



Privacy Impact Assessment
for the

SAS Predictive Modeling Environment (SAS PME)

DHS/USCIS/PIA-055

October 15, 2014

Contact Point

Donald K. Hawkins

Privacy Officer

United States Citizenship and Immigration Services

(202) 272-8404

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) implemented the SAS Predictive Modeling Environment (SAS PME) to provide USCIS offices with a means to conduct data management, pattern and trend analysis, and statistical and historical reporting. USCIS is conducting this PIA to document, analyze, and assess the current practices with respect to the personally identifiable information (PII) used for analysis in SAS PME.

Overview

DHS United States Citizenship and Immigration Services (USCIS) collects, tracks, and stores large amounts of information related to administering and processing benefit requests for all immigrants and nonimmigrants. USCIS reaps significant benefits from the analysis of this information, which better informs future business decisions. However, this analysis is a time consuming and burdensome task that not every USCIS system can conduct. To address this challenge, USCIS developed the SAS Predictive Modeling Environment (SAS PME) tool.¹ SAS PME, a subsystem of the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR),² allows USCIS to upload large amounts of data to conduct research and analysis, including predicting future circumstances that may affect USCIS operations. The tool allows users who conduct research and statistical analysis as part of their job duties to research and analyze large datasets to detect and analyze historical immigration trends, merge datasets between multiple USCIS systems, and forecast trends among applicant populations or form types. For example, USCIS can use SAS PME to predict how many applicants will apply for a certain benefit in a given year. Using this information, USCIS may decide to add or reallocate personnel to handle the additional workload.

While SAS PME has the capability to data mine, USCIS does not currently use the system to data mine under the Federal Agency Data Mining Reporting Act of 2007.³ To ensure data mining does not occur, the USCIS Office of Privacy requires all users to successfully complete SAS training and sign a Rules of Behavior (ROB) prior to accessing SAS.

Data Retrieval

SAS PME obtains data in two ways: (1) through a system interface or (2) through a data extract uploaded into the system from another source.

¹ SAS is a software suite developed by SAS Institute for advanced analytics, business intelligence, data management, and predictive analytics. SAS is not an acronym.

² See DHS/USCIS/PIA-023 - Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), available at www.dhs.gov/privacy.

³ See 42 U.S.C. § 2000ee-3.



System Interface

SAS PME has a direct interface to USCIS systems to ingest and analyze data. Through these interfaces, SAS PME can process and analyze information contained within the USCIS systems. Unlike other USCIS reporting tools, there is no filtering, cleaning, or transformation of data by the SAS PME in preparation for analysis. SAS PME users have access to the data sets from the source systems as defined by the service accounts established between SAS and the source systems eCISCOR⁴ and Fraud Detection and National Security Data System (FDNS-DS), further described in Appendix A of this PIA.⁵ These system interfaces are unidirectional and SAS PME users only have read-only access to the data.

SAS PME also allows users to analyze data other than data connected through system interfaces. SAS PME users can upload data extracted from other USCIS systems that do not have a system interface with SAS PME and other information related to furthering the USCIS mission. For example, some SAS PME users may need to upload extracted data such as public Census data, customer satisfaction rates, and revenue estimates. As outlined in the ROB and training, users are only authorized to upload data that is related to the USCIS-mission for a valid business purpose.

SAS PME Use

SAS PME is used throughout USCIS to conduct research on customers, operations (including adjudications), and detect patterns of fraud. SAS PME allows users to analyze and research large data sets, analyze historical trends in USCIS data, merge datasets between USCIS systems, conduct statistical analysis to uncover patterns and trends, and forecasting outcomes among populations or types of USCIS forms.⁶ The use of SAS PME varies by program office, however, general examples include:

- Comparing USCIS revenue estimates by year;
- Analyzing employee labor hours by location;
- Discerning a trend of rising fraudulent passports from a particular country;
- Comparing the increasing amount of visas in a particular country against another;
- Understanding the demographic applying for a particular benefit one year versus another;
- Reviewing customer satisfaction rates by USCIS Office location; and
- Comparing USCIS data against public U.S. Census Data.

⁴ See DHS/USCIS/PIA-023 - eCISCOR, available at www.dhs.gov/privacy.

⁵ See DHS/USCIS/PIA-013 FDNS-DS; DHS/USCIS/PIA-013(a) – FDNS Directorate, available at www.dhs.gov/privacy.

⁶ See Appendix C for more information on SAS PME users and uses.



USCIS uses this information to assist in making business decisions to improve USCIS operations such as creating more immigration officer positions, changing immigration application fees, or reducing the processing times on benefit applications. The reports created by SAS PME show aggregate analysis, modeling, and forecasting. If there is a valid need, generated reports may include PII; however, USCIS analysts render their analysis on aggregate data to determine trends and forecast future outcomes for populations, not individuals. While SAS PME has the capability of data mining, USCIS does not currently use the system to data mine.⁷ SAS PME will not be used for the purposes of detecting fraud, abuse, or criminal and terrorist activity. The USCIS Office of Privacy holds users accountable to this rule by requiring all users to successfully complete SAS training and sign a ROB prior to accessing SAS.

Reports

Depending on the functions and business needs of a particular USCIS office, USCIS uses SAS PME to generate various reports and predictions that can be used for internal or external purposes, such as showing statistical analysis or predictive anomalies⁸ to field offices, senior management, or Congress.

Users can export and save the report information in several formats, such as Microsoft Excel, Microsoft PowerPoint, Adobe PDF, and plain-text, or users may print the reports. Authorized users destroy the reports when no longer needed to conduct business.⁹ If users choose to save reports that contain PII, either in hard or soft copy, users ensure the reports are properly secured. Electronic reports are saved in access-controlled folders. Hard copy reports are physically secured in a locked device (e.g., drawer, cabinet, desk). These measures prevent unauthorized access by members of the public or other persons without a need to know.

Within SAS PME, users can create ad-hoc or use reports pre-defined by other users to meet various reporting needs at USCIS. Ad-hoc reports allow users to build their own reports and specify data elements to be included. SAS PME users can create, organize, and share ad-hoc reports within SAS PME, but will only display the information from the source systems in a read-only format. Offices may create pre-defined reports using specific criteria determined by business need, tasks, and user reporting requirements. Additionally, SAS PME users can manipulate or extend pre-defined reports to meet other reporting needs.

Users

Select offices within USCIS may use SAS PME with their office management's approval. To obtain access to SAS PME, users must have a valid purpose to use the system, complete the SAS PME Account Request form, ROB, SAS Privacy training, obtain appropriate

⁷ See Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3.

⁸ A predictive anomaly shows the discrepancies between what a predictive model shows to be a likely outcome and the actual outcome.

⁹ See General Records Schedule 20, Item 16, available at <http://www.archives.gov/records-mgmt/grs/grs20.html>.



signatures, and submit for processing. eCISCOR administrators can further restrict data access to SAS system users based on the Interchange Control Agreement signed between the systems. In addition, each office that uses SAS has a system owner who is responsible for authorizing access to SAS for its employees, as described above. Offices maintain a written record of which employees are authorized to work with what data within SAS. Once processed, the SAS PME Administration team will create and activate an account for the user and assign the user appropriate roles based on his or her department or division management's authorization.

There are three types of user groups for SAS PME:

Power user: Power users have the ability to create their own report dashboards, create ad-hoc reports, and save the ad-hoc report for others to use as pre-defined reports. These users typically create one or more pre-defined reports for a group of Standard users to use on a daily, weekly, or monthly basis.

Standard user: Standard users have limited privileges within SAS PME. These users have read-only ability to run pre-defined reports that a Power user created and saved. Standard users must use pre-determined criteria for their reports and cannot modify a report (i.e., they cannot add or remove fields defined in the report). However, these users can filter the information returned to the report, if needed.

Administrator: Administrators have system privileges within SAS PME, including access to pre-defined and ad-hoc reports. Only the SAS PME Development Team and identified USCIS SAS PME Administrators have administrator access.

If additional system interfaces or uses of SAS PME change, USCIS will update and reissue this PIA and subsequent appendices.

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 Immigration and Nationality Act, sections 101, 103, 264, and 290 authorize the collection of this information.¹⁰

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

Although SAS PME does not collect PII directly from individuals, the system interfaces often retrieve data by personal identifier, as noted in the Overview and in Appendix A.

¹⁰ 8 U.S.C. §§ 1101, 1103, 1304, 1360.



SAS retrieves data from the source systems based on the parameters defined by the SAS Power user who defines how the data is retrieved for SAS analysis. The majority of SAS analysis does not require retrieval of PII. Rather, users retrieve information such as country of birth or a date of birth range for analysis.

Appendix A also includes a list of all relevant SORNs that cover the retrieval of information by personal identifier. If SAS PME adds any new source systems, USCIS will update this Appendix.

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

The SAS PME Security plan is an addendum to the eCISCOR Security Plan, since SAS PME is a subsystem of eCISCOR. eCISCOR's Authority to Operate (ATO) was granted May 8, 2014, for a period of 36 months.

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

Yes. SAS PME retains queries for 90 days. SAS PME then archives or deletes the information. SAS PME displays read-only information from existing systems for reporting purposes. Users can export SAS analysis and reports into Excel, Word, and PDF formats. SAS PME users retain reports outside of the system for business purposes and then destroy them when no longer needed in accordance with NARA's General Record Schedule 20, Item 16. If users choose to save reports that contain PII, either in hard or soft copy, users ensure the reports are properly secured. Electronic reports are saved in an access-controlled folder. Hard copy reports are physically secured in a locked device (e.g., drawer, cabinet, desk). These measures prevent unauthorized access by members of the public or other persons without a need to know.

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.

SAS PME is not subject to the PRA because it is not the original point of collection for the data. However, the information SAS PME receives from other systems may be subject to the PRA.



Section 2.0 Characterization of the Information

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

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

SAS PME does not collect any PII. SAS PME analyzes and processes PII retrieved from the source systems about DHS employees, contractors, USCIS benefit requestors, and immigration practitioners. Authorized users may upload data extracts (e.g., public Census data) to SAS PME that will enhance the data contained in source systems. Appendix B provides a detailed list of data elements that SAS PME may retrieve from connected source systems. This information includes a benefit applicant's name, Social Security number (SSN), date of birth, residence address, phone number, e-mail address, certificate of citizenship number, naturalization certificate number, Alien Number (A-Number), name of employee processing the file, criminal history, financial information, and family information. This information is used to create report parameters. The majority of SAS analysis and reports do not contain specific data elements that can identify an individual.

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

The source of the information in SAS PME is either from USCIS system interfaces or from data extracts uploaded by the user. A complete list of the systems that provide information to SAS PME is in Appendix A. USCIS may add SAS PME system interfaces in the future to allow users to analyze additional data. If this occurs, USCIS will update the PIA appendices to discuss the privacy implications of the additional source system(s).

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

SAS PME can ingest public sources or commercial data originally obtained through source system interfaces or uploaded data extracts. Please see Appendix A for information on what system interfaces contain data derived from public source or commercial data sets.

2.4 Discuss how accuracy of the data is ensured.

SAS PME is not the original point of collection for the information generated in the reports it provides to its users. The accuracy of the data analyzed in SAS PME depends on the accuracy of the source system providing the information. Interconnected systems refresh data in



SAS PME to ensure the information is as up-to-date as possible. If the SAS PME user questions the accuracy of the information, he or she should refer to the source or data owner for validity.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the external data sources may be inaccurate and USCIS may therefore create erroneous reports.

Mitigation: USCIS does not use this information as part of the benefit determination process and will have no impact on USCIS customers.

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.

SAS PME provides USCIS business analysts, statisticians, and other relevant staff with the tools to conduct essential agency business processes to meet agency objectives. USCIS offices use the tool for pattern and trend analysis of USCIS data and other business-related data, and to create statistical or historical reporting as well as predictive models in a centralized manner. Because of SAS PME's forecasting and predicting capabilities, the reports SAS PME produces assists USCIS in making business decisions (e.g., staffing or changing immigration application fees) and understanding and improving USCIS operations (e.g., fraud patterns or application trends). SAS PME holistically analyzes and examines large data sets that show trends and patterns in populations, not individuals. USCIS creates these reports, which contain aggregate data, to show leadership and potentially external parties' patterns, trends, and anomalies in USCIS data. If reports contain PII, the purpose is to show trends of populations and not individuals. Users minimize the amount of PII used as much as possible and mark the report For Official Use Only (FOUO). The report is only shown to those within USCIS with a need to know. Furthermore, all reports containing PII are handled in accordance with the DHS Handbook for Safeguarding Sensitive PII.¹¹ If USCIS shares a report with an external agency, it is done in accordance with the Privacy Act of 1974 and Routine Uses outlined in the applicable SORN.

SAS PME allows USCIS users to examine multiple aspects of USCIS operations, such as the characteristics of USCIS applicants or petitioners, the information related to the receipt, processing, and adjudication of a form, and the outcome of the adjudication decisions. This allows statisticians and analysts to better understand USCIS operations and implement practical

¹¹ The DHS Handbook for Safeguarding SPII is available at www.dhs.gov/privacy.



business models based on real data. See Appendix C for specific information on how each office uses SAS PME.

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.

Yes. SAS PME is a statistical software package and is capable of deriving patterns and constructing predictive statistical models. The use of SAS PME allows USCIS users to sift through large amounts of data to discover anomalies in the data, and forecast trends that may affect USCIS operations in the future.

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

There are no other components with assigned roles and responsibilities in the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that SAS PME users may upload data that is not relevant to the USCIS mission.

Mitigation: SAS PME users will be able to work with data that is already possessed by USCIS and is collected via authorized sources. The user's supervisor or project manager identifies the interconnected systems to which the user needs access and the levels of access the user needs to do his or her job. In certain circumstances, user access will vary depending on the position the user holds (e.g., FDNS users will only have access to FDNS-DS data). In other instances, users who access a system's data through SAS PME are able to access all of the source system information (e.g., users accessing eCISCOR data through SAS PME, are able to access all of eCISCOR source systems.¹²) However, the level of information they receive is determined by their need for certain data sets, as authorized by their supervisor. The System Owner or designated representative must approve user access privileges.

Privacy Risk: SAS PME users who no longer require access to the tool may continue using the tool.

Mitigation: USCIS mitigates this risk by implementing a process for managers and supervisors to notify the SAS PME System Administrator when users are terminated or transferred, or when information system usage, need to know, or need to share settings change. Access to the tool is reviewed and re-validated regularly by managers, supervisors, and the SAS

¹² See DHS/USCIS/PIA-023 - Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), available at www.dhs.gov/privacy.



PME Information System Security Officer (ISSO). SAS PME access is tied to user's Active Directory (AD) account authentication. If a user is terminated from USCIS and is removed from the AD Global Access List, the user will not be able to access SAS.

Risk: There is a risk that SAS PME users may be able to access and use USCIS system information to which they normally do not have access.

Mitigation: Users are granted role-based access to the system interconnections with SAS PME. For example, only FDNS authorized staff will be able to work with FDNS DS data. Other SAS PME users will not be able to see or use the FDNS DS data. FDNS users, before gaining access to SAS PME, will have to have the FDNS DS subject area owner to sign off on their access; therefore, FDNS will be aware who is accessing their data via SAS PME and control the number and identity of the users.

Users that have access to eCISCOR data will be accessing the data based on their role (Standard or Power user) and their access will be restricted by the service account between the systems.

Risk: There is a risk that users may use SAS PME to data mine, which falls under the Federal Agency Data Mining Reporting Act.

Mitigation: Should the use of SAS PME change to include data mining that falls under the Federal Agency Data Mining Reporting Act, USCIS will update and republish this PIA to examine and discuss any new privacy risks associated with the change. USCIS will also fully comply with the reporting requirements of the Act.

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.

SAS PME does not provide specific notice prior to the collection of information because SAS PME is not the original point of collection. General notice is provided to individuals on the USCIS forms (the original point of collection), the associated source system SORNs,¹³ and this PIA.

¹³ See Appendix A for a list of source system SORNs.



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

SAS PME does not provide specific opportunities for consent prior to the collection of information because SAS PME is not the original point of collection. USCIS presents individuals who apply for USCIS benefits with a Privacy Act Statement as required by section (e)(3) of the Privacy Act. The Privacy Act Statement for each form is located on the form's instructions. The Privacy Act Statement details the authority to collect the information requested and the routine uses for which USCIS may disclose the provided information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Because SAS PME is not the source system of collection, there is a risk that individuals will not know about how SAS PME uses their information.

Mitigation: USCIS mitigates this risk through the publication of this PIA.

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.

SAS PME archives and removes data from the system after 90 days as a best practice to limit information retention to only as long as the organizational need for a data analysis.

At the time of system disposition system media (e.g., server hard drives) used to retain SAS PME data is sanitized or disposed of upon written consent from USCIS federal employees. The policy mandates that all media must be deleted prior to disposal or destruction. The USCIS Data Center (DC)-1 administrative team along with the DC-1 ISSO keeps records of all media that are destroyed or sanitized. All SAS PME users are trained on the proper procedures for safekeeping of sensitive storage media in their possession and are trained to notify the SAS PME ISSO or DC-1 Security Manager when media containing sensitive information is no longer required. This is covered during the annual security training.

Furthermore, users may export and save the report information in several formats, such as Microsoft Excel, Microsoft PowerPoint, Adobe PDF, and plain-text or print the reports. These reports are destroyed by the authorized user when no longer needed to conduct business in accordance with General Record Schedule 20, Item 16. USCIS employees are required to take annual Privacy and Records Management training that trains employees on how to properly manage and safeguard privacy sensitive records. If users choose to save reports that contain PII, either in hard or soft copy, users ensure the reports are properly secured. Electronic reports are saved in an access-controlled folder. Hard copy reports are physically secured in a locked device



(e.g., drawer, cabinet, desk). These measures prevent unauthorized access by members of the public or other persons without a need to know.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the system and users may retain data for longer than necessary.

Mitigation: The information maintained in SAS PME is only stored for 90 days. The 90-day destruction policy was crafted with both security and privacy best practices in mind to manage server resources and to not retain data for longer than necessary.

Additionally, authorized users who download or print reports will destroy the reports once the user fulfills his or her business requirement or when no longer needed in accordance with GRS 20. If the user determines that after a certain time period the report is no longer accurate, he or she can destroy the report and recreate the same type of report with accurate and updated information. If reports are saved either in hardcopy or electronic form, users ensure the reports are properly secured. Electronic reports are saved in an access-controlled folder. Hard copy reports are physically secured in a locked device (e.g., drawer, cabinet, desk). These measures prevent unauthorized access by members of the public or other persons without a 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.

USCIS may share reports generated by SAS PME with external agencies or Congress. USCIS provides reports to external parties to show statistical analysis or predictive anomalies of USCIS data. Any PII on reports shared externally removed entirely before sharing. This information is pertinent to provide statistical immigration information for agencies conducting quantitative studies and research on immigration. All external sharing is done in accordance with the Privacy Act of 1974 and Routine Uses outlined in the applicable SORN.

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

The applicable SORNs allow information to be shared with Federal, state, tribal, local, or foreign government agencies or organizations responsible for providing immigration benefits,



conducting investigations or prosecuting violations of civil or criminal laws, and protecting national security. Appendix A includes a list of the relevant SORNs that cover the information processed in SAS PME.

6.3 Does the project place limitations on re-dissemination?

Because the reports USCIS may contain aggregate data, external parties may re-disseminate statistical USCIS data without limitations. If the reports contain PII, and require external sharing, USCIS removes the PII before sharing information in accordance with the routine uses in the respective SORN and sets provisions on re-dissemination with the recipient party.

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

The project does not maintain a record of any disclosures outside the Department. The reports generated by SAS PME are not individual-specific; therefore, when sharing information externally, a record of disclosure will not be made. Reports that are shared externally contain aggregate data representing data for a large group of individuals with a specific trend or feature that allows USCIS to predict patterns and identify trends holistically.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of unauthorized disclosure of information contained within SAS PME.

Mitigation: USCIS mitigates this risk by limiting access to SAS PME to only those USCIS employees with a need to access the system. If USCIS chooses to distribute a report externally, the reports contain aggregate data that demonstrates a trend or pattern and do not specifically identify an individual. Reports that contain PII are for USCIS internal use only and will be marked FOUO.

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?

Individuals may not directly access their information in SAS PME. Individuals seeking access to their information should follow the directions provided in the source systems PIAs and SORNs. Individuals may request access to their information by submitting a Privacy Act request



unless the information is covered by an appropriate exemption from one or more of the Privacy Act requirements.

To obtain access to his or her information, the individual would have to make either a Freedom of Information Act or Privacy Act request. Individuals who are seeking information pertaining to them are directed to clearly mark the envelope and letter “Privacy Act Request.” Within the text of the request, the subject of the record must provide his/her full name, date and place of birth, and notarized signature, and any other information that may assist in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G-639, *FOIA/PA Request*, from the nearest DHS office, to submit a request for access. The procedures for making a request for access to one’s records can be found on the USCIS website, located at www.uscis.gov.

An individual that would like to file a FOIA/PA request to review his or her USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services
National Records Center
FOIA/PA Office
P O Box 648010
Lee’s Summit, MO 64064-8010

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

SAS PME itself does not permit individuals to amend erroneous information. Individuals seeking to correct inaccurate or erroneous information should follow the instructions provided in the source system SORN.

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

SAS PME provides notice to individuals about the procedures for correcting information through this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that USCIS may not afford an individual adequate opportunity to correct information that SAS PME maintains.

Mitigation: The PII used by SAS PME is obtained by other USCIS source systems. Individuals are given numerous opportunities during and after the completion of the benefit request process to correct information they have provided and to respond to information received



from other sources. USCIS does not claim any Privacy Act exemptions for SAS PME and therefore individuals may submit a redress request or appeal as stated in the DHS Privacy Act regulations.¹⁴

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 SAS PME ISSO is responsible for managing the audit records in conjunction with the Site System Administrator who also has access to perform these duties.

SAS PME assets are configured via the operating system images to audit for the following:

- Identity of each user and device accessing or attempting to access the information system;
- Time and date of the access and the logoff;
- Activities that might modify, bypass, or negate information security safeguards;
- Security-relevant actions associated with processing; and
- All activities performed using an administrator's identity.

SAS PME System Administrators have a limited audit capability via the use of Event Viewer logs on the servers and workstations. If there is a significant incident, assistance may be requested from the USCIS Computer Security Incident Response Center.

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

In order to receive, access, and use USCIS systems, each employee must take initial and annual refresher security and privacy awareness trainings. These trainings include guidance about federal laws, policies, and regulations relating to privacy and information integrity, as well as the handling of Sensitive but Unclassified/For Official Use Only Information. The USCIS IT Security office and the USCIS Office of Privacy verify that employees successfully completed the trainings and maintain a record of certificates on all USCIS employees and contractors.

¹⁴ See 6 C.F.R. § 5.21 (2011).



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

SAS PME enforces strict access controls. Only users with a need to know are able to access the data and produce reports. As a new user is defined for SAS PME, roles are assigned. Each role has one or more profiles associated with it. The Separation of Duties concept for SAS PME is applied in accordance with DHS policy and procedures. In addition, for management of SAS PME, different personnel staff the SAS PME System Administrators and SAS PME ISSO positions. All access requests and changes must be processed by at least two people.

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?

SAS PME does not have system interfaces with systems outside of USCIS, so there are no Memoranda of Agreement or other sharing agreements with other agencies. Within USCIS, however, all of SAS PME's information source systems (Section 2.2) have an Interface Control Agreement with SAS PME itemizing each data element sent to SAS PME for read-only reporting.

Responsible Officials

Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Services
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



APPENDIX A

Interconnected Systems:

Fraud Detection and National Security Data System (FDNS-DS) is a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns.

PIA: FDNS-DS¹⁵

SORN: FDNS Records¹⁶

Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) consolidates and manages immigration and naturalization information from several USCIS information systems, reducing the labor involved in accessing, reporting, and sharing information.

PIA: eCISCOR¹⁷

SORNs:

- Alien File, Index, and National File Tracking System of Records¹⁸
- Benefits Information System¹⁹

¹⁵ See DHS/USCIS/PIA-013 Fraud Detection and National Security Data System (FDNS-DS), available at www.dhs.gov/privacy.

¹⁶ DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

¹⁷ See DHS/USCIS/PIA-023 - Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), available at www.dhs.gov/privacy.

¹⁸ DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013).

¹⁹ DHS/USCIS-007 - Benefits Information System, 73 FR 56596 (September 29, 2008).



APPENDIX B

Source System Data elements:

FDNS-DS:

FDNS-DS can transmit the following information to SAS PME: full name, alias, Social Security number (SSN), Alien Number (A-Number), associated A-Numbers of close relatives and associates, Receipt Number, address (home and business), date and place of birth, country of citizenship, citizenship status, gender, telephone number(s), e-mail address, place of employment and employment history, organizations (place of business, place of worship, if place of worship is sponsoring the applicant), family lineage, bank account information or financial transaction history, marriage record, civil or criminal history information, uniform resource locators, education record, Internet Protocol addresses, biometric identifiers (e.g., photographs, fingerprints, signature), TECS²⁰ and NCIC²¹ data and analysis resulting from the investigation or routine background checks performed as part of the adjudication process, or any other unique identifying number or characteristic.

eCISCOR:

eCISCOR can transmit the following information to SAS PME: Receipt Number, attorney information, A-Number, class expiration date, country of birth information, class of admission, date of birth, full name, date of last arrival, sex, SSN, beneficiary immigration information, beneficiary address information, form number, petitioner immigration status, petitioner address information, valid to/from dates, citizenship country information, immigrant/non-immigrant status code, family information, case status information, applicant address information, e-mail address, gender, height, marital status, phone number, permanent resident date, application fee information, interview information, and region information.

²⁰ See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy. See also DHS/CBP-011 - U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

²¹ See FBI-001 National Crime Information Center (NCIC), 64 FR 52343 (September 28, 1999).



APPENDIX C

SAS PME Users:

USCIS Office of the Chief Financial Officer (OCFO) Financial Management Division (FMD) and Planning Division

Office Mission:

The OCFO FMD reports the USCIS monthly financial status including how much money USCIS collected in fees and an estimate of how much of the collected fees still needed to be earned (i.e., deferred revenue). The monthly financial data is reported to the Department's Financial Management Office and further passed on to the U.S. Department of Treasury (DOT) and the DHS Office of Inspector General (DHS OIG) to meet government-wide reporting requirements.

The estimate of collected fees still needing to be earned is done by using Computer Linked Application Information Management System (CLAIMS) 3,²² CLAIMS 4,²³ and Marriage Fraud Amendment System (MFAS) accessed through eCISCOR. FMD uses SAS PME to obtain a duplicate-free population to model the agencies financial behavior.

SAS PME Reports and Uses:

The OCFO generates monthly deferred revenue estimates, errors excluded for DHS OIG and DOT. OCFO uses these reports to prepare the monthly deferred revenue estimate and the quarterly sampling plan.

Federal accounting standards require that respective immigration benefit application and petition revenue be deferred until the adjudication is complete. Fees received by USCIS for applications and petitions that are not completed at the end of a financial reporting period are not considered earned during that period and are reported in USCIS's annual financial statements as deferred revenue. To accomplish this, each month OCFO Accounting and Reporting Branch (ARB) compile the deferred revenue data and apply a statistical adjustment to account for known error, which is based on the error rate determined during the previous quarter's quality assurance review. ARB will post the reported deferred revenue balance within the USCIS general ledger by the DHS Treasury Information Executive Repository (TIER) submission deadline. OCFO FMD uses SAS PME to verify the USCIS financial reporting that USCIS must provide to DOT on a monthly basis. The DHS OIG is required to audit and verify the reported financial information.

Data Sources:

OCFO FMD analyzes data from CLAIMS 3, CLAIMS 4, and MFAS. USCIS uses National File Tracking System (NFTS)²⁴ data to determine the location of the file when USCIS

²² See DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3), available at www.dhs.gov/privacy. See also DHS/USCIS-007 - Benefits Information System, 73 FR 56596 (September 29, 2008).

²³ See DHS/USCIS/PIA-015 USCIS Computer Linked Application Information Management System (CLAIMS 4), available at www.dhs.gov/privacy. See also DHS/USCIS-007 - Benefits Information System, 73 FR 56596 (September 29, 2008).

²⁴ See DHS/USCIS/PIA-032- National File Tracking System (NFTS), available at www.dhs.gov/privacy. See also DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013).



calculates the monthly deferred revenue. This information is accessed through eCISCOR.

Data Elements:

OCFO created filters to ensure that no PII is transmitted to these reports. In this data cleaning process, the PII found in eCISCOR (e.g., name, date of birth, country of origin, status date, naturalization dates) remains in eCISCOR and are not sent in the reports. Only aggregate data is reported.

For example, the reports that are provided to DOT and DHS OIG would say USCIS received \$ XXXXX.XX for a given month.

Report Retention:

OCFO retains supporting information regarding USCIS finances for 6 years and 3 months. Any supporting information containing PII is stored on a shared drive with strict access controls.

Sharing:

DOT only receives summary-level financial data. While no PII is transferred to the reports, as part of DHS OIG's annual audit, they review the detailed data sample at USCIS offices, including receipt number, A-Numbers, and payment amounts to verify the accuracy of the reported financial summary, verify USCIS purpose and need to collect the fees, and verify the existence of pending applications.



USCIS FDNS Reports and Analysis Branch (RAB)

Office Mission:

The FDNS Reports and Analysis Branch (RAB) creates reports, provides analysis, and ensures data quality in support of the FDNS and USCIS missions. RAB provides internal intelligence in the form of predictive and behavioral analysis so that managers and staff are better able to understand USCIS operations; develops and produces recurring managerial, summary, workload, and operational reports; responds to ad hoc data analysis requests from internal and external components (e.g., DHS Intelligence & Analysis); develops appropriate methodologies for data gathering and reporting; and ensures that the data contained in FDNS-DS is sufficient to facilitate the reporting and analysis requirements of the Directorate.

SAS PME Reports and Uses:

FDNS uses SAS PME to generate the following reports:

- Monthly – Standardized reports used by FDNS Management and FDNS Field Offices
 - Field Priorities Report – 12 pivot tables to track progress towards meeting yearly priority goals
 - Government Performance and Results Act (GPRA)²⁵ Reports
 - Overseas Verification (OV) workload report
 - Monthly Refugee, Asylum and International Operations (RAIO) Report
 - Hours Reporting – Reporting of total work hours captured in FDNS-DS
 - Monthly National Security Report

- Quarterly– Standardized reports used by FDNS Offices and Executive Management
 - Front Office Workload (FOW) – Workload/operational reports
 - Annual Operating Priorities (AOP) – Provided to USCIS leadership
 - Staffing Allocation Model (SAM)
 - Directors National Security Report – National Security Issues
 - Employee Workload Report

These reports contain summaries of workforce case loads, case management, and FDNS priorities. For example, the Field Priorities Report provides a predefined baseline of performance that managers use to measure case cycle times and the production and efficiency of FDNS staff.

FDNS uses SAS PME to understand FDNS business processes. RAB uses the results of SAS PME-generated reports to conduct correlation tests to better understand trends in applications and rates of fraud, aggregate reports of workload, hours, and auxiliary statistics to help managers understand their programs, and conduct advanced statistical tests to research better processes and methods for internal operations and evaluate new programs. FDNS leadership uses SAS PME-generated reports to assist with resource allocation, case trend analysis, and determining staffing levels.

²⁵ See Government Performance and Results Act of 1993, Pub. L. 103-62, 107 Stat. 285; GPRA Modernization Act of 2010, Pub. L. 111-352, 124 Stat. 3866 (2011).

Data sources:

FDNS-DS and eCISCOR

Data Elements:

Reports that track cases do contain PII including name; date of birth; country of birth; case number; and in some cases, receipt numbers. This information is all from FDNS-DS data extracts.

Report Retention:

Current and previous fiscal year reports are stored electronically and accessible via FDNS SharePoint site for authorized users. The reports placed on SharePoint are PII-free. Reports that contain PII will be stored within the SAS PME system on the server and archived.

Sharing:

FDNS RAB shares the documents within USCIS to promote the Strategic Priority to “Strengthen National Security Safeguards and Combat Fraud”. All of the FDNS AOP performance measures and our GPRA measures are included in these reports



USCIS Office of Policy and Strategy (OP&S) Research and Evaluation Division (RED)

Office Mission:

The OP&S RED has three core missions: to provide research and evaluation that will enable sound immigration policy making; to improve core USCIS functions and programs through program evaluation and targeted research; and to provide expertise in social science, demographic, and policy research and evaluation. Through these missions, the RED strives to understand the behaviors USCIS benefit requestors and staff, evaluate performance of new or changing programs, and assess impact of existing programs, and imposed legislation.

SAS PME Reports and Use:

RED plans to develop reports, largely of descriptive statistics that characterize particular features of specific data, most often presenting these in summarized tabular form. These tables offer original analysis of data answering questions of interest to internal USCIS stakeholders. For example, RED may use extracts of workflow information from the Performance Analysis System (PAS) or Performance Reporting Tool (PRT) or may be descriptive demographic data accessed via eCISCOR and derived from USCIS forms (e.g., states represented in I-485, *Application to Register Permanent Residence or Adjust Status* applications).

RED staff occasionally uses SAS PME to analyze external public use data sets, such as those produced by Census Bureau, including American Community Survey (ACS) and Current Population Survey (CPS). RED uses SAS PME to analyze and manipulate this data, producing reports that explore relationships at different levels and among different variables in the data. This is done in order to answer research questions of interest to internal USCIS stakeholders. SAS PME is also occasionally used to duplicate and validate analysis results performed on USCIS data by external contractors.

Data Sources:

eCISCOR and external sources such as public use Census Data

Data Elements:

OP&S creates reports that contain aggregate data. The use of PII (SSN, A-number, etc.) is used to create the report parameters but will not be included within the report.

Report Retention:

OP&S retains the reports, either electronically or hard copy, for as long as there is a valid business need in accordance with GRS-20. These reports do not contain PII.

Sharing:

RED shares data derived from SAS PME with internal stakeholders to assist with and answer research questions of interest to internal USCIS stakeholders.