Privacy Impact Assessment
for the

Visitor Management System

October 19, 2007

Contact Point
Russell Appleyard
Office of Security/Physical Security Division
Transportation Security Administration
Russell.Appleyard@dhs.gov

Reviewing Officials

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAprivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Introduction

The Privacy Impact Assessment (PIA) previously published on July 14, 2006 is being amended to reflect the collection of a photograph to be placed on the temporary badge. The photograph will be stored in the system only for so long as is required to create the badge, then is deleted to create the next badge. This PIA replaces the previously published PIA.

The Transportation Security Administration (TSA) Headquarters Buildings and the Transportation Security Operations Center (TSOC) have been designated as Level IV federal facilities pursuant to the guidelines established in the 1995 Department of Justice directive entitled, "Vulnerabilities of Federal Facilities." Pursuant to direction from the Department of Homeland Security (DHS) Chief Security Officer (CSO), the security requirements applicable to Level IV facilities require TSA's implementation of certain security procedures to ensure a safe and secure work environment for TSA Headquarters employees and visitors. TSA's Office of Security has established a Security Appointment Center (SAC), which will utilize a Visitor Management System (VMS). 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.

The SAC and the VMS will generate temporary badges 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 SAC will collect the names of visitors to the TSA Headquarters Buildings and the TSOC prior to the date of the visit by means of an online form. This information will not be used to perform vetting of any kind or to run criminal, immigration or other checks on visitors.

Section 1.0

Information collected and maintained

1.1 What information is to be collected?

The personal information that will be collected by the SAC, through the online form is the visitor's first and last name. The TSA employee that is hosting the appointment will be required to provide date of visit, time of visit, location of visit, name of the employee to be visited, and employee office phone number. When the individual arrives at the facility, the individual will have a photograph taken to put on the temporary badge.

1.2 From whom is information collected?

The TSA employee scheduling or hosting the appointment will provide the SAC with the visitor's name subsequent to obtaining the information from the visitor. In the event a visitor arrives to either TSA facility without a pre-scheduled appointment, the visitor will be asked to wait while the TSA employee the visitor wishes to meet completes and submits the visit request form to the SAC. Upon entry in the VMS, the security officer will be informed that he or she may proceed with confirmation of the visitor's identity and issuance of a temporary paper badge with photograph.

1.3 Why is the information being collected?

TSA is collecting the names and photographs of visitors to the TSA Headquarters Buildings and the TSOC in order to confirm the visitors' identity and issue them a temporary badge. The information will not be used to perform threat assessments of any kind.

The VMS allows the Office of Security to: (1) issue a temporary paper badge with photograph which allows for the immediate identification of a visitor and eliminates the need for generic serialized plastic badges which are costly to replace, (2) ensure that an unauthorized individual does not gain access to the TSA Headquarters Buildings or the TSOC, (3) eliminate the use of hand-written visitor logs, (4) account for the visitors on the premises at any given time during the day, as the VMS can be used to generate a report identifying the visitors present in either TSA facility and allow the security guards to account for those individuals during an emergency, (5) generate statistical reports concerning visitors to the TSA Headquarters Buildings and the TSOC.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

TSA Management Directive 2800.7, "Issuance of TSA Headquarters Photo Access Pass," and TSA Management Directive 2800.6, "Transportation Security Operations Center Access Control," address the collection of information for the VMS.

Pursuant to these Management Directives, the Office of Security, Physical Security Division, is responsible for creating and maintaining an access control program. The access control program requirements stipulate that each visitor must be issued a valid temporary access pass in order to be granted access to the TSA Headquarters Buildings or the TSOC.

Privacy Impact Analysis

TSA chose to collect the minimum amount of information necessary to confirm the identities of visitors to TSA Headquarters and the TSOC and issue them temporary paper badges with photographs. The photograph ensures that the individual issued the badge is the correct person thereby improving accuracy and security.

Section 2.0

Uses of the system and the information

2.1 Describe all the uses of information.

The information will be used to register the visitor in the VMS for his or her upcoming appointment at the TSA Headquarters Buildings or the TSOC. It will allow the TSA security officer to verify the existence of an appointment and the TSA point of contact, and to print and issue a temporary paper badge with photograph.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

TSA expects visitors and employees setting up appointments to provide accurate information about themselves.

Visitors arriving for appointments are processed through the Visitors Center, the lobbies of the TSA Headquarters Buildings, or the TSOC. The visitor provides the security officer with an approved form of government issued photo identification (e.g., state driver's license, passport, military identification, or credentials). The security officer then matches the identification with the appointment information in the VMS and a temporary paper badge with photograph is issued to the visitor.

Inaccuracies will be manually corrected in the VMS database by either the security officer or SAC personnel prior to the issuance of the badge. For example, if a visitor's first name on his or her photo identification does not match the first name stored in the VMS database due to a misspelling, the error will be corrected in the computer and a badge will be issued. In the

event an error is discovered subsequent to the issuance of the badge, the error will be corrected in the VMS database and a new badge will be printed.

Privacy Impact Analysis

The name of the visitor is provided only to TSA employees and contractors who need access to this information in the performance of their official duties. The SAC program manager will monitor use of the VMS to ensure that personally identifiable information is protected and used solely for the purpose of allowing access to the TSA Headquarters Buildings or the TSOC.

Section 3.0

Retention

3.1 What is the retention period for the data in the system?

Hard copy versions of the records in the system are printed on a daily basis and will be destroyed two years after final entry or two years after date of document in accordance with General Records Schedule 18. Data will be stored in the VMS database in order to compile a statistical report which allows TSA to track the number of visitors it processed in a given day, week, and month for 30 days before being deleted. Photographs are retained only so long as necessary to create the temporary badge.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes. Specifically, the VMS system records are covered by GRS 18, section 17: Visitor Control Files, which has been approved by NARA for use throughout the government.

Privacy Impact Analysis

By following NARA's approved General Records Schedule 18, which requires agencies to retain visitor control files for two years, TSA ensures that personally identifiable information about visitors is kept for the shortest possible retention period.

.

Section 4.0

Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

As part of the operational component of VMS, personal information is shared internally with personnel in the Office of Security. Pursuant to TSA's mission, the Office of Security, Physical Security Division, is mandated to provide a safe and secure work environment, which is accomplished by contracting with a private security company. The security officers assigned to these TSA facilities play an integral part in the monitoring, processing and screening of visitors, and information in the VMS system is shared with these individuals in the performance of their assigned duties.

In addition, contract personnel are assigned to the Security Appointment Center (SAC). The personnel assigned to the SAC are essential to the processing of all incoming visit requests and entering the visit information into the VMS.

4.2 For each organization, what information is shared and for what purpose?

The names of visitors, as well as the name and contact information of the TSA employee setting up the appointment, is provided to SAC personnel in order to process visit requests. This information is also shared with the contracted security force for the purpose of confirming the identity of the visitor prior to granting access to either TSA facility. Photographs are not shared beyond that necessary to create the temporary badge.

4.3 How is the information transmitted or disclosed?

The information is disclosed to the contracted security force through the use of the VMS. The information contained in the visit requests submitted to the SAC for processing is transferred to the VMS database, either manually or by import, by the SAC personnel, enabling the security officers in the Visitors Center or lobbies to retrieve and view appointment information as it relates to each individual visitor upon arrival to either location.

Privacy Impact Analysis

Personally identifiable information from the VMS system will be shared only with those employees and contractors who need the information to perform their official duties. The SAC program manager, personnel contracted to enter data into the VMS, and security personnel

contracted to provide physical security at the TSA Headquarters Buildings and the TSOC have a need to know the personally identifiable information in the performance of their duties.

Safeguards that prevent unauthorized individuals from gaining access to personally identifiable information through the VMS are in place through the use of physical and technical security measures. These security measures will be discussed in Section 8.0.

Section 5.0

External sharing and disclosure

5.1 With which external organizations is the information shared?

In certain circumstances, TSA may share this information with Federal, state, and local law enforcement agencies and emergency response workers.

5.2 What information is shared and for what purpose?

Information from the VMS including visitor name, date of visit, and name of the employee visited may be shared with law enforcement agencies when relevant to an investigation into a theft or other potentially criminal incident. In the event of an emergency at a TSA facility, this information may also be shared with emergency response workers.

5.3 How is the information transmitted or disclosed?

Depending on the urgency and scope of the request, information may be disclosed manually, telephonically, or electronically.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

No, there is no MOU in place with any external organizations.

5.5 How is the shared information secured by the recipient?

Federal agencies are subject to the safeguarding requirements of the Privacy Act and under the Federal Information Security Management Act, Title III of the E-Government Act, Pub. L. 107-347 (FISMA). To the extent that information is shared with state or local agencies, TSA expects that information associated with a law enforcement investigation will be

safeguarded in accordance with procedures designed to protect such information, and that emergency response personnel will not retain the information except to confirm the safety of the individual. If any other information is necessary for emergency response, it will be obtained by the emergency responder directly from the individual.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

None.

Privacy Impact Analysis

External sharing of personal information in the VMS system will be limited to sharing with law enforcement agencies when relevant to an investigation, or emergency response workers in the event of an emergency at a TSA facility. It is expected that such disclosures will be rare.

Section 6.0

Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

No. All information in the VMS is stored and retrieved exclusively by date. Therefore, the VMS does not create a Privacy Act system of records and does not require a Privacy Act notice.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. Visitors may decide that they do not wish to provide their first or last name, or show an approved form of government issued photo identification upon arrival at either TSA facility. However, without this information, TSA cannot confirm the identity of the individual and cannot grant him or her access to the facility.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Yes. By providing the requested information, individuals consent to the use of the information in order to verify their identity and grant access to either TSA facility. There are no other uses made of this information.

Privacy Impact Analysis

The VMS system will collect limited personally identifiable information on visitors in order to verify their identities and grant them access to either TSA facility. Visitors have the option of declining to provide the information, but failure to provide proof of identity will result in TSA's inability to grant access to the facility.

Section 7.0

Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

In the event a visitor to the TSA Headquarters Buildings requests to see the form on which his or her name appears, the security officer will contact the SAC. The SAC personnel will retrieve a hard copy of the form and deliver it to the Visitors Center for viewing. In the event a visitor to the TSOC requests to see the form a facsimile will be transmitted from the SAC to the TSOC.

Visitors may request access to their information by submitting a FOIA request to TSA in writing at the following address:

Transportation Security Administration, TSA-20, West Tower
FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

FOIA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA request must contain the following information: full name, address, and telephone number. Provision of an e-

mail address is optional. For questions or assistance please refer to the TSA FOIA web site (http://www.tsa.gov/public/display?content=0900051980003b93).

7.2 What are the procedures for correcting erroneous information?

Inaccurate or erroneous information will be corrected in the VMS database either by the security officer, the SAC program manager, or SAC personnel when the error is discovered upon the visitor's arrival. In the event an error is discovered subsequent to the issuance of a temporary paper badge with photograph, one of the individuals named above will change the error in the VMS database and print a new badge.

7.3 How are individuals notified of the procedures for correcting their information?

Upon discovering a discrepancy, the security officer will either inform the visitor of the nature of the discrepancy or be informed of the discrepancy and explain that the discrepancy will be corrected in the VMS prior to issuance of a badge.

7.4 If no redress is provided, are alternatives available?

Inaccuracies may be corrected upon the visitor's arrival and discovery of the erroneous information. No additional redress procedures are necessary.

Privacy Impact Analysis

The SAC is collecting minimal personally identifiable information from visitors. The correction procedure is simple and straightforward. If the security officer or visitor notices a misspelling or other mistake with the visitor's name in the VMS, the correction will be made immediately.

Section 8.0

Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.

The SAC program manager, the contracted SAC personnel, technical security system

administrators, and the contracted private security officers will have access to the VMS system.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. Contractor personnel are responsible for entering information into the VMS. Further, contractor personnel provide private security at the TSA Headquarters Buildings and the TSOC, which involves the retrieval of information from the VMS when visitors arrive at either TSA facility.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. The TSA technical security administrators responsible for procuring the system and its components will have system administrator access privileges The SAC program manager and personnel, as well as the contracted private security officers, will have program administrator access privileges which are more limited. The SAC program manager and personnel access privileges include, but are not limited to, the ability to pre-register visits in the VMS, retrieve appointment information, make certain amendments or changes to the visit information stored in the VMS database, generate reports, sign-in a visitor, issue a temporary paper badge with photograph, and sign-out a visitor. The contracted private security officers have the ability to retrieve appointment information, make certain amendments or changes to the visit information stored in the VMS database, sign-in a visitor, issue a temporary paper badge with photograph, and sign-out a visitor.

All user actions are traceable to individual accounts, whether the action is by a system administrator, program administrator, or security officer. The software employed for purposes of this system, Passage Point, maintains an audit trail for each visit detail. The audit trail includes information about the date, time, and location of the visit record's creation, as well as information about the user that created the record. Any subsequent change or amendment to the visit record is a separate item in the audit trail and is referred to as an "update." The date, time, and location of the update, as well as the particular user responsible for the update are part of the audit trail as well.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Each terminal permitting access to the VMS is password protected, thus allowing access by authorized users only. In addition, the level of access permitted at each terminal is configured

based on the type of user: technical security administrator, SAC program managers and personnel, and security officers.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The actual assignments of roles and rules are verified through user identification and password protection, which are current TSA Information Technology security procedures.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Auditing measures will be conducted using established Management Control Techniques published in TSA Management Directives 2800.6 and 2800.7. The technical safeguards in place to prevent misuse of data are as follows:

- Password protection for e-mail which sends files among personnel with a need to know in the course of their official duties.
- Password protection for files containing personal data to prevent unauthorized internal and external access.
- Network firewalls to prevent intrusion into DHS network and TSA databases.
- User identification and password authentication to prevent access to the VMS database by unauthorized users.
- Security auditing tools to identify the source of failed TSA system access attempts by unauthorized users and the improper use of data by authorized operators.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All TSA employees and contractors needing access to the system are required to complete annual online privacy training. In addition, as part of VMS training, all users are informed that any TSA information to which they are granted access shall be used only for the purpose of carrying out the provisions of their contract. Information retrieved through the VMS shall not be divulged or made known, in any manner to any person, except as may be necessary in the performance of their contract.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Data is secured in accordance with FISMA requirements. The Certification & Accreditation was last completed on June 30, 2004 by certifying authority TSA's Chief Information Security Officer, Office of the Chief Information Officer.

Privacy Impact Analysis

Role-based access controls are in place for contractors entering data into the VMS, as well as security personnel retrieving information from the VMS. System administrators will have unlimited access privileges to the VMS. The Program Manager and SAC personnel will have the ability to enter data into the VMS and make changes as needed. Security officers will have the lowest level of access privileges of all users of the VMS. TSA will conduct regular audits of the system.

Access to the SAC is limited to authorized personnel through the use of a proximity card reader outside the Office of Security door. Once inside the SAC, access to the VMS terminals is limited through password protection. Access to the VMS for security personnel retrieving data is limited to the officers assigned to the TSA Headquarters Buildings Visitors Center and lobby security posts, and the TSOC main gate and lobby posts. Only the aforementioned officers will have passwords to access the VMS.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The VMS and PassagePoint 4.5 software were purchased and installed in existing computer hardware.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The VMS and PassagePoint 4.5 software and hardware were ultimately chosen because they offered the highest level of lobby security and visitor management. The VMS operates on a closed and certified network. Additionally, it allows for identification and authentication control mechanisms to be put in place that support the minimum requirements of access control, least

privilege, and system integrity.

9.3 What design choices were made to enhance privacy?

The system was chosen because the design enhances privacy by allowing for the following: (1) limited data collection without compromising the integrity of the system or its functionality, (2) using "roles" to assign access privileges to users of the system, (3) ensuring access by only authorized users and preventing misuse of the data stored in the VMS database, and (4) using a detailed audit trail to trace all actions to individual accounts, whether the action is performed by a system administrator, program administrator, or security officer.

Conclusion

TSA believes the use of the VMS will enhance the physical security at the TSA Headquarters Buildings and the TSOC contributing to the goal of ensuring a safe environment for TSA employees, contractors, and visitors. TSA's implementation of the system will entail the collection of a minimal amount of personally identifiable information from visitors, and will be used in order to verify the identity of visitors and issue temporary paper badges with photographs. TSA has adopted and carried out strict data security and privacy protections, including prohibitions on the access of personal data by TSA employees and contractors without an official need to know, and the use of personal information for any purposes other than for the VMS system. Additionally, the VMS system will employ real time auditing procedures to determine when data has been accessed and by whom. By implementing strict rules for oversight, training personnel handling the data, and employing a strong auditing system to detect potential abuse, TSA will continue to ensure that privacy is an integral part of the program once it becomes operational.

Responsible Officials

Russell Appleyard
Office of Security/Physical Security Division
Transportation Security Administration

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security