Privacy Impact Assessment Update
for the

Transportation Security Administration Enterprise Performance Management Platform (EPMP)

DHS/TSA/PIA-034(a)

February 3, 2014

Contact Point
James Watts
Operational Process & Performance Metrics
Transportation Security Administration
Jim.Watts@dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) Enterprise Performance Management Platform (EPMP) is designed to assist in performing security management functions using a wide variety of data associated with security, equipment, and screening processes from TSA's security activities. EPMP maintains personally identifiable information (PII) about members of the public in excess of basic contact information, which triggered the requirement to conduct the EPMP Privacy Impact Assessment (PIA) dated May 10, 2011. TSA is updating this PIA to reflect 1) the inclusion of the Visible Information Management System (VIMS), a data management module within the EPMP framework that supports the Visible Intermodal Prevention and Response (VIPR) Program; 2) the transfer of payroll transactions for Transportation Security Officers (TSO) from the Performance Management Information System (PMIS) to the Airport Information Management (AIM) System; and 3) the storing of PII on individuals identified in the Terrorist Screening Database (TSDB) as posing a threat to transportation or national security in the AIM System.

Introduction

EPMP is principally used to generate statistical and operations management information, such as equipment maintenance, property tracking, number of enplanements, and employee service information. EPMP uses data from a variety of sources to generate performance information.

The principal application within EPMP is the Performance Information Management System (PIMS), which is both a business tool and a data warehouse. Principal data sources within the PIMS data warehouse include the similarly-named PMIS System and AIM. PMIS is used to securely communicate information, previously passed via e-mail by TSA customer service and/or security operations center personnel, to TSA field personnel regarding individuals transiting through U.S. domestic airports who are under special travel arrangements, and individuals identified in the TSDB.

AIM is an application that assists facilities in managing day-to-day activities and includes a variety of employee and equipment information. AIM will now process payroll transactions between TSA and the United States Department of Agriculture, National Finance Center (NFC) by using a hashed algorithm to mask TSOs' Social Security Numbers (SSN) while correlating names, job titles, airport locations, and hours worked.

Although AIM will assume the responsibility of processing payroll transactions, PMIS will remain a data entry source for a variety of TSA metrics associated with security activities, such as screening throughput, number of prohibited items intercepted, security drills, wait times, number of checkpoints and lanes, and machine resources.

VIMS is a data management module within the EPMP framework that supports the TSA VIPR Program.[1] The VIPR Program comprises teams of Behavior Detection Officers; Federal Air Marshals; Explosives Detection Canine Teams; Transportation Security Inspector (TSI); TSOs; Transportation Security Specialists – Explosives (TSS-E); and federal, state, local, or tribal law enforcement officers assigned to provide a visible deterrent to potential terrorist activity at various transportation facilities (e.g., AMTRAK stations, airports, mass transit stations, bus terminals). TSA uses VIMS to manage and track overt/covert security operations at these locations. VIMS serves primarily as a reporting tool for VIPR teams and may contain limited contact information (name, agency, and business/mobile phone numbers) on VIPR team members.

EPMP also uses the TSA Performance and Results Information System (PARIS) for statistical information. While dominated by statistical information, AIM, PMIS, and PARIS maintain some PII on employees and members of the public.

Categories of PII in PMIS: Individuals under special travel arrangements (such as diplomatic considerations or escorted travel); and individuals identified in the TSDB as posing a threat to transportation or national security.

Categories of PII Maintained in AIM: Employee information used for the management of operations (e.g., payroll information including employee SSNs, date of service information, pay band, supervisor, leave data, contact information, work schedules, uniform issuance, and controlled property tracking); dependent names, dates of birth, and emergency contact information; customer service information such as complaints/compliments; lost and found item identifications; damaged bags identification; information relating to individuals involved in incidents at the facility (may include security incidents or non-security incidents such as slip and fall, theft, etc.); and individuals identified in the TSDB as posing a threat to transportation or national security.

Categories of PII in PARIS: Individuals and witnesses involved in certain significant security incidents.

Categories of PII in VIMS: In addition to contact information on DHS personnel, VIMS will maintain names, agencies, and business/mobile phone numbers of federal, state, local, or tribal law enforcement officers serving as contacts for the planning and conduct of VIPR operations.

Reason for the PIA Update

TSA is updating this PIA to reflect the inclusion of VIMS, a data management module within the EPMP framework that supports the VIPR Program; the transfer of payroll transactions

[1] http://www.tsa.gov/about-tsa/visible-intermodal-prevention-and-response-vipr

for TSOs from PMIS to AIM; and the storing of PII on individuals identified in the TSDB as posing a threat to transportation or national security in the AIM System.

VIMS will maintain the name, agency, and business/mobile phone number of VIPR team members participating in overt/covert security operations at various transportation facilities (e.g., AMTRAK stations, airports, mass transit stations, bus terminals).

AIM will now process payroll transactions between TSA and the NFC by using a hashed algorithm to mask TSOs' SSNs while correlating names, job titles, airport locations, and hours worked.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

VIMS will now maintain the name, agency, and business/mobile phone number of VIPR team members.

There are no changes to the type of information collected by AIM as it assumes the responsibility of processing payroll transactions for TSOs from PMIS.

Uses of the System and the Information

In addition to the uses described in the original EPMP PIA published on May 11, 2011,[2] TSA will use the information contained in VIMS to manage VIPR program points of contact, conduct reports, and analyze program-related data.

TSA will now use AIM instead of PMIS to process payroll transactions between TSA and the NFC for TSOs.

There are no additional changes to the uses of the information within the remaining EPMP activities.

Retention

TSA submitted records retention schedules discussed in Section 1.4 of the May 10, 2011 PIA to the National Archives and Records Administration (NARA) for information not currently covered by existing schedules. TSA will seek to retain VIMS data in accordance with NARA Record Schedule N1-560-04-10, Item 3.

Internal Sharing and Disclosure

No changes.

[2] http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa

External Sharing and Disclosure

PII in VIMS falls within DHS/ALL-002 Mailing and Other Lists System of Records, 73 FR 71659, November 25, 2008.

There are no additional changes to the uses of the information within the remaining EPMP activities, which fall within DHS/TSA 001 Transportation Security Enforcement Record System (TSERS), 75 FR 28042, May 19, 2010.

Notice

No changes.

Individual Access, Redress, and Correction

No changes.

Technical Access and Security

In addition to the Technical Access and Security features discussed in Section 8 of the May 10, 2011 PIA, VIMS incorporates "least privileges" to permit user access to specific views with specific data rights, such as view, create, and edit. VIMS incorporates auditing capabilities that allow site administrators to ensure that only authorized users maintain access to the system.

There are no technical access and security changes associated with AIM assuming payroll processing responsibilities from PMIS. Human Resources personnel will merely use a separate system to complete the payroll transactions.

To enhance data security, TSA segregates customer service information contained in AIM modules assigned to customer contact management, lost and found tracking, damaged bag management, claim processing modules, and individuals transiting through airports who are under special travel arrangements. Based on the users role at a particular airport or TSA facility, TSA site administrators establish and enforce separation of duties through assigned automated access authorizations for information as well as individual users. For example, a typical user may be able to access and view reports for an individual airport/facility, while a Federal Security Director (FSD) will have the ability to access and view reports related to multiple airports/facilities.

TSA also segregates data on individuals identified in the TSDB as posing a threat to transportation or national security by using AIM to securely communicate information, that is currently passed by e-mail, to designated TSA personnel that need the information in the performance of official duties and/or to provide an operational response.

TSA segregates TSO employee time and attendance and payroll management data contained in AIM modules separately from data obtained from customer service information discussed above by using automated role-based access restrictions that prevent unauthorized users from accessing PII in various segregated AIM modules.

The entire EPMP architecture employes the concept of least privilege, allowing only authorized access for users necessary to accomplish assigned tasks in accordance with organizational missions and business functions. In addition, EPMP employs automated auditing capabilities and stores audit logs on a centralized server for simplified access and correlation with other types of information technology security events.

Technology

In addition to the Technology features discussed in Section 8 of the May 10, 2011 PIA, VIMS tracks venue profiles, modes and capability of venues, and local and state laws related to VIPR operations. The VIMS solution is based on the Microsoft .NET framework, which provides robust software security capabilities. By design, VIMS coexists on the same hardware configuration and servers as PIMS. Data collected in VIMS is available real-time in the PIMS Business Intelligence and reporting tool. TSA separates VIMS users and data from PIMS and the other systems and data within the EPMP framework.

There are no technology or framework changes associated with AIM assuming payroll processing responsibilities from PMIS. AIM previously maintained human resources modules capable of performing payroll transactions for TSOs.

Responsible Official

James Watts
Operations Performance Division
Office of Security Operations
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security