISM 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 as revised, 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:

- The ESC PRISM system has a Continuous Monitoring Assessment (CMA) process that supports reaccreditation/reauthorization of the system. The CMA addresses the OMB Circular A-130 requirement for annual testing.
- Encryption of PII which is stored and/or transmitted is compliant with FIPS 140-2 standards.
- ESC PRISM personnel handling sensitive information are required to undergo appropriate background checks to assess their suitability to perform in public trust positions. Additionally, all staff undergoes initial security awareness training and annual refresher training, and the procedures for properly protecting the privacy of users' personal information are stressed in this training.

ESC PRISM is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees, and contractors. ESC PRISM 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 ESC PRISM 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. ESC PRISM is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

The system 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 is allowed to ESC PRISM prior to receiving the necessary clearances and security and privacy training as required by the Department. All users at the federal level are made aware of the Rules of Behavior (ROB) for IT Systems and accept them prior to being assigned a user identifier and password and prior to being allowed access to ESC PRISM. The ESC PRISM system tracks in an audit file each entry to ensure data integrity and record accuracy.

## 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.*

This system implements a continuous monitoring strategy that includes a configuration management process that determines the security impact of changes to the system and its environment, conducts ongoing assessments, and reports the state of system to organizational officials. An independent assessment team is used to monitor the security controls in the information system on an ongoing basis.

## Responsible Official

Laura Herz
Information System Owner
Associate Director, Project Management and Systems, OST B-30
Phone: (202) 336-9948
Email: laura.herz@dot.gov

## Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer