Federal Trade Commission
Privacy Impact Assessment

for the:

Visitor Management System

January 2012

1 System Overview

The Federal Trade Commission (FTC) Security Office is establishing a Visitor Management System (VMS), which will be used to maintain an electronic log of visitors to the FTC's Washington, DC, headquarters buildings. These (FTC) buildings have been designated as Level IV Federal facilities pursuant to the guidelines established in the 2010 Interagency Security Committee standard entitled, "*Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard.*" Pursuant to direction from the FTC Chief Security Officer (CSO), the security requirements applicable to Level IV facilities require FTC's implementation of certain security procedures, such as the VMS, to ensure a safe and secure work environment for FTC headquarters employees and visitors. The VMS uses a commercially available software package installed on in-house agency IT equipment, and will replace the current paper visitor logs used by the FTC's security staff. Information about visitors who have scheduled appointments with agency officials or staff can be entered into the system prior to their visit in order to expedite their check-in process when they arrive. The system will also enable FTC security staff to print out temporary paper identification badges with each visitor's photograph on his or her badge, in lieu of the current handwritten badges.

By controlling and limiting the issuance of official temporary badges through VMS, the system will help ensure that such badges are only issued to those individuals authorized to be in an FTC facility on a given day.

2 Information Collected and Stored within the System

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

2.1 What information is to be collected, used, disseminated, or maintained by the system?

The VMS will include the following data fields:

Field	Status
Last Name	Active
First Name	Active
Middle Initial	Active
Date of Birth	Inactive
Company Name	Active

Title	Active
Telephone	Inactive
ID Verified	Active
Building /Site	Active
Room	Active
Contact Name	Active
Contact Phone	Active
Email	Inactive
ALT Contact Name	Active
Alt Contact Phone	Active
Last Visit: From	Active
Last Visit: Until	Active
Access Card List	Inactive
Badge Style	Inactive
Parking Area	Inactive
Make/Color	Inactive
Plate Number	Inactive
State	Inactive
Authorized By	Active
Purpose of visit	Active
Details	Active
Prior/Past Visit(s)	
Date	Active
Contact Name	Active
Alt Contact Name	Active
Authorized By	Active
Building /Site	Active

Room	Active

In addition, when the individual arrives at the facility, the individual will have a photograph taken, which is maintained by the VMS solely to print out the photo on the visitor's temporary badge, and then deleted by the system, as noted below. Each visitor will also be required to show some form of personal Government-issue photo identification (e.g., driver's license) so that the FTC can verify the visitor's information in the system, but that identification will not be used to collect additional information (e.g., driver's license number or Social Security number) from the visitor.

2.2 What are the sources of the information in the system?

The sources of information are the FTC employee who has invited the visitor and the visitor.

2.3 Why is the information being collected, used, disseminated, or maintained?

The information in the VMS is collected and maintained in order to confirm the visitors' identities, issue them temporary badges, and maintain records of such visits for building access and security purposes. The information will not routinely be used to perform criminal, immigration, or other background checks or threat assessments in order for the individual to gain admittance to the facility. Collection of this information also expedites visitor processing.

In particular, the VMS allows the FTC to: (1) issue a temporary paper badge with photograph to the visitor, which allows for the immediate identification of that visitor and eliminates the need for generic serialized plastic badges, which are costly to replace; (2) help ensure that an unauthorized individual does not gain access to FTC headquarters facilities; (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 an FTC facility and allow the security guards to account for those individuals during an emergency; and (5) generate statistical reports concerning visitors to the FTC headquarters buildings.

2.4 How is the information collected?

Information about a visitor will normally be obtained by the FTC employee who has invited the individual, and forwarded to the Security Office (normally by e-mail) for manual data entry by that Office into the system. (FTC security desk staff will then have access to the VMS at designated building entrances.) The FTC Contract Security officers will also be able to directly input information into the systems for visitors who arrive unannounced. As noted earlier, information will be verified from the visitor's Government-issued photo identification (e.g., driver's license) when presented by the visitor at the time of his or her arrival at the FTC facility.

2.5 How will the information be checked for accuracy and timeliness (currency)?

FTC expects visitors and employees setting up appointments to provide accurate information about themselves. As noted, the visitor will be asked to show an approved form of government-issued photo identification (e.g., state driver's license, passport, military identification, or credentials). The security officer will then match the identification with the appointment information in the VMS.

Inaccuracies will be manually corrected in the VMS database by either the security staff at the FTC building entrance desk or the FTC Security Office staff prior to issuance of the badge. In the event an error is discovered after issuance of the badge, the error will be corrected in the VMS database, a new badge will be printed, and the incorrect badge will be destroyed.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

Yes, the FTC has not previously used a commercial software and hardware system to establish a VMS. See section 2.8 below regarding how this technology might affect individuals' privacy and how such privacy risks are being mitigated.

2.7 What law or regulation permits the collection of this information?

- 5 U.S.C. § 301, Government Organization and Employees
- Section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. § 1441)
- Executive Order 12977, Interagency Security Committee
- Homeland Security Presidential Directive-7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection
- National Infrastructure Protection Plan
- Government Facilities Sector Sector-Specific Plan
- Interagency Security Committee Standard: Physical Security Criteria for Federal Facilities, April 12, 2010; and
- Federal Property Regulations, July 2002.

The FTC Security Office 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 FTC headquarters buildings or its satellite locations.

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Currently the FTC uses a paper-based system to gather this information. The FTC has not identified any conversion risks, as it will not be transferring data from those paper logs to the VMS.

The VMS will collect a photograph in addition to what the paper-based log system collected. An electronic system, however, potentially raises other privacy risks that are not necessarily raised by a paper-based system. In particular, an electronic system that is widely distributed on a agency network without proper access controls or other appropriate safeguards could be more vulnerable to data theft, breach, or misuse.

The FTC has minimized or eliminated these risks in the following ways. First, it has installed the system on a closed, stand-alone set of IT equipment (server and terminals). Second, the system is physically and logically accessible only to a very small number of FTC Security Office staff and building security staff (i.e., security guards at designated FTC entrances). Third, all personnel that utilize the system have background investigations conducted by the Federal Protective Service (FPS) or the Office of Personnel Management (OPM) to assist in determining their trustworthiness in handling the information. Fourth, system data cannot be readily downloaded, e-mailed, or otherwise transferred out of the system. The CD drives and thumb drive readers on the VMS work stations have been turned off so that they cannot be used to copy material from the system. The workstations are not on the FTC network so they do not have access to the internet and cannot be used to email information outside of the system.

The vendor will train the FTC Security Staff on the use of the system. It will be the responsibility of the FTC Security Office to train the contract guard force on the use of the system. All FTC Security Office users and all contract officer personnel will be required to sign applicable rules of behavior prior to being issued a password to use the system.

The Site Secure Domain Controller server and System Server maintain the information used by the VMS system and are located in the FTC Security Command Center. The Command Center is under video surveillance and has a 24-hour armed guard. Furthermore, terminals at guard desks that can be used to access the VMS are under continuous 24-hour video surveillance. Finally, as noted earlier, the information collected on visitors is limited to basic identifying information. Thus, the potential privacy risk, if any, appears to be minimal in the event of unauthorized use, access, or loss.

The VMS should result in greater control over the issuance of badges, because they can only be printed and issued from the system (and not simply handwritten) and will contain an individual photo. These features are more likely to prevent an individual visitor from being impersonated.

3. Use and Access to Data in the System

The following questions are intended to clearly describe how the information in the system will be used, and who will use it.

3.1 Describe how information in the system will or may be used.

As already discussed, the information will be used to register visitors in the VMS for their appointments. It will allow the FTC to verify the existence of an appointment, the FTC point of contact, and to print and issue a temporary paper badge with a photograph. The system also will allow the guards to input a visitor who arrives unannounced, input who their FTC point of contact is and make a badge with a picture.

Information may also be used to compile a statistical report, which allows FTC to track the number of visitors it processed in a given day, week, and month for 30 days.

3.2 Which internal entities will have access to the information?

The FTC Security Office staff and approved system users (i.e., security guards) will have access to this information. Departments or bureaus within the FTC that are conducting authorized internal investigations (i.e. OIG) may have access to the information contained in the system.

3.3 Which external entities will have access to the information?

No external entities are authorized as system users. In certain circumstances, however, FTC may be asked to share information with Federal, State, and local law enforcement agencies when relevant to an investigation into a theft or other potentially criminal incident. In the event of an emergency at a FTC facility, this information may also be shared with emergency response workers. Such information would need to be downloaded by authorized internal users, and approved for sharing through formal agency internal procedures for interagency access requests. See 16 C.F.R. 4.11(c), (d). Likewise, it is possible that system data could be the subject of legal process or other requests by external individuals or entities under the Freedom of Information Act (FOIA), discovery in court litigation, Congressional requests or otherwise. Such requests do not result in automatic access, and would also need to be formally granted or denied through the agency's internal procedures cited above.

4 Notice and Access for Individuals

The following questions are directed at how or whether the individual is notified of the scope of information collected. They also concern the individual's right to consent to uses of information, right to decline to provide information, ability to ensure the accuracy of the information collected, and right to access their information.

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

The FTC employee scheduling the visitor's appointment will normally inform the individual of the collection of information. Further information about how the FTC's uses personal information we collect is contained in the FTC's privacy policy, www.ftc.gov/ftc/privacy.shtm. As discussed in section 8 below, there is also a Privacy Act system of records notice that explains the routine uses of the data in this specific system. In addition, Privacy Act statements are being made available at security guard desks to inform individuals of what visitor log information is collected by the FTC and how it is used.

4.2 Do individuals have the 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 FTC's facilities; however, without this information, FTC cannot confirm the identity of the individual and cannot grant him or her access to the facility.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

If the individual agrees to submit the information, the individual does not have a right to determine its uses by the agency, which is explained in the agency's privacy policy and Privacy Act system notice, as noted earlier. The individual, however, does have the right to consent as to whether he or she will provide the information, which is a condition of being granted access to FTC facilities.

4.4 What are the procedures that allow individuals to gain access to their own information?

Visitors do not have access to the VMS, which is limited to internal users described earlier (FTC Security Office and security guards). Visitors may request access to data in the system about them, if any, by submitting a FOIA request to FTC in writing at the following address:

Freedom of Information Act Office
Federal Trade Commission
600 Pennsylvania Avenue, NW, room H-585
Washington, DC 20580

FOIA requests may also be submitted by fax at: 202-326-2477. The FOIA request must contain

the following information: full name, address, and telephone number. Provision of an email address is optional. Please visit the FTC's page for full details on filing a request: http://www.ftc.gov/foia/index.shtm.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Since visitors do not have access to the VMS, there are no privacy risks associated with such access.

5 Web Site Privacy Issues

This section is not applicable to the VMS. The system is not accessible, and does not collect or maintain information, through any Web site, page, or online form on the Internet.

6 Security of Information in the System

The following questions are intended to describe technical safeguards and security measures.

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

Yes. The VMS operates on a closed 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.

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

The VMS resides on a FISMA system that has a current Certification & Accreditation.

6.3 Has a risk assessment been conducted on the system?

The VMS resides on a FISMA system that has a current risk assessment.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

No.

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

An FTC security technician is the administrator responsible for the system and its components. This technician will have system administrator access privileges. The CSO, security staff, and contracted private security officers will have access privileges which are more limited. The CSO, and security staff 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 visitor 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. These roles are documented in the FTC Security Office.

All user actions are traceable to individual user accounts, whether the action is by a system administrator, security office staff, or security officer. The software employed for purposes of this system, Site-Secure, 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.

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, security office staff personnel, and security officers.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC employees and contractors needing access to the system are required to complete annual online privacy training. In addition, as part of VMS training, all security officers are informed that any FTC 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.

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

The following in-place auditing measures and technical safeguards are applied to prevent misuse of data. The Security Office constantly evaluates new technologies and procedures to enhance these capabilities. These controls include:

Authenticator/Password Management -- Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.

Account Management -- Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of need-to-know.

Access Enforcement -- Application and monitoring of access privileges.

Least Privilege -- Provision of the minimum tools required for a user to perform his/her function.

Stand-alone-system to prevent intrusion into FTC security network databases.

Unsuccessful Login Attempts -- System automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempts is exceeded.

Audit trails are generated by system applications. The audit trails facilitate intrusion detection and are a detective control for identifying data misuse. The system also is configured to protect audit information and tools from unauthorized access, modification and deletion. Audit notifications are generated in response to pre-specified triggers.

The audit files are reviewed monthly to ensure only authorized personnel are accessing the files. In addition the ports on the desk tops are configured so as not to allow them to be used to save data to an outside source.

Finally, all personnel that have access to the system have background checks conducted on them. The minimum level of background check is an National Agency Check with Inquiries (NACI).

6.8 Questions regarding the security of the system.

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7 Data Retention

This section addresses for how long data is maintained, and how and when it is disposed of.

7.1 For what period of time will data collected by this system be maintained?

There are two tables in the system. One is the visitor table. The visitor table will contain the information entered in the active data fields listed in section 2.1 above, including the active data fields for past visit(s). The visitor table also includes the photographs taken of visitors when they arrive at the FTC facility. Information in the visitors table is set up to delete 30 days after the visitor's most recent visit. Visitors returning outside of this 30 day window will have to be reentered into the system.

Hard copy versions of the information in the visitors table are printed on a daily basis and will be destroyed two years after final entry or two years after the date of the document, in accordance with General Records Schedule 18, applicable to security and protective service records maintained by Federal agencies. The hard copy versions do not include the photographs taken of visitors.

The second table in the system is the audit log. The audit log maintains the names of visitors and the date they entered the facility. The purpose of this feature is to be able to recall the names of visitors that entered the facility on a given day in case of an incident. The vendor is configuring the system so that information in the audit log is deleted after one year.

7.2 What are the plans for destruction or disposal of the information?

All data will be deleted/destroyed in accordance with Office of Management and Budget, National Archives and Records Administration and National Institute of Standards and Technology regulations and guidelines.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

See Section 2.8 for information regarding privacy risks identified in the data retention. No

privacy risks have been identified in the disposal of the data.

8 Privacy Act

This section addresses the applicability of the Privacy Act of 1974 to the system, and whether or not the system is covered by a System of Records Notice (mandated for some systems by the Privacy Act of 1974).

8.1 Will the data in the system be retrieved by a personal identifier?

Yes. Authorized system users (e.g., security guards) pull up (i.e., retrieve) visitor appointment records from the system by visitor name when the individual arrives at the FTC facility.

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

Yes. See FTC II-11, Personnel Security, Identity Management, and Access Control Records System–FTC, which can be read here: http://www.ftc.gov/foia/sysnot/ii-11.pdf.

9 Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

The VMS will collect, use and disclose information in a manner that is consistent with FTC's privacy policy. The VMS will enhance the physical security at the FTC facilities, contributing to the goal of ensuring a safe environment for FTC employees, contractors, and visitors. FTC'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. FTC has adopted and carried out strict data security and privacy protections, including prohibitions on the access of personal data by FTC 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, FTC will continue to ensure that privacy is an integral part of the program once it becomes operational.

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date:_____
Charles King
CS)/System Owner

Review:

_____ Date:_____
Alexander C. Tang
Office of the General Counsel

_____ Date:_____
Peter Miller
Acting Chief Privacy Officer

_____ Date:_____
Jeffrey Smith
Information Assurance Manager

_____ Date:_____
Jeffrey Nakrin
Records and Filings Office

Approved:

_____ Date:_____
Jeffrey Huskey
Chief Information Officer