Privacy Impact Assessment
for the

Foreign National Visitor Management System (FNVMS)

March 30, 2011

Contact Points
David Colangelo
Security System Division, Office of the Chief Security Officer
Management Directorate
(202) 447-5320

Leo Wisniewski
Internal Security and Investigations Division, Office of the Chief Security Officer
Management Directorate
(202) 254-6495

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Foreign National Visitor Management System (FNVMS), a module hosted on the Department of Homeland Security (DHS) Integrated Security Management System (ISMS) information technology (IT) platform, is a risk assessment tool that provides the DHS with an application to log, track, and review non-U.S. Persons (foreign nationals) who visit or perform work at DHS facilities.

Overview

The FNVMS is a risk assessment tool that provides DHS with the ability to log, track, and review foreign nationals who visit or perform work at DHS facilities.

The FNVMS enables the DHS Office of the Chief Security Officer (OCSO) to track checks conducted with one or more U.S. Government agencies to determine whether adverse information exists on a foreign national visiting a DHS facility or personnel. The DHS component sponsoring the visit collects information regarding the foreign national from the individual or a representative of the Embassy of the country or company the individual represents. The information may be provided telephonically to a DHS employee, via e-mail, or fax. The DHS component sponsoring the visit enters this information directly into the FNVMS. OCSO personnel then provide this information to the security office or representative of the DHS employee who is hosting the visit. This enables the individual hosting the visit to make a risk-based assessment on whether to host the visit. Access to the FNVMS is granted to DHS employees or contactor employees who have been identified by their supervisors as requiring access to perform their assigned duties. All individuals granted access have been cleared for access to sensitive and/or classified information. Furthermore, access to FNVMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege (i.e., user access is limited to that information necessary to accomplish his/her duties).

Information collected on foreign national visitors to the Department maintained in FNVMS may include: name; known aliases; organization being represented, title, or position held; date of birth; place of birth; passport number and photograph; country of citizenship; country sponsoring the visit, visa information; the stated reason for the visit; and the DHS component sponsoring the visit. Also recorded will be information on the DHS employee or contractor designated as the point-of-contact for the hosting component. This information will include the employee's or contractor's name, telephone number, and office or program name.

The FNVMS is a DHS enterprise application and is currently in use by DHS Headquarters, US Customs & Border Protection (CBP), US Citizenship and Immigration Service (USCIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), US Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), and the US Secret Service (USSS).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The DHS Chief Security Officer (CSO) is responsible for developing and implementing security policies, programs, and standards to protect and safeguard the Department's personnel, property, facilities, and information. To do this, the OCSO has established access control policies designed to limit access to DHS facilities to authorized individuals. In order to know if an individual is authorized access to a facility, the identity of the individual must be established. OCSO does this by obtaining PII related to the individual and then conducting appropriate checks of records maintained by DHS and other U.S. government agencies. Authorities associated with protecting federal property and information include:

- 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;"
- Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security;"
- Presidential Decision Directive 12, "Security Awareness and Reporting of Foreign Contacts;"
- 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.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following DHS SORN applies to information on DHS employees and contractor employees as well as foreign nationals in FNVMS:

Department of Homeland Security/All—024 DHS Facility Access Control and Visitor Management, Federal Register: February 3, 2010, (Volume 75 5609) and Final Rule for Privacy Act Exemptions August 24, 2009, Federal Register (Volume 74 42578).

The following Privacy Act SORN applies to information on DHS employees or contractor employees contained in the FNVMS:

Department of Homeland Security/All-023 Personnel Security Management Systems of Records, Federal Register: February 23, 2010 (volume 75, Number 35, pages 8088-8092).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan has been completed for ISMS IT platform that hosts the FNVMS. A security certification authorizing the Authority to Operate (ATO) was granted on April 21, 2008, by the DHS Information Systems Security Manager Certifying Official. The ISMS Federal Information Security Management Act (FISMA) ID is ISD-03501-MAJ-03501.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

FNVMS adheres to the following NARA General Records Schedules (GRS):

- GRS 11, Space and Maintenance Records, item 4a, identification credentials including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room and visitors' passes, and other identification credentials are destroyed three months after return to issuing office.
- GRS 18, Security and Protective Services Records, item 17 registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers for areas under maximum security are destroyed after final entry or five years after date of document, as appropriate.

Where records are used as evidence in an investigation or in an administrative, litigation, or other proceeding, the records will be retained until final disposition of the investigation or proceeding.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

OCSO is working with the PRA program management office to address clearance requirements.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Information collected on foreign national visitors contained in FNVMS may include:

- name;
- known aliases;
- organization being represented;
- title or position held;
- date of birth; place of birth;
- passport number and photograph;
- country of citizenship;
- country sponsoring the visit;
- visa information;
- the stated reason for the visit; and
- the DHS component sponsoring the visit.

The FNVMS also records information on the DHS employee or contractor employee designated as the point of contact for the hosting component. This information may include the employee's or contractor employee's name, telephone number, and office or program name. To confirm the identity of the sponsoring employee or contractor, the FNVMS accesses the employee's or contractor's personnel security record in the ISMS Personnel Security Module. The employee's or contractor employee's personnel security record contains their name, SSN,[1] and contact information used to verify the sponsoring individual's identity within the ISMS Personnel Security Module.[2]

FNVMS also has a Concur/Non-Concur function since OCSO does not approve or disapprove a visit; this decision rests with the host component. In most cases, a Non-Concur means information has been developed during the check which will require that the host receive a briefing from OCSO.

[1] The SSN is needed in order to verify sponsoring individual's identity within the ISMS Personnel Security Module. Authority for collection of the SSN is Executive Order 13467 and 5 CFR Parts 731 and 732.

[2] Information on DHS employee's and contractor employee's PII accessed by the FNVMS is contained in the DHS PIA titled; "Integrated Security Management System" and DHS Systems of Records Notice DHS/All-023, Personnel Security Management System of Records, Federal Register: February 23, 2010 (Volume 75, Number 35, pages 8088-8092).

2.2 What are the sources of the information and how is the information collected for the project?

Information regarding foreign nationals is collected from the individual or a representative of the Embassy of the country or company the individual represents. The information may be provided telephonically to a DHS employee, via e-mail, or fax. The DHS component sponsoring the visit is responsible for obtaining the information and entering it into the FNVMS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Information concerning foreign nationals is not obtained from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Information is collected directly from the foreign nationals or their representative and verified for accuracy by checking the information against information collected and maintained by U.S. government agencies. In most cases, the information provided by the foreign national is the same as that on their passport or visa application.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk associated with the accuracy of foreign national names in the FNVMS. Translation errors may occur when a foreign national name is adapted from its native alphabet to the modern Latin alphabet (as prescribed in International Organization for Standardization (ISO), International Electrotechnical Commission Standard 646) for entry into FNVMS. Name translation errors could result in misidentification of the foreign national requesting access to DHS facilities.

Mitigation: To minimize risks associated with translation errors additional information, such as date of birth or country of citizenship is requested in order to validate a foreign national's identity.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The DHS CSO is responsible for developing and implementing security policies, programs, and standards to protect and safeguard the Department's personnel, property, facilities, and information. To do this, the CSO and the OCSO has established access control policies designed to limit access to DHS facilities to authorized individuals. In order to know if an individual is authorized access to a facility the identity of the individual must be established. OCSO does this by obtaining PII related to the foreign national and then conducting record checks with other U.S. Government agencies.

Information in the FNVMS enables the DHS OCSO to track checks conducted with one or more U.S. Government agencies to determine whether adverse information exists on a foreign national visiting a DHS facility or personnel. This information is needed for the protection of DHS facilities, personnel, and information.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

There are no in-built data analysis functions to identify patterns or new areas of concern. The system does, however, have the ability to collate information on foreign national visitors.

3.3 Are there other components with assigned roles and responsibilities within the system?

The FNVMS is a DHS enterprise application and is currently in use by DHS Headquarters, CBP, USCIS, FEMA, FLETC, ICE, TSA, and the USSS. The component sponsoring a foreign national visitor is responsible for obtaining the information on the visitor and uploading it to the FNVMS via a secure interface portal.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There are a minor risks associated with the handling of PII and system security risks. Privacy risks associated with the handling of PII occur when data is extracted from the system and the individual using the data improperly distributes or stores the data. Privacy risks associated with system security concern an "insider threat" where an individual authorized access to the system conducts unauthorized activities, e.g., attempting to access information for which they do not have permission.

Mitigation: To address these risks the following controls and mitigation strategies are in place:

- Handling of PII

- A Data/Report request form must be completed, signed, and approved by the requester, requester's manager and their Division Chief prior to the creation and/or distribution of personnel security data, to avoid accidental, inappropriate or unauthorized use of the data;
- Access to information is granted on a "need to know" basis;
- Access to FNVMS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
- FNVMS user accounts are individually approved by the Chief, OCSO, Internal Security and Investigations (ISID) Division;
- All users have received DHS Computer Security training and have been vetted and/or cleared for access to privacy, sensitive, and/or classified information;
- Access to FNVMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access; and
- Write capability, which is limited to a few roles, is tracked and audited.

- System Security

  - When information is stored as an attachment on the server, file access will be restricted by file permissions to prevent access by those without an appropriate requirement for access;
  - All automated data processing equipment supporting the application environment is located in a DHS data center;
  - Specific security roles have been defined and implemented within the application to control access to information;
  - A system security certification was performed and obtained in accordance with the Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources; and
  - Network access to the application is made via a Secure Sockets Layer (SSL) connection to the ISMS environment.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Information is generally collected directly from the foreign national or his representative with notice provided in written or verbal form at the time PII is collected. A privacy statement is contained on the data collection tool or e-mail message provided to the foreign national or the

representative of the foreign national (e.g., Embassy personnel). See Appendix.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Foreign national visitors invited or requesting to visit DHS facilities are advised that access control procedures require the submission of their PII. They are also advised that DHS will use this information to vet them to determine if access may be granted to a DHS facility or program and that failure to furnish the requested information may delay or prevent their access.

4.3 Privacy Impact Analysis: Related to Notice

The foreign national visitor from whom the data is collected may use a representative (e.g., Embassy staff) to provide the data. Accordingly, there is a risk that the representative may not convey the e(3) statement explaining why DHS is requesting the information and how the information will be used and stored. This PIA serves as an additional notice as well as a further explanation regarding the way DHS receives and manages FNVMS data. Notice is also provided through DHS/All-024, Facility and Perimeter Access Control and Visitor Management System of Records.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Information on foreign nationals visiting DHS facilities is retained in accordance with the following General Records Schedule (GRS):

GRS 18, Item 17, registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers for areas under maximum security are destroyed five years after final entry or five years after date of document, as appropriate.

Pursuant to GRS 11, Item 4a, identification credentials including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room and visitors' passes, and other identification credentials are destroyed three months after return to issuing office.

Where records are used as evidence in an investigation or in an administrative, litigation, or other proceeding for a foreign national or DHS employee or contractor employee, the records will be retained until final disposition of the investigation or proceeding.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: The privacy risks associated with the retaining or sharing this information is the possible dissemination of PII to unauthorized external entities.

Mitigation: This risk is mitigated by DHS limiting the sharing of this information to those who have an official need to know.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

FNVMS information is shared outside DHS as part of normal operations for conducting record checks on the individual with other U.S. government agencies. The U.S. government agency to which the information is sent uses the information to search its records for information about the subject. Each agency maintains its records in accordance with its privacy policies. Some record checks are conducted with U.S. government agencies that maintain national security systems consistent with the requirements of Executive Order 12333, as amended, "United States Intelligence Activities."

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Routine uses of the records in the FNVMS associated with foreign nationals accessing DHS facilities are addressed in DHS SORN/All—024 DHS Facility Access Control and Visitor Management, Federal Register: February 3, 2010, (Volume 75 5609) and Final Rule for Privacy Act Exemptions August 24, 2009, Federal Register (Volume 74 42578).

6.3 Does the project place limitations on re-dissemination?

The FNVMS enables the DHS OCSO to track checks conducted with one or more U.S. government agencies to determine whether adverse information exists on a foreign national visiting a DHS facility or personnel. The information provided by DHS to other U.S. government agencies to conduct the record checks may be maintained or used by those agencies in accordance

with that agency's guidelines and Privacy Act requirements.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

FNVMS tracks the checks conducted with other U.S. government agencies concerning a foreign national requesting access to a DHS facility or program. A FNVMS data field identifies those agencies from which DHS requested information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: As discussed in Section 3.4, there is the potential for an individual authorized to access the system conducts unauthorized activities, e.g., attempting to access information or extracting and sharing information for which they do not have permission.

Mitigation: To address this risk the following controls are in place:

- A Data/Report request form must be completed, signed, and approved by the requester, requester's manager and their Division Chief prior to the creation and/or distribution of personnel security data, to avoid accidental, inappropriate or unauthorized use of the data;
- Access to information is granted on a "need to know" basis;
- Access to FNVMS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
- FNVMS user accounts are individually approved by DHS, OCSO, ISID Chief;
- All users have received DHS Computer Security training and have been vetted and/or cleared for access to privacy, sensitive, and/or classified information;
- Access to FNVMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access; and
- Write capability is limited to a few roles, is tracked and audited.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Pursuant to the Privacy Act, individuals can access information they have provided to DHS. Privacy Act requests for access to an individual's record must be in writing and may be addressed to the DHS FOIA/PA, The Privacy Office, U.S. Department of Homeland Security,

245 Murray Drive SW, STOP-0550, Washington, DC 20528-0550. Requests should conform to the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS: The request should include a description of the records sought, the requestor's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received. After conferring with the appropriate DHS office, applicable exemptions may be waived in appropriate circumstances where it would not appear to interfere with or adversely affect the law enforcement or national security missions of DHS.

Most records in the system concern foreign nationals who visit or work at DHS facilities. The record for the foreign national visitor is linked to the DHS employee or contactor employee – a U.S. Person – who sponsors the visit. Therefore a "mixed system" has been created that collects, maintains, and disseminates information in an identifiable form about U.S. Persons and non-U.S. Persons. Accordingly, as a matter of Department of Homeland Security (DHS) policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system is treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Foreign national visitors are notified of the procedures to address possible inaccurate or erroneous information through this PIA and the DHS Privacy Office website.

7.3 How does the project notify individuals about the procedures for correcting their information?

Foreign national visitors are made aware of redress procedures through this PIA and the DHS Privacy Office website.

7.4 Privacy Impact Analysis: Related to Redress

There are no redress procedures beyond those described above and afforded under the Privacy Act, the DHS mixed systems policy, and FOIA.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The FNVMS is on the ISMS IT platform. Access to the ISMS IT platform and FNVMS information is via an authenticated web interface. Access control is role-based and data is only accessible if a specific user has been approved for access to the data. Information presented on screens is defined based on specific roles and information required to facilitate those functions. Permissions can be assigned to a specific role having either "read-only" or "edit" capability. Additionally, ISMS provides the ability to mark specific records as "Limited Access" and only those users with Limited Access privileges can view those records.

The system has auditing capabilities that stamps who, when, and what changes were made to a given record. Periodic reviews are conducted on the application of user roles and administrative actions are conducted by the ISMS Support team.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS employees and assigned contractor staff receive appropriate privacy and security training, and have undergone necessary background investigations and/or security clearances for access to sensitive, privacy, or classified information or secured facilities. DHS ensures this through legal agreements with its contractors and enforcement of internal procedures with all DHS entities involved in processing the background checks. Additionally, robust standard operating procedures and system user manuals describe in detail user roles, responsibilities and access privileges.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

FNVMS user accounts are individually approved by DHS, OCSO, ISID Chief. All users must have received DHS Computer Security training and have been vetted and/or cleared for access to privacy, sensitive and/or classified information. Furthermore, access to FNVMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The ISMS IT platform that hosts the FNVMS establishes data sharing agreements with external entities using Interconnection Security Agreements (ISAs). DHS 4300A, Sensitive System Handbook, September 2008, establishes this requirement for DHS systems. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/Designated Accrediting Authority (DAA). The ISA documents the security protections that must operate on interconnected systems to ensure

that transmissions between systems permit only acceptable transactions. The ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The DAA for each organization is responsible for reviewing and signing the ISA.

Responsible Officials

David Colangelo
Chief, System Security Division
Management Directorate, Office of the Chief Security Officer
Department of Homeland Security

Leo Wisniewski
Chief, Internal Security and Investigations Division
Management Directorate, Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

Original signed version on filed with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Privacy Act Statement:

Authority: Executive Order 12977, "Interagency Security Committee," and Interagency Security Committee Standard, "Physical Security Criteria for Federal Facilities" authorizes the collection of this information.

Purpose: DHS will use this information to vet foreign nationals to determine if access may be granted to a DHS facility or program.

Routine Uses: The information will be used by and disclosed to DHS personnel, contractor employees, or other agents who require the information to determine if access to a DHS facility or program should be granted. DHS may also share the information with other government agencies as necessary to determine if adverse information exists on the individual seeking access to a DHS facility or program.

Disclosure: Furnishing this information (including your Passport information) is voluntary; however, failure to furnish the requested information may delay or prevent your requested access to a DHS facility or program.