Privacy Impact Assessment Update
for the
Foreign Access Management System (FAMS)

DHS/ALL/PIA-048(a)

December 12, 2014

Contact Point
Richard Moreta
Foreign Access Management, Office of the Chief Security Officer
Management Directorate
(202) 447-5315

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

Abstract

The Department of Homeland Security (DHS) Office of the Chief Security Officer (OCSO) created the Foreign Access Management System (FAMS), formerly known as Foreign National Visitor Management System (FNVMS), to support the OCSO/FAM mission. DHS uses FAMS to vet foreign nationals that seek access to DHS personnel, information, facilities, programs, or systems. DHS is updating this Privacy Impact Assessment (PIA), last published on March 30, 2011, to document the system's name change, note that the system is now used by all DHS Components, clarify the categories of individuals screened by FAMS, clarify the types of checks done by the system, describe the forms created to support the OCSO/FAM Program, and clarify the information used as part of the screening process.

Overview

The Foreign Access Management System (FAMS), formerly known as Foreign National Visitor Management System (FNVMS),[1] is a module hosted on the Department of Homeland Security (DHS) Integrated Security Management System (ISMS) information technology (IT) platform.[2] FAMS is a tool used by the DHS Office of the Chief Security Officer (OCSO)/Foreign Access Management (FAM) program to manage the risk assessment process for foreign national contacts and visitors. FAMS is an application that maintains information about the following groups of individuals:

- Foreign nationals and foreign entities seeking access to DHS personnel, information, facilities, programs, and IT systems, including:
  - Dual U.S. Citizens and Lawful Permanent Residents (LPR) representing foreign interests,
  - LPRs providing construction or contractual services (e.g., food services, janitorial services), and
  - Foreign contacts and foreign visitors officially met outside a DHS venue;
- When requested, foreign visitors to fusion centers and state and local government homeland security programs; and
- Foreign contacts of DHS employees outside the scope of the employee's official activities.[3]

[1] *See* Foreign National Visitor Management System (FNVMS) PIA, *available at* www.dhs.gov/privacy.
[2] For additional information on ISMS, see DHS/ALL/PIA-038(a) Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.
[3] *See* Presidential Decision Directive/NSC-12 (Aug. 5, 1993), *available at* http://www.clintonlibrary.gov/assets/DigitalLibrary/PDD/PDD12.pdf.

Foreign Access Requests

The foreign national requesting access, his or her Embassy, foreign government agency, or foreign national's company provides information about the visiting foreign national to a DHS employee from the DHS Component sponsoring the foreign national. Information may be provided by telephone, email, DHS form, or fax. The DHS Component sponsoring the foreign national's access enters this information directly into FAMS. This process applies to both the foreign national and entities seeking access to DHS personnel, information, facilities, programs and IT systems, and foreign visitors to fusion centers and state and local government homeland security programs. DHS created six forms to assist with the FAMS screening process when appropriate:

1. DHS FM 11052, International & Domestic Release Worksheet - collects the foreign national and DHS employee information associated with the release of any DHS information to foreign nationals as part of their official interaction with DHS;
2. DHS FM 11055, Foreign National Screening Request (updated) - collects the foreign national and DHS employee information associated with a foreign request to access DHS;
3. DHS FM 11055-1, Supplemental Foreign National Screening Request - collects the foreign national and DHS employee information associated with the internal process of hosting foreign access;
4. DHS FM 11055-5, Continuous Foreign Access Notification - collects the identifying information of DHS employees whose official duties entail continuous contact with foreign nationals;
5. DHS FM 11056, Foreign Access Security Review - collects the foreign national and DHS employee information associated with a suspicious event that occurred during the course of approved foreign access to DHS; and
6. DHS FM 11057, Foreign Access Security Plan - collects the foreign national and DHS employee information associated with a long term foreign national assignment or detail to DHS.

Foreign Contact Reporting

Foreign contact reporting is not intended to inhibit or discourage contact with foreign nationals. Rather, it permits the Government to manage the risk posed by certain foreign nationals who seek to exploit personal relationships for purposes of collecting classified or sensitive information. DHS employees and contractors with Sensitive Compartmented Information (SCI) or other special program access have a responsibility to report all foreign contacts that are of a close, continuing personal association and any contacts with known or

suspected intelligence officers from any country.[4] Failure to report foreign contacts as required may result in reevaluation of eligibility for that access. DHS created DHS form FM 11053-5, Foreign Contact, to collect foreign national and DHS employee information associated with unplanned contact outside a DHS venue. This form serves two purposes: first, to provide a method for employees and contractors to report foreign contact to their special security officers and personnel security offices; and second, to allow OCSO/FAM to screen foreign nationals who have made contact with DHS employees and contractors under suspicious circumstances.

Foreign National Screening

All foreign nationals go through the same FAMS screening process, regardless of whether their information was submitted as an access request or contact reporting. The foreign national screening process consists of both the internal Identity Validation (IVal) and external Intelligence Community (IC) checks. DHS uses the foreign national's name; known aliases; organization represented, title, or position held; date of birth; place of birth; passport number; passport copy; photograph; country of citizenship; address; telephone number; country sponsoring the visit; visa information; and email address(es) to initiate the IVal process.

The IVal consists of unclassified checks of U.S. Customs and Border Protection's (CBP) Automated Targeting System (ATS),[5] CBP Arrival and Departure Information System (ADIS),[6] and the National Protection and Programs Directorate (NPPD) Office of Biometric Identity Management's Automated Biometric Identification System (IDENT).[7] OCSO/FAM maintains the results of the IVal check in ISMS. OCSO/FAM uses the Homeland Secure Data Network (B-LAN) and the Homeland Top Secret Network (C-LAN) to process external checks.[8] Each day, OCSO/FAM transmits batch files via B-LAN and C-LAN and uploads them to the appropriate IC platforms because FAMS does not directly connect to any external information system at this time. OCSO/FAM uses this information to check for any risks associated with providing the foreign national with the requested access. OCSO/FAM validates the foreign national's identifying information provided via FAMS internal check through the OCSO/FAM IVal process before conducting external checks with the IC.

OCSO/FAM maintains derogatory results uncovered during the OCSO/FAM screening process, as well as trend analyses and risk analyses on the C-LAN. OCSO/FAM provides

[4] There may be other situations in which foreign contact is likely and reportable, such as: membership in professional organizations that have foreign national members, attendance at seminars and conferences with a worldwide interest and international attendees, sponsorship of the entry or the presence of a foreign national in an employee's household (e.g., exchange student, housecleaner, gardener, au pair), and dating a foreign national.
[5] *See* DHS/CBP/PIA-006(d) Automated Targeting System (ATS) Update: TSA-CBP Common Operating Picture Phase II, *available at* www.dhs.gov/privacy.
[6] DHS/CBP/PIA-024(a) Arrival and Departure Information System, *available at* www.dhs.gov/privacy.
[7] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[8] External checks are performed in collaboration with IC agencies. Tailored batch files of FAMS data is transmitted to B-LAN and C-LAN and uploaded to the respective IC platforms.

information of concern to the sponsoring Components in a classified report transmitted on the C-LAN. OCSO/FAM maintains the results of the IC check in a Microsoft Access database on the C-LAN. OCSO/FAM uses the information in the Microsoft Access database to create the Foreign National of Concern Report, which OCSO/FAM sends to the hosting Component or agency. FAMS contains no derogatory information about the foreign national and only tracks identity discrepancies uncovered during the screening process. Although the information in FAMS is used in the screening process, the system serves solely as a tracking tool that facilitates trend and risk analysis centered on the foreign visitor's access to DHS.

OCSO/FAM provides the results of the screening and a determination of risk to the requesting Component. OCSO/FAM makes recommendations, but does not usually prevent access to the DHS resource. The sponsoring Component makes a risk-based assessment on whether or not to provide the foreign national with the requested access to DHS.

Reason for the PIA Update

DHS is updating this PIA to document the system's name change, note that the system is now used by all DHS Components, clarify the categories of individuals screened by FAMS, clarify the types of checks done by the system, describe the forms created to support the OCSO/FAM Program, and clarify the information used as part of the screening process.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

In addition to the authorities listed in the March 2011 PIA, Executive Order 13549, Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities, authorizes the collection and use of information for the FAMS program.

Characterization of the Information

As indicated in the March 2011 PIA and described above, DHS collects information about the foreign national, including: foreign national's name; known aliases; organization represented, title, or position held; date of birth; place of birth; passport number; passport copy; photograph; country of citizenship; address; telephone number; country sponsoring the visit; visa information; and email address. In addition to the data elements previously collected, DHS will

now collect Alien Registration Numbers (A-Number)[9] from LPRs screened through FAMS to further assist in positive identification of the individual. In some cases, passport numbers are expired, and A-Numbers provide an alternative method of identification.

The FAMS module also automatically generates a unique case number associated with a new record. This FAMS number (known previously as the FNV number) is specific to the system module and is used to facilitate system queries. As a result of a technical upgrade to the system, DHS only collects the name and Component of the DHS employee who enters the information into FAMS. FAMS no longer receives the employee's Social Security number.

Uses of the Information

Since the March 2011 PIA, DHS has adopted FAMS as the screening tool for all foreign national screening requirements of the Department. Maintaining a centralized system to log and track foreign national access requests increases the efficiency of the foreign national screening process by eliminating the need for each Component to conduct its own foreign national screening activities. Having one system also improves the screening process by eliminating gaps in information sharing and identifying trends that could indicate a risk, threat, or vulnerability to DHS personnel or programs. As a tracking tool, FAMS reports are accessible to all Components. In the case of the Multi-Visit function of FAMS, all affected Components have visibility of multi-visit requests.

Privacy Risk: Now that FAMS is used Department-wide, there is a risk that FAMS users may be able to access information in FAMS that they would not otherwise be able to access and do not need access to in the performance of their duties.

Mitigation: OCSO/FAM mitigates this risk by limiting access to the system to only those individuals with a need verified by the respective Component program manager and OCSO/FAMS. Like its parent system, ISMS, FAMS applies role-based access rules to limit information to what is necessary for an employee's job requirements. FAMS users will not be able to access information from the screening systems they would not have authority to access directly.

Notice

DHS continues to provide notice to the public through this PIA and the DHS Facility and Perimeter Access Control and Visitor Management System of Records Notice (SORN).[10] DHS also provides notice through a Privacy Act Statement on each FAM form. For additional

[9] Alien Registration Number is a unique seven-, eight-, or nine-digit number assigned to a noncitizen by the Department of Homeland Security. http://www.uscis.gov/tools/glossary.
[10] DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (Feb. 3, 2010).

transparency, per DHS's Mixed Systems Policy,[11] DHS is in the process of developing a Foreign Access Management SORN to cover all processes and information described in this PIA.

Data Retention by the project

In addition to the General Records Schedules described in the March 2011 PIA, DHS retains FAMS data in accordance with NARA-approved retention schedule N1-563-09-1-1. Consistent with other NARA-approved records schedules related to investigations and counterintelligence, DHS retains information collected on foreign visitors for screening in FAMS and in the C-LAN Access database for twenty years.

Information Sharing

OCSO/FAM shares foreign national information with other federal agencies to determine whether the individual in question has attempted to access another federal agency. The OCSO/FAM Program also sends the foreign national's submitted information and any derogatory information found through the IVal process to the IC. Names are submitted through the IVal process one at a time; however, the IC process involves batch file transfers on C-LAN via the Office of Intelligence and Analysis file transfer process. The information is shared by secure means commensurate with the classification of the information to be shared. IVal results are maintained in the remarks section of ISMS, and any results indicating a suspicious pattern or potentially nefarious activity are added to the classified person record. Foreign entities collaborating with the U.S. government may access multiple U.S. government agencies in the normal course of business, or when certain programs span the scope of several U.S. agencies. In such situations, OCSO/FAM may let the other government agency know that DHS found a security concern. When appropriate and consistent with the DHS Facility and Perimeter Access Control and Visitor Management SORN, OCSO/FAM may share derogatory information with another government agency.[12]

No DHS employee information is shared with outside agencies. Information sharing is restricted to the foreign national identifying information necessary to determine any risks to the Department.

Redress

No change from the March 2011 PIA.

[11] DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM 2007-01, DHS PRIVACY POLICY REGARDING COLLECTION, USE, RETENTION, AND DISSEMINATION OF INFORMATION ON NON-U.S. PERSONS (2009), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[12] *Id*.

Auditing and Accountability

No change from the March 2011 PIA.

Responsible Official

Richard Moreta
Foreign Access Management
Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security