Privacy Impact Assessment

for the

Foreign Access Management System (FAMS)

DHS Reference No. DHS/ALL/PIA-048(c)

August 15, 2022

Homeland Security

Abstract

The Department of Homeland Security (DHS), Under Secretary for Management (USM), Office of the Chief Security Officer (OCSO), Center for International Safety and Security (CISS) manages the Foreign Access Management (FAM) program that vets foreign nationals,[1] foreign entities,[2] and certain United States Persons (USPER)[3] that seek access to DHS personnel, information, facilities, programs, or systems. This Privacy Impact Assessment (PIA) update reflects the end of the Foreign Access Management Enterprise (FAME) Pilot program and the end of the agreement between OCSO/CISS and the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC). This Privacy Impact Assessment update also covers the addition of systems that will be included in the CISS vetting process; an increase in the foreign contact reporting population based on Security Executive Agent Directive (SEAD) 3,[4] which expanded reporting requirements to DHS employees and contractors (covered individuals) holding sensitive positions; and a discussion on CISS's use of Tableau as a dashboard for DHS security personnel.

Overview

The primary mission of DHS is to prevent terrorism and enhance security, which includes mitigating threats against the U.S. Government. Within DHS, OCSO's 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 CISS to lead the execution of foreign access management and security vetting. CISS has the mission to identify and assess foreign access threats, vulnerabilities, and risks, and proactively mitigate these through extensive intradepartmental and interagency communication, coordination, and vetting. CISS manages the risk assessment process for foreign national access to:

- DHS personnel, information, facilities, programs, and systems;
- Fusion Centers;[5]

[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] Legal Permanent Residents and/or Dual-citizens representing a foreign interest, or who are providing a contractual service (such as food delivery, janitorial, or other services) to DHS.
[4] *See* Security Executive Agent Directive-3 (SEAD-3), Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (June 12, 2017), *available at* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf.
[5] Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners."

- State and local government, tribal, and territorial (SLTT) homeland security programs; and
- U.S. Government departments and agencies that submit foreign access vetting requests to CISS on an as needed basis when an information sharing agreement has been executed and directly supports a DHS mission area.

CISS conducts vetting for the following:

- **Foreign Access Requests -** CISS vets foreign nationals and foreign entities seeking access to personnel, information, facilities, programs, and systems, as well as foreign visitors to fusion centers and SLTT homeland security programs.
- **Foreign Contact Reporting -** Employees and contractors with access to Sensitive Compartmented Information (SCI) or other special access programs (SAP), and covered individuals as defined by SEAD 3, are required to report close and continuing personal foreign contacts and any foreign contact of a suspicious nature. All DHS employees are required to report suspicious behaviors or security concerns encountered during foreign collaboration, as well as other suspicious activity reporting resulting from personal foreign contact or occurring during foreign travel. CISS vets the foreign contact, when reported.

CISS uses the Integrated Security Management System (ISMS)[6] Foreign Access Management (FAM) Module (called the Foreign Access Management System (FAMS) in previous Privacy Impact Assessments) to manage foreign access requests. CISS maintains access to the ISMS Personnel Security Module to review DHS covered individuals' foreign travel and foreign contact data.

To collect the necessary information to conduct its vetting and reporting, CISS employs the forms below. DHS Forms 11052, *International & Domestic Release Worksheet*, and 11055-5, *Continuous Foreign Access Notification*, are no longer being used.

- DHS Form 11055, *Foreign National Screening Request* - collects the foreign national and DHS employee information associated with a foreign request to access DHS;
- DHS Form 11055-1, *Supplemental Foreign National Screening Request* - collects the foreign national and DHS employee information associated with the internal process of hosting foreign access;
- DHS Form 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;
- DHS Form 11057, *Foreign Access Security Plan* - collects the foreign national and DHS

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED SECURITY MANAGEMENT SYSTEM (ISMS), DHS/ALL/PIA-038 (2011 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-department-wide-programs.

employee information associated with a long term foreign national assignment or detail to DHS; and

- DHS Form 11053-5, *Foreign Contact* - collects foreign national and DHS employee information associated with unplanned contact outside a DHS venue.

All foreign nationals go through the same FAM vetting process, regardless of whether their information was submitted as an access request or contact reporting. The foreign national vetting process consists of both internal and external checks.[7] CISS provides the results of the vetting and an assessment of risk to the Component that submitted the request. CISS makes recommendations but does not prevent access to the DHS resource. Using the assessment and vetting results, the sponsoring Component will determine whether or not to provide the foreign national with the requested access to DHS.

In 2017, DHS engaged in the FAME Pilot program to identify requirements for government standards and enhanced information sharing regarding a federated foreign access management service. The pilot was planned to test the feasibility and benefit of CISS providing a foreign access request vetting service to other U.S. Government agencies.[8]

Reason for the PIA Update

DHS is updating this Privacy Impact Assessment to document the removal of the FAME Pilot program, the associated Memoranda of Agreements (MOA), and information sharing agreements. This Privacy Impact Assessment update also includes an expansion of the foreign contact reporting population, the addition of several systems through which CISS conducts identity validation and vetting, and a discussion of CISS's use of Tableau as a dashboard for DHS security personnel to assess and communicate threat data.

Discontinuation of FAME Pilot Program

The discontinuation of the FAME Pilot program resulted from project scope, feasibility, and funding issues between ODNI and DHS. The agreement between ODNI and DHS OCSO has been terminated. Foreign national data collection did not occur as the pilot never became operational.

[7] For more information about the details of these checks, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE FOREIGN ACCESS MANAGEMENT SYSTEM (FAMS), DHS/ALL/PIA-048(a) (2014), *available* at https://www.dhs.gov/privacy-documents-department-wide-programs.

[8] For more information about the details of the FAME pilot, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE FOREIGN ACCESS MANAGEMENT SYSTEM (FAMS), DHS/ALL/PIA-048(b) (2017), *available* at https://www.dhs.gov/privacy-documents-department-wide-programs.

Expansion of Foreign Contact Reporting Population

This Privacy Impact Assessment update documents an increase in the population of DHS "covered individuals reporting foreign contacts as required by SEAD 3, which was published in 2017, but partially implemented by DHS in 2022. This Directive increased the requirement for all personnel with an active security clearance or who hold a sensitive position to report close and continuing foreign contact and personal foreign travel. The process by which vetting of individuals identified through foreign contact and personal foreign travel have not changed.

Additional Systems Used for FAMS Identity Validation and Vetting Process

CISS will submit foreign access data to the systems below, in addition to conducting foreign national identity validation and vetting checks as described in previous iterations of this Privacy Impact Assessment.

U.S. Customs and Border Protection's (CBP) Analytical Framework for Intelligence[9]

Previously, CISS submitted foreign national biographic information to CBP through CBP's Automated Targeting System-Passenger (ATS-P) system,[10] but transitioned to the Analytical Framework for Intelligence (AFI) due to its ability to accept batch files for bulk searches while still conducting checks against ATS and other appropriate CBP systems. AFI is an intelligence product creation and dissemination platform that supports multiple DHS components, specifically CBP and ICE. AFI provides technology and tools that produces timely and actionable intelligence for DHS personnel protecting the nation's borders, enhances collaboration between DHS intelligence analysts in a shared workspace, and more effectively shares threat information and intelligence to other federal partners charged with securing the Homeland. AFI shortens the time and expense of disseminating intelligence products to intelligence analysts in the field because reports are posted in a main repository and distributed to pre-identified communities.

AFI contains biographic and biometric information obtained by immigration and customs officials at ports of entry that will provide CISS with previously inaccessible intelligence to support its mission. AFI will allow expedited access to information, eliminating the need to physically search through multiple databases, resulting in a more effective and timely vetting process. AFI provides an expedited identity validation and vetting process, and improves efficiency and effectiveness of the CISS research and analysis process.

---

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI), DHS/CBP/PIA-010 (2012 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[10] S*ee* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-006 (2007 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

CBP's Automated Targeting System - Unified Passenger (UPAX)

CISS enters foreign national biographic information into the UPAX web portal[11] to search for and validate visa status, when applicable, as part of the identity validation and vetting process. UPAX functionality unifies multiple possible match results from multiple source systems, reduces record duplication, and streamlines the review process. CISS' use of UPAX also benefits from its ability to pull previously separate data from data sources identified in the previous FAMS Privacy Impact Assessments.

Department of State's Consular Consolidated Database (CCD)

CCD is a Department of State data warehouse that stores current and archived data from all worldwide Consular Affairs (CA) post databases.[12] CCD provides Consular Affairs real-time aggregated consular transaction activity collected domestically and at posts worldwide. Authorized Department of State and interagency users employ the CCD Web Portal to view centralized data through various reports and to access other Consular Affairs and interagency applications. CCD is also the repository of data flows between DHS, the Department of Justice (DOJ) Federal Bureau of Investigation (FBI), the Department of Defense (DOD), and other federal agencies providing input into the visa and passport review and approval process.

CISS enters foreign national biographic information into the CCD Web Portal to search for and validate visa status when applicable as part of the identity validation and vetting process. CISS does not create any new records within the CCD system.

Tableau

Tableau is an off the shelf data analytics tool capable of visualizing trends, conducting statistical mapping, and making risk measurements. CISS uses this tool for these purposes as it relates to foreign access data, which includes foreign nationals requesting some form of access to DHS. Tableau is also used for foreign travel and foreign contact data. All data is derived from the ISMS FAM and Personnel Security modules.

The data is then uploaded into Tableau, currently through manual processes, but in the future directly to the DHS Tableau Server. Data is transferred from the ISMS modules by CISS personnel only. CISS will export foreign national visitor, foreign contact, and foreign travel reports from the ISMS Report Server into an Excel spreadsheet file. This exported file will then be added to Tableau. Data collected and stored in Tableau is private and secure, and managed by the CISS

[11] For more information about ATS UPAX, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-006(e) (2017), *available* at https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

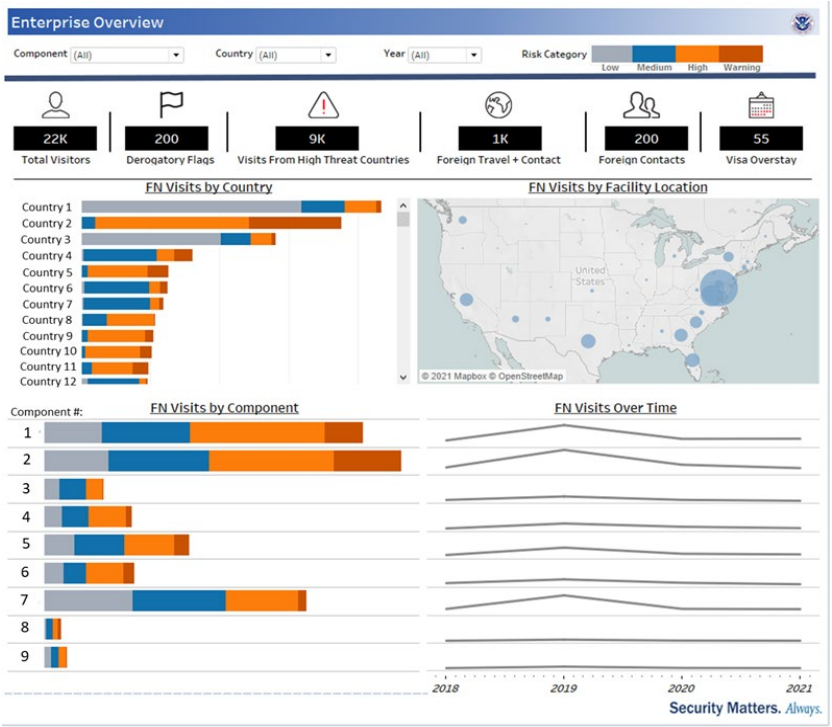
[12] For more information about the Department of State's CCD, please *see* DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE (CCD)(2018), *available at* https://www.state.gov/privacy-impact-assessments-privacy-office/.

Director. Tableau access is granted by CISS-designated Site Administrator Explorers and accessed through DHS single-sign on authentication.

CISS will use Tableau-generated risk scores in its analytic products, such as the FAM Report of Concern (RoC),[13] FAM Notification of Concern (NoC),[14] foreign access threat assessments,[15] and future products tailored to CISS's stakeholders. CISS will provide a dashboard in Tableau for Components' security personnel to access data to see their own foreign visit, foreign contact, and foreign travel data reporting and assessments. The Tableau dashboard provides all the same data these personnel would have under the previous FAM processes, but in a more consumable and efficient manner.

The only addition is the generated risk scores. The risk visualization dashboard provides an overview of enterprise foreign access risk, individual risk profiles, and risk scores for foreign nationals requesting access to DHS facilities, trends in foreign visits sponsored, foreign contact reports, and foreign travel reports by DHS employees. Additional views can display the risk of each individual foreign national and the risk of each country.

Figure 1: Tableau Dashboard for DHS Foreign National Visit Overview



[13] Report of Concern: A classified threat assessment that identifies foreign national, purpose of visit, and assessed threat of the visit taking place, and provides countermeasures to reduce risk.
[14] Notification of Concern: An equivalent product to the ROC but does not include classified sourcing. Advises recipient of classified reporting and the NOC, and provides general countermeasures.
[15] General risk assessments pertaining to a specific activity or trend.

Privacy Impact Analysis

Authorities and Other Requirements

In addition to the authorities listed in the prior versions of this Privacy Impact Assessment, Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (June 12, 2017), requires all covered individuals as defined by SEAD 3 to report close and continuing personal foreign contacts and any foreign contact of a suspicious nature.

The FAMS System of Records Notice (SORN)[16] continues to provide coverage for the collection of information used throughout the above processes.

Characterization of the Information

CISS is collecting only data previously disclosed in prior versions of this Privacy Impact Assessment. However, due to the requirements of SEAD 3, the population of covered individuals who must report foreign contacts has expanded. In addition, through the implementation and use of Tableau, CISS is creating risk assessments and scores for foreign national visitors based on the results of the vetting returns. The Tableau tool generates a low/medium/high risk score for each foreign visitor. CISS has developed a baseline of criteria to score, with CISS analysts developing ranking categories using multiple world threat assessment documents as source material. The reports and scores are used by DHS Components to decide whether to permit visits or if additional security controls are required when hosting certain visitors. Tableau also presents data in an efficient method for DHS security personnel. Tableau can present a single view of a foreign national visitor, including dates/locations of previous visits to DHS facilities, caution/risk assessments, and other biographic data rather than using disparate systems or relying upon manual lookups and queries.

CISS uses multiple IC systems and returns consisting of intelligence, counterintelligence, and criminal reports concerning submitted individuals, as described in previous Privacy Impact Assessments. CISS also uses DHS and Department of State systems that provide visa status and travel information to determine if the individual is in the country legally and validate the identity of the individual. In addition to those source systems, CISS now uses CBP's Automated Targeting System - Unified Passenger and Analytical Framework for Intelligence and the Department of State's Consular Consolidated Database (CCD), as described above.

As described in the previous Privacy Impact Assessments, information is collected directly from the foreign visitor, Component representative/sponsor, or entered directly into FAMS. Information is also provided from personnel security via self-reporting from covered individuals.

[16] *See* DHS/ALL-039 Foreign Access Management System of Records, 83 Fed. Reg. 19078 (May 1, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

CISS does not use commercial data aggregators or social media but does search publicly available information (e.g., Google) to corroborate identities and vetting results as part of its process. Public information is identified if it is included in a CISS report.

Privacy Risk: There is a risk that CISS will use inaccurate source data.

Mitigation: This risk is mitigated. Due to technological constraints, there is not a direct system-to-system connection between Tableau and the source data. Data has to be manually pulled from the ISMS FAM and Personal Security modules, then entered into Tableau for CISS to generate the risk-scoring and present data to dashboard users. To mitigate this risk, CISS pulls information from ISMS daily and purges old data. This ensures CISS is using current information to analyze and provide reporting to Components. CISS has determined that daily updates of the data are programmatically sufficient and fulfill its responsibilities from a security and risk perspective.

Further, CISS trains its analysts on intelligence and information evaluation techniques, and clearly identifies its sources and judgements when providing a final risk assessment to a component. Identities are checked against multiple databases to ensure vetting results are attributed correctly. CISS recommendations are based on its own process and defers ultimate determinations to Components.

Privacy Risk: There is a risk that the Tableau-generated risk scoring will be inaccurate or provide Components with improper information on which they base their determinations about a foreign national visitor.

Mitigation: This risk is mitigated. CISS has worked with the DHS Privacy Office to develop its methodology for generating the risk-score and ensuring it is applied appropriately. The risk-scoring is intended to be an additional security assessment tool rather than a predictive measure. It does not use artificial technology or other machine learning capabilities. The methodology is based on CISS subject matter experts' use of multiple world threat assessment documents as source material to generate scoring criteria. CISS informs its customers of the methodology and how they should apply the risk-scoring as it is intended to be an additional measure with which they can assess foreign national visitors, in coordination with FAM Reports of Concern, FAM Notifications of Concern, foreign access threat assessments, and other future products tailored to CISS's stakeholders.

Uses of the Information

CISS continues to use the information collected as outlined in previous Privacy Impact Assessments. CISS will use additional source systems to conduct identity validation and vetting (e.g., DOS CCD), and Tableau to generate automated risk scores to enhance CISS reporting to Components and requestors. CISS will use Tableau to allow appropriate Component personnel access to their own foreign visit, foreign travel, and foreign contact data, and the associated risks.

Components will have a reviewer only role in the Tableau dashboard.

Privacy Risk: There is a risk that the data made available through Tableau will be used inappropriately.

Mitigation: This risk is mitigated. Sharing of information is restricted to DHS security personnel that have the appropriate need-to-know. Tableau access is granted by CISS-designated Site Administrator Explorers and accessed through DHS single-sign on authentication. Component personnel will have read-only access to the information in Tableau.

In addition, certain data is accessible only to those Components that are responsible for that particular data. While all foreign national visit data is accessible across Components, sponsor data and foreign travel reporting data are only accessible to Component security personnel who are responsible for that employee. For example, CBP security personnel would have access to the profile of a foreign visitor that has visited U.S. Immigration and Customs Enforcement (ICE) facilities in the past, but not any sensitive information about the foreign national's ICE sponsor . The sponsor's contact information only will be accessible to CBP security personnel who may need to contact the ICE sponsor for additional information about the foreign visitor. The purpose for this bifurcated access is to ensure that the Component has all the information needed from a risk assessment perspective, but not the sensitive identifying information of other DHS employees. All Tableau users will have access to aggregate-level reporting such as that represented in Figure 1.

Notice

As noted in the previous Privacy Impact Assessments, notice is conveyed via the information collection forms and their Privacy Act Statements and Privacy Notices. However, notices may not be provided in situations where the foreign national is identified during foreign contact or foreign travel self-reporting. In these cases, notifications may reduce the effectiveness of monitoring and personnel security activities. Therefore, this Privacy Impact Assessment and associated FAMS System of Records Notice provide an additional measure of notice.

Data Retention by the Project

CISS maintains visit records in accordance with retention schedule N1-563-09-1-1 for 20 years from the date of the last visit for any foreign national. This supports CISS' requirement to track and analyze visitor information and assess visit trends indicating risk to the Department. After 20 years, CISS will reassess if retention is required to support current operations or investigations. CISS policies describe how the data will be accessed, maintained, and destroyed, which reduces the risk of inappropriate retention. CISS personnel are provided these policies and standard operating procedures when they start with the organization. With respect to the discontinuation of the FAME Pilot program, no data was collected as the FAME pilot never became operational.

Information Sharing

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. As part of this Privacy Impact Assessment update, data is checked against additional CBP systems, and also externally against the Department of State's Consular Consolidated Database.

Redress

Redress does not change with this Privacy Impact Assessment update. Individuals are provided a Privacy Act Statement or Privacy Notice on the DHS Forms listed above explaining how the information will be used and provide their consent to the Department's collection of their personally identifiable information. Further, any individual seeking access to or amendment of their records may submit a request in writing to the DHS Chief Privacy and Chief Freedom of Information Act (FOIA) Officer at the address below, or to the respective Component's Freedom of Information Act Officer, which can be found at https://www.dhs.gov/foia-contact-information. DHS also accepts Privacy Act and Freedom of Information Act requests submitted electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form.

Chief Privacy and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Sensitivities associated with information in FAMS may prevent DHS from providing access or the ability to correct information.

Auditing and Accountability

Policies and procedures are revalidated annually with all operations personnel to ensure there are no deviations to the policies, procedures, or requirements presented in this or previous Privacy Impact Assessments. The CISS branch chief, vetting lead, and program manager are the only CISS personnel authorized to grant access to FAMS and any associated systems/data (e.g., Tableau). Access controls for CISS personnel are revalidated annually.

All DHS personnel receive a standard, mandatory privacy training which includes handling and protection of personally identifiable information. CISS also provides specific user training prior to granting access to FAMS.

Responsible Official

Derrick Shack
Director, CISS
USM/OCSO/TMO
Derrick.Shack@hq.dhs.gov

Approval Signature

Original, sign version on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717