Privacy Impact Assessment Update
for the
Visitor Management System

DHS/TSA/PIA-004(b)

March 11, 2013

Contact Point
Russell Appleyard
Office of Security
Transportation Security Administration
(571) 227-3659

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Visitor Management System (VMS) Privacy Impact Assessment (PIA), previously published on October 19, 2007, is being amended to reflect that Transportation Security Administration (TSA) field locations may choose to implement an electronic system to log visitors. Where deployed, these systems will be used in place of paper visitor logs. These systems will generate temporary paper visitor badges, which may include the visitor's photograph, for entry to a TSA facility. This PIA is conducted pursuant to the E-Government Act of 2002 because TSA will collect personally identifiable information (PII) on members of the public as part of the electronic visitor system.

Introduction

In 2006, TSA installed an electronic Visitor Management System (VMS) at the TSA Headquarters and the Transportation Security Operations Center (TSOC). Both locations are designated as Level IV federal facilities pursuant to the guidelines established in the 1995 Department of Justice directive entitled, "Vulnerabilities of Federal Facilities."[1] TSA is required to comply with security procedures to ensure a safe and secure work environment for TSA Headquarters employees, TSOC employees, contractors, and visitors. The VMS is a system by which computerized visitor logs will be generated and temporary paper badges with photographs will be issued for all visitors entering the TSA Headquarters Buildings and the TSOC.

Additional TSA facilities, although not designated as a Level IV federal facility, may install similar electronic visitor systems to manage visitor access and issue temporary badges to visitors accessing TSA field facilities. The use of electronic visitor systems assists in providing a safe and secure work environment for TSA employees, contractors, and visitors by ensuring that badges are only issued to those individuals authorized to be in the TSA facility on a given day. The temporary badges may include photographs.

Visitors must provide a government issued photo identification card that will be swiped through a scanner equipped with an optical character recognition (OCR) device. The device will collect and store the name and picture of the visitor. The device will automatically add the date, location, and time of the visit to the collected information and store it. Visitors who do not present a government issued photo identification card will be identified by the employee being visited as part of the screening process. A photograph of the visitor will be taken and used to produce a visitor badge.

The visitor may be asked to provide his or her mobile telephone number, which TSA will use to contact the visitor while in the building in the event of an emergency. Failure to provide a mobile telephone number will not prevent access to the TSA facility.

[1] U.S. Department of Justice, U.S. Marshals Service, Vulnerability Assessment of Federal Facilities, Washington, DC, June 28, 1995.

Reason for the PIA Update

The PIA is being updated to reflect that TSA field locations may use an electronic visitor management system to manage visitor information and provide identification badges for visitors entering a facility. For example, TSA may deploy such electronic systems at an airport for visitors to access Federal Security Director (FSD) offices.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The Security Appointment Center (SAC) in Headquarters and the TSOC employs a VMS that requires visitors to be pre-registered by the TSA employee being visited. The employee provides the date, time, and location of visit, the name of the employee to be visited, and the employee's contact information.

The Airport Coordination Centers (ACC) may pre-register the visitor or register the visitor at the time of the visit to the field location.

The visitor may be asked to provide his or her mobile telephone number, which TSA will use to contact the visitor while in the building in the event of an emergency. Failure to provide a mobile telephone number will not prevent access to the TSA facility.

Uses of the System and the Information

The system and information will be used to register the visitor, allow security personnel to verify the visit and TSA contact, create a temporary badge authorizing access to the field facility, eliminate hand-written visitor logs, and generate statistical reports concerning visitors to the facility.

Retention

No update.

Internal Sharing and Disclosure

No update.

External Sharing and Disclosure

No update.

Notice

Notice will be provided to visitors that their information will be collected and maintained in order to enter the facility. The visitor may be asked to provide his or her mobile telephone number, which TSA will use to contact the visitor while in the building in the event of an emergency.

Individual Access, Redress, and Correction

No update.

Technical Access and Security

No update.

Technology

In addition to the technology in place at TSA Headquarters and the TSOC, TSA field locations may use a scanner equipped with an OCR device to read the front of a visitor's government-issued ID. The device will capture the name and picture of the visitor. The extracted information is used to electronically prepare and print a badge which includes the visitor's picture.

Responsible Official

Russell Appleyard, Special Agent
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security