U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary of Transportation (OST)
Office of Financial Management (B-30)
Enterprise Support Systems (ESS)

Responsible Official

David Rivait
DOT Deputy Chief Financial Officer
202-493-0476
David.Rivait@dot.gov

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
DOT Chief Privacy & Information Asset Officer
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 Enterprise Support System (ESS). The ESS is comprised of a suite of General Support Systems which support delivery of Delphi Federal Financial Services to the Department's FSSP customers and CASTLE Time and Attendance for the Department. This Privacy Impact Assessment (PIA) was conducted because the ESS collects personally identifiable information (PII) from individuals associated with the Department's FPPS customers. ESS utlizes a subsystem called Secure File Transfer Protocal (SFTP) that transmits all data between Delphi and CASTLE through a Secure Shell protocol (SSH). SFTP is utlized to provide secure file access, secure file transfer, and secure file management For all of DOT FPPS customers. The Department's PIAs Delphi and CASTLE may be found at 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 ESS environment that provides financial services to aid the Department and its FSSP customers in meeting current and future financial mission requirements.[1]

ESS is comprised of four subsystems described below:

- **Kintana:** is a ticketing system though which FPPS customers submit System Change Requests (SCR) and Requests for Service (RFS). Contact information (name, affiliation, email, phone, and fax) of requestors is captured by ESS staff during the course of ticket creation and is entered manually in the appropriate ticket fields. Additionally, Personally Identifiable Information (PII) may be captured in supplemental documentation provided by the requestor to aid in the identification and resolution of issues or by ESS as evidence of correction when system changes have been made. Individuals may create tickets by calling the ESC Help Desk, sending email to customerservice@esc.gov, or via the ESC Customer Portal, http://www.esc.gov/help_desk.asp.
- **Secure File Transfer Protocol (S-FTP)**: facilitates data exchange, including Sensitive PII between FPPS customers and Delphi and CASTLE systems as appropriate. The records in this system are considered to be part of the Delphi and/or CATLE environments as appropriate are removed once the data exchange is complete.
- **Service Oriented Architecture (SOA)**: facilitates connectivity between Delphi and and its ESC PRISM Subsystemwith CASTLE. There is no PII or SPII housed in SOA.
- **Serena Professional Version Control Software (PVCS)**: provides version control for the Delphi and CASTLE program code. There is no PII or SPII housed in PVCS.

[1] Appendix A lists the Department's FSSP customers at the time this PIA was developed.

Fair Information Practice Principles (FIPPs) Analysis

The 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) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

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

Customer service tickets maintained in the Kintana portion of ESS are retrieved by individual identifier and are protected under the Privacy Act. The Department is in the process of updating its current system of records notice (SORN), DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002, to explicitly cover these records. Individuals are notified by the Department that their information is being captured for records keeping purposes at the time that their ticket is created and that it will be used to facilitate communication during the resolution process. The Department's FSSP's customers are responsible for publishing SORNs for the financial and time and attendance records maintained in Delphi and/or CASTLE.

The publication of this PIA furthers demonstrates Department's commitment to provide appropriate transparency into ESS. Individual's wishing to inquire the Department's privacy program or contact privacy officials to address privacy concerns can visit the DOT privacy office website at www.dot.gov/privacy.

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.

Individuals whose information is incorrectly captured in an ESS/Kintana ticket may submit a Request for Service ticket in Kintana to correct any personal information discrepancies. Amendments to the original collected information are housed in Kintana tickets and new information must be specified by the individual.

Under the provisions of the DOT's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of ESS 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 particular assigned to the individual. In the Privacy Act, an individual is defined to

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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 DOT by complying with DOT Privacy Act regulations, 49 CFR part 10.

DOT 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. DOT 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:

Claire W. Barrett
Departmental Privacy Officer
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 its collects, uses, maintains, or disseminates PII.

ESS is a support system for the Department's FPSS Delphi and CASTLE service offerings, and collects PII only in support of those activities. As of December 2011 the Department no longer collects SSNs the puproses of creating user accounts in ESS/Kintana. SSNs previously collected for the purpose are obvuscated fine the database and not made available to users in electronic or paper copy.

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.

ESS records are considered temporary and maintained in accordance with NARA's General Records Schedule 3.1 General Technology Management Records item 20 Information technology operations and maintenance records and item 30, Configuration and Change Management Records, and 40, and are deleted from the system between 3 and 5 years from the date of activity completion in accordance with

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.

PII maintained in ESS/Kintana is used only for the purposes for facilitating resolution of customer service tickets. The Department as the provider of FSSP services does not access or use information exchanged through the S-FTP service.

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 ESS components are Commercially Off the Shelf (COTS) software which is furnished with a front-end application login page providing quality control and accountability of users with authorized credentials. Only Authorized users with credentials are allowed to view ESS information. Information in ESS is used as intended solely for business purposes. Kintana software data validation is enabled on the input fields and sections in Kintana have predefined fields that are configured by administrative personnel. Authorized Kintana users can create or modify a ticket to change PII information for relevancy, accuracy, and completeness. The accuracy of information entered into the S-FTP is inherited by the actions of the personnel uploading the data.

The Delphi Change Control Board (DCCB) has been formally established for the system and the approving body for ESS components application changes/updates. The DCCB meetings occur on a weekly basis to discuss the upcoming system change requests. FAA AMZ Functional/Help Desk support also have input into the DCCB. The ESS Information System Security Officers (ISSOs) are members of the DCCB. The ISSOs must approve all requested modifications, from a security perspective, to the ESS production environment in Kintana. The security controls corresponding to the minimum security requirements are defined in the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53, including control enhancements. In addition, there are DOT and FAA requirements that are addressed in the implementation of the minimum security controls. The System Security Plan (SSP) provides a description of how each of the security controls, including control enhancements, in the applicable baseline is being implemented or is planned to be implemented.

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.

ESS is hosted in a secure facility that is not publically accessible. Armed guards control access to the facility. Physical access to the data center is controlled through the use of a badge-activated turnstile, identification badges and key card entry devices. Those accessing the data center that does not have a key card are required to sign in and must be escorted. An automatic log is kept whenever a person accesses the secure data center area with their key card. The ESS servers and other physical hardware within the data center are secured in a caged area with limited personnel access. Cameras have been installed throughout the data center to monitor activities within the facility. ESS and Delphi functional/technical personnel are instructed privacy responsibilities, security awareness and incident response training annually to ensure effectiveness.

ESS follows the DOT enterprise-wide privacy incident handling and response standard operating procedures. The privacy incident policy includes multiple points of contact for notification of suspected privacy leakage including the line of business privacy coordinator, incident liaisons, security personnel, and chief information officer and the chief financial officer. Personnel are directed to immediately inform the FAA Cyber Security Management Center (CSMC) of the detection or discovery of suspected or confirmed incidents involving PII, no matter the format. In the incident handling procedures personnel are directed to following the steps therein to triage, response, escalation, containment, analysis, investigation, assessment of the leakage, document, notify, and mitigate the risk.

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.

Administrators managing ESS must complete a privacy courses at least annually. Policies, procedures, and compliance of privacy controls are governed by the OMB, DOT, FAA orders that minimizes the use and increases the protection of sensitive material. Users in ESS have segregation of duties and responsibilities that prevent data leakage and minimize the likelihood of inappropriate data utilization. ESS has audit logs enabled for accountability and Intrusion Detection Systems (IDS) monitoring enabled for the information system in real time. The Department ensures that the controls that govern the privacy of ESS are tested, reviewed, and assessed at least annually by an independent assessment group. A copy of the ESS Certification Authorization can be requested from the system Information Systems Security Manager (ISSM). Every three years it is required for ESS to acquire a Security Authorization and subsequent CMAs in order to remain compliant with applicable orders, policies, laws and regulations. The authorizing official approves the Security Authorization and CMA packages giving the authority to operate in the current environment. When the package is signed, the authorizing official accepts the privacy risk associated with the implemented security controls. If risks are introduced that cannot be remediated, support personnel will mitigate risks to an acceptable level with the approval from the authorizing official. Audits logs are reviewed to identify suspicious activities on a weekly basis. All logical information stored in ESS is controlled by roles and responsibilities. Any individual with an account is authorized to print, but has the responsibility to ensure documents are safeguarded and only disseminated to authorized personnel. The breach of sensitive information would initiate the incident response plan process. Security control health checks and vulnerabilities scans are completed monthly to advise personnel of the current risk level associated with ESS.

Responsible Official

David Rivait
DOT Deputy Chief Financial Officer
Office of Financial Management
202-493-0476
david.rivait@dot.gov

Approval

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

Appendix A – US Department of Transportation Federal Shared Service Provider Customers

The following federal agencies have engaged with the Department of Transportation to provide shared services for financial management

- Commodity Futures Training Commission (CFTC)
- Consumer Product Safety Commission (CPSC)
  - Financial Management Service (FMS)
- Department of Interior (DOI)
  - National Finance Center
- Department of Transportation
  - Office of the Inspector General (OIG)
  - Office of the Secretary of Transportation (OST)
    - National Transportation Center (Volpe)
  - Federal Aviation Administration (FAA)
  - Federal Highway Administration (FHWA)
  - Federal Motor Carrier Safety Administration (FMCSA)
  - Federal Railroad Administration (FRA)
  - Federal Transit Administration (FTA)
  - Maritime Administration (MARAD)
  - National Highway Traffic Safety Administration (NHTSA)
  - Pipeline and Hazardous Materials Safety Administration (PHMSA)
  - Surface Transportation Board (STB)
- Government Accountability Office (GAO)
- Institute of Museum and Library Services (IMLS)
- Securities and Exchange Commission (SEC)