Privacy Impact Assessment Update
for the

Foreign Access Management System (FAMS)

DHS/ALL/PIA-048(b)

April 10, 2017

Contact Point
Richard Moreta
Director
Center for International Safety & Security
Office of the Chief Security Officer
Management Directorate
(202) 447-5315

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

Abstract

The Department of Homeland Security (DHS), Office of the Chief Security Officer (OCSO), Center for International Safety & Security (CISS) manages the Foreign Access Management (FAM) program that screens foreign nationals[1] and foreign entities[2] that seek physical and electronic access to DHS personnel, information, facilities, programs, or systems. DHS also provides this service to the United States Department of Agriculture (USDA) on a full-time basis, and occasionally to other agencies as needed. DHS has provided legacy support to USDA as a result of its presence at the DHS Plum Island Animal Disease Center (PIADC).

This Privacy Impact Assessment (PIA) update reflects the incorporation of non-DHS foreign access screening request data into the Integrated Security Management System (ISMS) Foreign Access Management System (FAMS). In addition, this update reflects the expanded support to USDA and other U.S. Government agencies to assess the feasibility and benefit of screening as a service for foreign nationals accessing non-DHS Government personnel, information, facilities, programs, and systems. Unless otherwise noted, the information provided in previously published PIAs[3] remains in effect. Individuals are encouraged to read all program PIAs to fully understand CISS's privacy assessment of the FAM program.

Overview

The primary mission of the Department of Homeland Security (DHS) is to prevent terrorism and enhance security, including the mitigation of threats against the U.S. Government. Within DHS, the Office of the Chief Security Officer's (OCSO) mission is to lead the collaborative security program to safeguard the Department's people, information, and property so that the Department can secure the Homeland. As such, OCSO established the Center for International Safety & Security (CISS) in order to lead the execution of foreign access management and security screening. CISS has the objective to identify foreign access threats, vulnerabilities, and risks, and proactively mitigate these through extensive intradepartmental and interagency communication and coordination. CISS manages the risk assessment process for foreign national access to:

- DHS personnel, information, facilities, programs, and systems;
- Fusion centers;

[1] A foreign national is defined as a person who was born outside the jurisdiction of the United States, who is subject to some foreign government, and who has not been naturalized under U.S. law.
[2] A foreign entity is defined as any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation, or organization organized under the laws of a foreign state if either its principal place of business is outside the United States or its equity securities are primarily traded on one or more foreign exchanges.
[3] For more information about Foreign Access Management System (FAMS), please visit https://www.dhs.gov/publication/dhs-all-pia-048a-foreign-access-management-system.

- Tribal, territorial, state, and local government homeland security programs;
- United States Department of Agriculture (USDA) and other U.S. Government programs with specific homeland security implications, on an as needed basis.

Currently, CISS conducts screening for the following:

- **Foreign Access Requests -** CISS screens foreign nationals and foreign entities seeking access to personnel, information, facilities, programs, and systems, as well as foreign visitors to fusion centers and state and local government homeland security programs.
- **Foreign Contact Reporting -** Employees and contractors with access to Sensitive Compartmented Information (SCI) or other special programs are required to report close and continuing personal foreign contacts, contact with foreign government officials, and any foreign contact of a suspicious nature. Employees are required to report suspicious behaviors or security concerns encountered during foreign collaboration, as well as other suspicious activity reporting. CISS screens the foreign contact, when reported.

OCSO/CISS uses the Integrated Security Management System (ISMS)[4] Foreign Access Management System (FAMS) module to manage foreign access requests and suspicious foreign contact reporting.

Due to the success[5] of OCSO/CISS's risk assessment and screening process for foreign access to DHS facilities and personnel, OCSO/CISS has been identified as a partner with the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC) to establish minimum standards for agencies for foreign access management processes, screening procedures, and reporting mechanisms. As a result of this partnership, OCSO/CISS and NCSC are testing the viability of a centralized foreign access management screening process.

The Foreign Access Management Enterprise (FAME) pilot is designed to test the feasibility and benefits of providing a voluntary screening service for U.S. agencies whose mission necessitates foreign engagement. While not required, authorized U.S. Government security officials may request that CISS screens those foreign nationals who have applied for access to their facilities. CISS, in coordination with NCSC, will compare visitor application information to information previously provided to immigration and law enforcement officials, as well as perform watch list matching services and security reviews. When necessary, security reviews may include

[4] *See* DHS/ALL/PIA-038(b) Integrated Security Management System (ISMS) (November 24, 2015), *available at* http://www.dhs.gov/publication/dhsallpia-038b-integrated-security-management-system-isms. As of the date of this PIA, expanded USDA support did not include the use of ISMS/FAMS to process non-PIADC USDA foreign partners.

[5] On March 25, 2014, OCSO/CISS was designated by the Secretary of Homeland Security as a Foreign Access Management Center of Excellence to develop and implement a department-wide Center of Excellence for the screening and tracking of foreign nationals officially accessing DHS, and support and complement the foreign national screening activities of other U.S. Government agencies.

classified and unclassified governmental terrorist, law enforcement, and intelligence databases, including databases maintained by DHS, Department of Defense, National Counterterrorism Center, and Federal Bureau of Investigation. Information regarding individuals of concern may be shared with NCSC or other government agencies and organizations for national security, law enforcement, immigration, or intelligence purposes in response to potential or actual threats to U.S. Government programs, and as necessary to facilitate an operational response to such threats. The pilot also offers an opportunity to assess the viability of U.S. Government-wide foreign access data for use by the DHS Immigration Enterprise.

Reason for the PIA Update

DHS is updating this PIA to describe the impact of the FAME pilot. The pilot is designed to identify requirements for government standards and enhanced information sharing regarding a federated foreign access management service. The pilot will also test the feasibility and benefit of CISS providing a foreign access request screening service to other U.S. Government agencies.

The goals of the pilot include:

- Test CISS's functional ability to screen foreign nationals requesting access to other federal agencies;
- Assess a method for providing customers the results of CISS screening, refine foreign access security analysis, and identify a reporting solution for suspicious activities or security violations occurring during foreign access; and
- Gather requirements for:
  - A web-based government-wide consolidated security incidents solution;
  - NCSC-led analytics of foreign nationals that meet the criteria as "individuals of concern," who have been deemed a significant security risk for access to federal facilities; and
  - An aggregation of federal foreign access management data through an IT solution.

The pilot will be conducted using sample groups selected based upon documented risk criteria[6] designed to keep the pilot small in scale. Once the foreign national visitor screening process is established, and depending on resources and demand, OCSO/CISS may expand the number of screenings to include additional test cases. Should the pilot expand beyond its current proposed scope, CISS will update this PIA.

[6] Country-based criteria will be determined based on a combination of factors such as the President's National Intelligence Priority Framework, national trends, and previous Institute for Defense Analyses (IDA) research and analysis.

Thirty-four (34) federal agencies (listed in Appendix A) may participate in the pilot. For 120 days, these agencies will voluntarily submit to CISS the biographic information provided by a sample subset of foreign nationals requesting official access to their facilities or programs, as well as provide suspicious incident reporting related to the visit (if applicable).

CISS will provide foreign access data to NCSC to support additional analysis as well as the development of requirements for additional data repositories. CISS will screen prospective foreign visitors and provide the hosting agency with risk mitigation recommendations based on identity validation, immigration status checks, and any information already held in DHS foreign access records in ISMS/FAMS.

OCSO/CISS will conduct screening using the following functional process:

1. A non-DHS federal agency submits to CISS data provided by the foreign national through an encrypted DHS Form 11055, *Foreign National Screening Request Form,* (or modified version thereof) in a manner that can be uploaded to ISMS/FAMS for processing.
2. CISS checks the foreign national data against existing DHS foreign access holdings within ISMS/FAMS.
3. CISS checks the foreign national data against DHS immigration holdings.[7] CISS will notify the source system Component of any significant identity anomalies.
4. CISS compiles the foreign national data into batch files, and the files are transferred to a classified network for secure processing.
5. CISS submits the batch files through external Intelligence Community (IC) partners, to include NCSC, for screening against classified search tools and data sets (for example, terrorist watch lists).
6. CISS analysts review findings using documented risk criteria. An assessment indicating risk above a pre-set threshold requires a determination of "concern."
7. CISS makes an unclassified notification to the non-DHS federal agency in the form of a "high-concern/low-concern" recommendation, and associated risk-mitigation protocols commensurate with the findings. Examples of risk-mitigation protocols include additional physical screening of individuals entering facilities or an increased escort/visitor ratio. CISS does not make access determinations, and does not have the authority or mission to deny foreign national access to the U.S. Government. No one will be denied the ability to access the U.S. Government or enter a facility based solely on the results of CISS screening.
8. CISS retains classified findings and analysis, and shares them with authorized personnel within the affected agency as follows:

[7] A list of the DHS immigration holdings databases that are used can be found in Appendix B.

a. If significant derogatory information is found, the results are transmitted on a classified network for agencies with access to classified systems.

b. Agencies with no classified access will only be provided unclassified security countermeasures derived from the derogatory information intended to minimize the risks of the particular incident.

Authorized federal agency personnel with appropriate clearance levels can request additional information via classified means. Customers will report security anomalies prior to, during, or after foreign access through an encrypted DHS Form 11056, *Foreign Access Security Review Form* (or a modified version thereof). CISS will coordinate information sharing with the IC partner that originally generated the derogatory data before sharing the information with the affected agency.

Institute for Defense Analyses

In addition to conducting the foreign national screening and vetting checks described above, CISS will provide foreign access information to the Institute for Defense Analyses (IDA) for analysis over the course of the pilot. IDA is a not-for-profit corporation that currently operates three Federally Funded Research and Development Centers (FFRDC):[8] the Systems and Analyses Center, the Science and Technology Policy Institute, and the Center for Communications and Computing. For the FAME pilot, IDA will use "IDA Text Analytics" (ITA) for exploratory analysis to discover patterns and provide rich overviews of the entire pilot data set to help answer various researchable questions of interest.

IDA will conduct a one-time analysis of the foreign access management pilot data to determine relevant patterns. Based on the IDA findings, CISS will publish a report on foreign access management trends. CISS will provide only information about foreign nationals, but not their U.S. Government federal employee sponsors, to IDA. CISS will provide all information to IDA via classified networks. IDA will complete its research and analysis process within 180 days of the first transfer of information from OCSO. CISS has directed IDA to destroy all pilot information 30 days after the completion of a final IDA report.

[8] FFRDCs are unique independent entities sponsored and funded by the U.S. Government to meet long-term technical needs that cannot be met as effectively by existing governmental or contractor resources.

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 prior versions of this PIA,[9] CISS is conducting this pilot under the authority of the Economy Act of 1932, as amended,[10] the Counterintelligence Enhancement Act of 2002,[11] the Intelligence Reform and Terrorism Prevention Act,[12] 40 U.S.C. 1315,[13] and Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (February 12, 2013). In addition, DHS is issuing a new System of Records Notice (SORN), Foreign Access Management System of Records. The forthcoming SORN permits the Department to collect records to conduct foreign access management screening activities for federal agencies other than DHS.

Characterization of the Information

The information that OCSO/CISS collects for foreign access management screening and vetting remains unchanged. The pilot will collect the same data elements for screening for other Federal Government agencies as for DHS and its current partners. These data elements include:

Federal employee sponsor information:

- Full name;
- Title;
- Organization and component;
- Phone number; and
- Email address.

Foreign Visitor information:

- Full name;

[9] *See* DHS/ALL/PIA-048 Foreign National Visitor Management System (March 30, 2011), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-fnvms-march2011_0.pdf and DHS/ALL/PIA-048(a) Foreign Access Management System (December 12, 2014), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-fams-december2014.pdf.
[10] 31 U.S.C. § 1535(a).
[11] 50 U.S.C. § 3383.
[12] Pub. L. No. 108-458, § 7220(d), 119 Stat. 3838-39 (2004).
[13] The Secretary of Homeland Security has the authority and responsibility to "protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality or wholly owned, or mixed-ownership corporation thereof) and the persons on the property." 40 U.S.C. 1315(c).

- Alias(es);
- Gender;
- Date of birth;
- Place of birth;
- City/country of residence;
- Country of citizenship;
- Photograph;
- Address;
- Telephone number(s);
- Email address(es);
- Country sponsoring visit;
- Stated reason for the visit;
- DHS component sponsoring the visit;
- Diplomatic identification information;
- Organization represented, title, or position held;
- Actual employer information (including job title and employer contact information);
- Passport information (country of issue, number, expiration date);
- Passport copy;
- Visa information (type, number, expiration date, and issuance location);
- Foreign Access Management System number;
- Alien registration number; and
- Potential anomalous or derogatory information identified as part of screening and vetting results.

The data is provided directly by the federal sponsor via email to CISS in a password-protected attachment. In most cases, the foreign individual requesting access provides his or her information via his or her federal sponsor. The federal sponsor then works with the relevant security office within his or her agency. OCSO/CISS will accept screening requests from the agency security office responsible for overseeing foreign access to the respective agency. Non-

DHS security offices are not granted access to ISMS/FAMS or other DHS systems, and access to DHS data is not granted solely upon participation in this pilot.

Privacy Risk: There is a risk that DHS will collect more information than is needed to meet its mission, as OCSO/CISS will be vetting individuals who have no nexus to DHS personnel, facilities, or information.

Mitigation: The risk is partially mitigated by providing standardized forms that specify only the information to be collected, as well as providing agencies participating in the pilot with guidelines regarding the collection of data by authorized personnel. This risk is additionally mitigated given the narrow scope of the pilot information and the broad scope of authorities governing the national security activities of OCSO/CISS.[14]

Privacy Risk: Because the federal sponsor submits the information on behalf of the foreign national requesting access, there is an increased risk that information may be erroneous or incomplete.

Mitigation: This risk is partially mitigated. DHS recommends that the individual requesting access complete the form him or herself whenever possible. However, because this is a pilot with a goal to minimize disruption of established business practices, this is not always possible depending upon the existing practice at a given agency. DHS relies upon its redress process to mitigate the adverse impacts of any inaccurate information.

Uses of the Information

While the scope of individuals OCSO/CISS processes is expanding to include all foreign national visitors to USDA and the agencies participating in the pilot, the uses of the information collected during the pilot are consistent with the uses for foreign access requests detailed in the 2014 PIA Update,[15] except that OCSO/CISS will now conduct screening on behalf of other agencies. OCSO/CISS and NCSC will provide foreign access information to IDA for research and analysis, and is currently studying the viability of foreign access information for use by the DHS immigration enterprise.

---

[14] Additional authorities are granted and guided through: 5 U.S.C. § 301; 40 U.S.C. § 11331; Executive Order (E.O.) 12977; E.O. 13286; E.O. 13549; Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience" (February 12, 2013); DCI Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)" (July 2, 1998); Presidential Decision Directive (PDD)/NSC- 12, "Security Awareness and Reporting of Foreign Contacts" (August 5, 1993); E.O. 13556, "Controlled Unclassified Information;" E.O. 13549, "Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities;" National Security Decision Directive (NSDD) 298, "National Operations Security Program," January 22, 1988; Intelligence Reform and Terrorism Prevention Act of 2004; DHS Delegation Number 12000, "Delegation for Security Operations within the Department of Homeland Security," (June 2012); DHS Management Directive 11052, "Internal Security Program."

[15] *See* DHS-ALL-PIA-048(a) Foreign Access Management System (December 12, 2014), *available at* https://www.dhs.gov/publication/dhs-all-pia-048a-foreign-access-management-system.

Notice

The pilot will use DHS Form 11055, *Foreign National Screening Request Form*, with a DHS-approved Privacy Notice to provide notice to the individual providing his or her information. The form refers to the forthcoming Foreign Access Management System of Records SORN, which also provides notice of screening activities for federal agencies other than DHS.

Privacy Risk: There is a risk to notice since foreign nationals who request access to U.S. Government facilities may not know that they are submitting information directly to DHS.

Mitigation: DHS mitigates this risk by requiring participating customer agencies to use DHS Form 11055, *Foreign National Screening Request Form*, which contains a Privacy Notice that indicates DHS is collecting this information. The foreign national or federal employee sponsor who completes the form at the point of collection will have notice that the information is being collected by DHS. In addition, DHS is publishing the forthcoming Foreign Access Management System of Records SORN to describe the access, correction, and redress procedures for individuals to access their information.

Data Retention by the project

OCSO/CISS will destroy all foreign national screening request forms from the participating pilot agencies within 90 days of the completion of the 120-day pilot. Screening results and analysis will be retained consistent 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 for twenty (20) years.

Privacy Risk: There is a risk that the data shared with the pilot partners and participating agencies will be retained longer than needed to determine a foreign visitor's access to government facilities.

Mitigation: This risk is mitigated. Screening results, analysis, and information collected on foreign visitors will be retained for 20 years in accordance with NARA-approved retention schedule N1-563-09-1-1. OCSO/CISS and NCSC will publish an addendum to the existing Memorandum of Agreement (dated July 22, 2015) indicating the retention requirements.

Information Sharing

The pilot will require information sharing between the customer agencies, the IC partners, and OCSO/CISS, as described above. In addition, OCSO/CISS will share foreign access information with IDA and NCSC for analysis during the course of the pilot. The information provided to IDA and NCSC will consist of historical foreign access and derogatory background information or security incident or concern information on particular foreign nationals for the conduct of trend and other analysis. OCSO/CISS will not share federal employee sponsor information during the course of the pilot.

OCSO/CISS has prepared a Memorandum of Agreement (MOA) to provide guidelines for USDA, and for agencies participating in the pilot. Aside from addressing the handling of third-party information, the MOA template contains the following language:

> *By signing this Agreement, (AGENCY) agrees to apply DHS privacy provisions to the handling of foreign national information in accordance with the DHS Privacy Impact Assessment titled Foreign Access Management System, dated December 12, 2014. U.S. Person information associated with the reporting of foreign access-related incidents will be handled in accordance with the Privacy Act of 1974.*
>
> *The disclosure of foreign national personally identifiable information (PII) pursuant to name check requests referenced herein may be limited by federal law depending on the circumstances of the request. For purposes of this Agreement, "PII" is information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, national ID number, date and place of birth, mother's maiden name, biometric records and any other personal information that is linked or linkable to a specific individual.*
>
> *The Parties agree to review and make appropriate changes, if any, to their privacy compliance documents, including applicable Privacy Act system of records notices and notices required by the Privacy Act [5 U.S.C.552a (e) (3)], in advance of the implementation of this Agreement to ensure the scope and routine uses of such notices permit the collection, maintenance, and sharing of PII as set forth in this Agreement.*
>
> *Each Party will immediately, upon discovery, report to the other Party each instance in which data received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches).*
>
> *Section (c) of the Privacy Act, 5 U.S.C. 552a (c), requires that an agency maintain the ability to provide an accounting for covered disclosures made by the agency to persons or entities outside the disclosing agency. The accounting must include the data, nature, and purposes of each disclosure and the name and address of the person or agency to whom/which the disclosure is made. The accounting must be maintained for five years.*
>
> *Each Party that discloses PII is responsible for making reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant.*

All external information sharing will be consistent with the forthcoming Foreign

Access Management System of Records SORN.

In addition, as described in the Privacy Notice on the forms provided to the visitor and the MOAs with participating agencies, OCSO/CISS will share information internally across DHS when that information is necessary for another DHS Component to fulfill its mission. For example, if an individual applying to access another U.S. Government agency's facilities, through the course of the screening and vetting checks, is identified as having violated an immigration law, OCSO/CISS may share that information with ICE or USCIS.

Privacy Risk: There is a risk that OCSO/CISS will share information external to DHS in a manner that is inconsistent with DHS information sharing policies.

Mitigation: DHS is publishing a new SORN to describe the permissible routine uses for external sharing of foreign access management information. In addition, OCSO/CISS and NCSC will publish an addendum to the Memorandum of Agreement (dated July 22, 2015) to define the parameters for NCSC's handling, retention, and use of OCSO/CISS and pilot customer agency information, consistent with the forthcoming Foreign Access Management System of Records SORN.

Redress

Foreign nationals may request access and correction of their records maintained by DHS. All requests for access from non-U.S. citizens or non-lawful permanent residents are handled consistent with the Freedom of Information Act. Sensitivities associated with information in FAMS may prevent DHS from providing access or the ability to correct information. All agencies participating in the pilot will collect information using DHS Form 11055, *Foreign National Screening Request Form,* with Privacy Notices referring to the forthcoming Foreign Access Management System of Records SORN. In cases in which an individual seeks immediate redress through the hosting agency, the appropriate point of contact at the hosting agency must contact OCSO/CISS directly to provide additional or mitigating information.

Privacy Risk: There is a risk that partner agencies will not refer individuals to DHS for redress and that foreign nationals will not realize they can contact DHS directly for redress.

Mitigation: This risk is partially mitigated by the DHS-specific Privacy Notices on the information collection forms. If an individual seeking access contacts his or her hosting agency for information, his or her point of contact must contact OCSO/CISS to resolve any redress concerns.

Auditing and Accountability

OCSO/CISS has developed an MOA template that captures roles and responsibilities for USDA and the pilot, and provides detailed steps that must be taken to secure sensitive and personally identifiable information both in transit, during processing, and at rest.

All participating agencies are required to execute an MOA with OCSO/CISS to ensure accountability and compliance with these requirements.

The DHS Privacy Office will conduct a Privacy Compliance Review on the FAME pilot.

Responsible Official

Richard Moreta, Director
Center for International Safety & Security
Office of the Chief Security Officer
Management Directorate
Department of Homeland Security

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

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

Appendix A

Pilot Participant Departments and Agencies

1. Air Force Office of Special Investigations
2. Army Counterintelligence Center
3. Central Intelligence Agency
4. Centers for Disease Control
5. Drug Enforcement Agency
6. Defense Intelligence Agency
7. Department of Defense
8. Department of Energy
9. Department of Health and Human Services
10. Department of Interior
11. Department of Justice
12. Department of State
13. Department of Transportation
14. Department of Veterans Affairs
15. Defense Support of Civil Authorities
16. Environmental Protection Agency
17. Federal Aviation Administration
18. Federal Bureau of Investigation
19. General Services Administration
20. Government Accountability Office
21. U.S. House of Representatives Security
22. National Archives and Records Administration
23. National Credit Union Administration
24. National Geospatial-Intelligence Agency
25. National Aeronautics and Space Administration
26. National Security Agency
27. Nuclear Regulatory Commission
28. Office of Personnel Management
29. Overseas Private Investment Corporation
30. Pentagon Force Protection Agency
31. U.S. Senate Security
32. U.S. Department of Agriculture
33. U.S. Agency for International Development
34. Institute for Defense Analysis

Appendix B

OCSO/CISS checks the foreign national data against DHS immigration holdings. This holding include information from the following systems:

- U.S. Customs and Border Protection Advance Passenger Information System (APIS);[16]
- U.S. Customs and Border Protection Arrival and Departure Information System (ADIS);[17]
- U.S. Customs and Border Protection Automated Targeting System (ATS);[18]
- U.S. Customs and Border Protection TECS;[19]
- U.S. Immigration and Customs Enforcement Criminal Arrest Records and Immigration Enforcement Records (CARIER);[20]
- U.S. Immigration and Customs Enforcement Student and Exchange Visitor Information System (SEVIS);[21]
- National Protection and Programs Directorate Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT);[22]
- U.S. Citizenship and Immigration Services Central Index System (CIS);[23] and
- U.S. Citizenship and Immigration Services Person Centric Query Service (PCQS).[24]

---

[16] *See* DHS/CBP/PIA-001 Advance Passenger Information System (APIS), *available at* https://www.dhs.gov/publication/advanced-passenger-information-system-apis-update-national-counterterrorism-center-nctc, and DHS/CBP-005 Advance Passenger Information System, 80 FR 13407 (March 13, 2015).
[17] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* https://www.dhs.gov/publication/arrival-and-departure-information-system, and DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2015).
[18] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update, and DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[19] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* https://www.dhs.gov/publication/dhscbppia-021-tecs-system-platform, and DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[20] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016).
[21] *See* DHS/ICE/PIA-001 Student and Exchange Visitor Information System (SEVIS), *available at* https://www.dhs.gov/publication/dhsicepia-%E2%80%93-001a-student-exchange-visitor-information-system-sevis, and DHS/ICE-001 Student and Exchange Visitor Information System, 75 FR 412 (January 5, 2010).
[22] *See* DHS/NPPD/PIA-002 DHS Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system, and DHS/USVISIT-004 DHS Automated Biometric Identification System, 72 FR 31080 (June 5, 2007).
[23] *See* DHS/USCIS/PIA-009 Central Index System (CIS), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf.
[24] See DHS/USCIS/PIA-010 USCIS Person Centric Query Service (PCQS), available at https://www.dhs.gov/publication/dhsuscispia-010-person-centric-query-service.

Appendix C
Privacy Notice - DHS Form 11055

AUTHORITY: The collection of this information is authorized by 5 U.S.C. § 301; 40 U.S.C. § 1315; 40 U.S.C. § 11331; the Economy Act of 1932, as amended; the Counterintelligence Enhancement Act of 2002; the Intelligence Reform and Terrorism Prevention Act; Executive Order (E.O.) 12977; E.O. 13286; E.O. 13549; Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience" (February 12, 2013); DCI Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)" (July 2, 1998); and Presidential Decision Directive (PDD)/NSC- 12, "Security Awareness and Reporting of Foreign Contacts" (August 5, 1993).

PURPOSE: The purpose of this information collection is to perform screening for foreign nationals seeking access to DHS and partner U.S. Government agency personnel, information, facilities, programs, research, studies, and IT systems. This information is also used to screen foreign contacts and foreign visitors reported by DHS and partner U.S. Government agency employees who have met and/or befriended such contacts and visitors outside the scope of the employee's official duties.

ROUTINE USES: The information will be used by and disclosed to DHS security personnel, contractor employees, or other agents responsible for evaluating foreign nationals who request access to DHS. DHS may share the information when appropriate and permissible as described in this PIA or under a routine use in the "DHS/ALL-039 Foreign Access Management System (FAMS) System of Records Notice." The Department's full list of system of records notices can be found on the Department's website at http://www.dhs.gov/system-records-notices-sorns. DHS may also share this information internally if that information is necessary for another Component to perform its support its mission.

CONSEQUENCES OF FAILURE TO PROVIDE INFORMATION: Providing the requested information is voluntary, but failure to do so could result in the denial of the foreign national's access to DHS information, personnel, systems, and facilities.