Privacy Impact Assessment
for the

Office of Immigration Statistics (OIS) Statistical Data Production and Reporting

DHS/ALL/PIA-071

December 7, 2018

Contact Point
Gary Lukowski
Office of Immigration Statistics (OIS)
Office of Policy
(202) 447-3401

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Office of Immigration Statistics (OIS) is responsible for carrying out two statutory requirements: 1) collecting and disseminating to Congress and the public information useful in evaluating the social, economic, environmental, and demographic impact of immigration laws; and 2) establishing standards of reliability and validity for immigration statistics collected by the Department's operational Components. To meet these requirements, OIS collects immigration-related data from across DHS and other federal immigration agencies, prepares the data for statistical purposes, and creates a variety of statistical products to inform the public, Congress, and Department leadership on key trends in immigration to the United States. OIS is conducting this Privacy Impact Assessment (PIA) as it collects and uses personally identifiable information (PII) to create its statistical products to inform the public on use of its PII and demonstrate how OIS mitigates privacy risks.

Introduction

Federal statutes, including the Immigration and Nationality Act of 1965, as amended, and the Homeland Security Act of 2002, as amended, as well as Executive Orders and mandates from Congressional appropriators and the Secretary of Homeland Security, require OIS to regularly prepare an extensive series of analytical and statistical reports on border security, immigration enforcement activities, refugee and asylum claims, and other immigration benefits. In December 2015, Congress's explanatory statement accompanying DHS's 2016 appropriations legislation specifically directed the DHS Office of Policy (which includes OIS), to report on the "enforcement lifecycle," defined as "the full scope of immigration enforcement activities, from encounter to final disposition, including the use of prosecutorial discretion." Further, Congress directed that "[a]ll data necessary to support a better picture of this lifecycle and the Department's effectiveness in enforcing immigration laws shall be considered and prioritized, including appropriate data collected by the [Executive Office for Immigration Review (EOIR)] at the Department of Justice [DOJ]."[1]

Fulfilling these requirements requires OIS to collect data related to the granting of immigration benefits, such as nonimmigrant admissions, grants of lawful permanent residence, changes in legal status, and naturalizations, as well as information related to the enforcement of immigration law, from across DHS and other federal immigration agencies such as the Department of State and the Department of Justice. These data contain both PII and Sensitive PII (SPII).[2] Using the statistical programming software SAS,[3] OIS processes these data, originally collected for

[1] *See* Consolidated Appropriations Act 2016 (Pub. L. No. 114-113), Division F, Joint Explanatory Statement.

[2] More information about PII and SPII can be found here: Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[3] SAS is a software suite developed by SAS Institute for advanced analytics, business intelligence, data

operational purposes, to prepare it for statistical analysis. This involves evaluating data for completeness, matching records across datasets, de-duplicating records, and converting or dropping data not formatted to standard codes.

OIS has several publicly available annual publications it produces from the data it receives, including the Yearbook of Immigration Statistics,[4] and reports on refugees and asylees, lawful permanent residents, naturalizations, non-immigrant admissions, and enforcement actions. OIS produces population estimates on the unauthorized population, lawful permanent residents, and nonimmigrants residing in the United States. Recent executive orders and memoranda and congressional and Department mandates have increased requirements for statistical analysis and reporting, including an immigration cohort outcomes analysis showing the broad movement of groups of individuals through the immigration enforcement system and reporting on legal immigrant adjustments of status.[5]

OIS uses information that was initially collected by DHS and other federal immigration agencies for their operational purposes. OIS receives data from Components within DHS through the DHS Policy for Internal Information Exchange and Sharing, also known as "One DHS" policy, which allows access within the Department to those with a need to know. For these and for agencies outside the Department, OIS is working to update and formalize data sharing arrangements with appropriate documentation in each case, including memoranda of agreement (MOA) and PII Request Forms or Computer Readable Extract (CRE) Request Forms, as appropriate.

This initial collection of information is outlined in source system Privacy Act system of records notices (SORN). Source system SORNs that provide OIS information include:[6]

- U.S. Citizenship and Immigration Services, Immigration and Customs Enforcement, and Customs and Border Protection Alien File, Index, and National File Tracking System of Records;[7]

management, and predictive analytics. SAS is not an acronym.

[4] The most recent Yearbook of Immigration Statistics is *available at* https://www.dhs.gov/immigration-statistics/yearbook.

[5] *See*, for example, Memorandum for the Secretary of State, the Attorney General, the Secretary of Homeland Security (March 6, 2017), *available at* https://www.whitehouse.gov/presidential-actions/memorandum-secretary-state-attorney-general-secretary-homeland-security/.

[6] The source systems may expand as future OIS requirements and responsibilities are determined. However, the data will be used and shared in the same manner that it is described in this PIA. Appendix A lists all of the source system SORNs from which OIS receives data from.

[7] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).

- U.S. Citizenship and Immigration Services Asylum Information and Pre-Screening System of Records;[8]
- U.S. Citizenship and Immigration Services Benefits Information System;[9]
- U.S. Customs and Border Protection Border Crossing Information;[10]
- U.S. Customs and Border Protection Border Patrol Enforcement Records;[11]
- U.S. Customs and Border Protection TECS;[12]
- U.S. Immigration and Customs Enforcement Criminal Arrest Records and Immigration Enforcement Records (CARIER);[13]
- U.S. Department of Justice (Executive Office for Immigration Review) Records and Management Information System;[14] and
- U.S. Department of State Refugee Case Records.[15]

While the collected operational data are covered by the respective SORNs, OIS intends to publish its own SORN, as it adjusts its methods for retrieving information by personal identifiers, to provide more clear notice of how the records are maintained and used once they enter OIS's analytical environment and are used for statistical purposes. Once in this environment, OIS cleans and processes the records in preparation for use in statistical analysis. Analyses may include merging of records from these distinct data systems to create new records.

OIS receives data from the data owners and evaluates it to ensure it aligns with statistical analysis needs. When OIS has questions about the data it receives, it reaches out to the data owner for clarification. Possible issues might include clarifying what a new data element means, ensuring the most important data elements are extracted, or prompting a search for missing data covering subsets of the population. OIS then processes this raw data and produces production datasets, or datasets ready for statistical analysis. From these datasets, OIS produces statistical tabulations and writes several of its reports. These reports highlight emerging trends in immigration and explain critical caveats about the data to stakeholders including Congress and the public.

In some cases, OIS merges datasets from multiple data owners across the Department and the immigration domain (including agencies within other federal departments). For example, in

[8] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015).
[9] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[10] DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016).
[11] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[12] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[13] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016).
[14] EOIR-001 Records and Management Information System, 69 FR 26179 (May 11, 2004) and 72 FR 3410 (January 25, 2007).
[15] STATE-59 Refugee Case Records, 77 FR 5865 (February 6, 2012).

order to conduct its immigration cohort outcomes analysis, OIS matches datasets from U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), and DOJ's EOIR. Linking these datasets is not automatic but involves analysis to determine which records are linkable and depends on what unique identifiers are available in each dataset. Though linking records is currently not 100% accurate, accuracy is sufficient for showing the broad movement of individuals through the immigration enforcement system, helping to identify bottlenecks in case processing and inform effective immigration policy and resource use.

The information OIS uses in its analyses is collected from several DHS Components and other federal agencies. These entities initially collect the information on members of the public to process immigration enforcement and benefits. PII data elements that OIS receives and uses to correctly merge datasets include:

- Name;
- Date of Birth;
- Gender;
- Citizenship;
- Alien Registration Number (A-Number) (a person-based identifier given to all immigrants, both authorized and unauthorized);
- IDENT-FINs (a biometric identifier based on fingerprints collected from those aged 14 and up);[16] and
- EID civ ID (ICE ENFORCE-generated identification number, of which an alien can receive multiple).[17]

OIS receives other non-PII data elements in the datasets about individuals that are not used for merging or matching but are used to report on outcomes and administrative events. Such events include immigration enforcement actions (*e.g.*, issuing a Notice to Appear (NTA) or Final Order of Removal, detention, or deportation) as well as grants of an immigration benefit (*e.g.*, admission at a port of entry, admission as or adjustment to lawful permanent resident status, or grant of naturalization).[18] Other information received includes the dates at which these events occur.

[16] More information can be found in DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

[17] More information can be found in DHS/ICE/PIA-015 Enforcement Integrated Database (EID) Criminal History Information Sharing (CHIS) Program, *available at* https://www.dhs.gov/publication/dhsicepia-015h-enforcement-integrated-database-eid-criminal-history-information-sharing.

[18] *See* https://www.dhs.gov/immigration-statistics/data-standards-and-definitions/definition-terms for selected definitions.

OIS does not retrieve records by personal identifier for the purpose of making decisions about individuals. However, records are merged by linking personal identifiers to ensure the data are correctly attributed to one individual across multiple datasets. The purpose of this is to enable OIS to examine large trends in groups or cohorts of those who interact with the immigration system. While these analyses will inform high-level strategic operational planning, data OIS possesses are not used directly for operational purposes such as the vetting of an individual or the adjudication of a benefit. OIS data are strictly used for statistical analysis and reporting.

OIS plans to leverage USCIS's instance of SAS Predictive Modeling Environment (SAS PME) for its merging and reporting needs.[19]

SAS PME is a shared data analytics platform used by USCIS. SAS PME, a suite of reporting tools connected to the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR),[20] allows USCIS to access large amounts of data from eCISCOR to conduct research and analysis, including predicting future circumstances that may affect USCIS operations. SAS PME 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 from multiple systems, and forecast trends among populations or form types. SAS PME allows users to run various pre-set statistical models (*e.g.*, regressions) and derive conclusions based on data.

USCIS will establish a separate, dedicated storage instance attached to the USCIS SAS PME cloud environment for OIS statisticians to perform their statistical analysis. Specifically, at the application level, OIS will have access to the appropriate USCIS data (via eCISCOR) and will co-mingle that data with other data it receives separately from other Components and external agencies within the OIS storage space. DHS Component data will be uploaded manually to the Secure File Transfer Protocol (SFTP) server and copied nightly to the OIS dedicated storage space.

OIS statisticians will work directly in SAS PME working simultaneously with USCIS data and with other DHS Component data stored separately in the isolated OIS storage space. The isolated OIS storage space will be an encrypted storage container that will only be accessible to OIS employees that are assigned to OIS. OIS users will log into SAS PME and will have appropriate access to the OIS storage space and to only USCIS data for which they have a need to know. OIS plans to migrate its datasets from current holding in its shared network drive to the dedicated provisions storage attached to SAS PME. As updated datasets are received, OIS will continue ingesting the information into SAS PME.

OIS is choosing to use SAS PME because of resource constraints to stand up its own

[19] For more information, please *see* DHS/USCIS/PIA-055 SAS Predictive Modeling Environment (SAS PME) and forthcoming eCISCOR Reporting Tools PIA, *available at* https://www.dhs.gov/privacy.

[20] *See* DHS/USCIS/PIA-023 Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* https://www.dhs.gov/privacy.

environment; OIS will update this PIA when it does stand up its own environment. SAS PME meets the interim capability requirements of OIS. OIS is planning to use SAS PME for the next two to three years, and ultimately plans to acquire its own analytic environment. OIS will access SAS PME through license agreements with USCIS. Only authorized OIS personnel will access the system.

Holding and combining records with PII raises a number of privacy risks. Because OIS does not collect the data directly from the public, a risk exists that the public may not be aware of OIS's use of the data. A risk exists that the data could be intercepted in transit from the data owner to OIS, or an external attacker could access the data. A risk exists that internal personnel without a need to know may be able to access it, or that personnel with some level of access to the data may access more than they need for their legitimate mission purpose or may use it in an unauthorized manner. These risks are heightened because OIS combines data from multiple Federal agency sources and a breach potentially jeopardizes more information about an individual than a breach of the original data at the data owner level. Further risks exist that OIS may keep the data for longer than needed, the data may be erroneous, or members of the public may not be able to correct OIS records pertaining to them.

OIS respects the risks raised above and is working to mitigate them to the greatest practicable extent possible. OIS seeks to address certain risks through the publication of this PIA, which notifies the public how OIS uses its data, despite not having the opportunity to inform those on whom data are collected at the time of collection. OIS is developing information technology (IT) solutions such as SFTP with partners to ensure data are protected in transit, and moving away from physically transporting data on CDs or other media. When data must be transported on CDs, OIS and partners use appropriate encryption. Within OIS, the Principal Director determines who needs access to which data, and OIS is exploring IT and standard operating procedure (SOP) solutions to more narrowly allow specific personnel access to subsets of the data. All personnel with access to the data take mandatory IT security and privacy training.

Though data owners have their own records retention schedules, OIS complies with its own records retention schedule approved by the National Archives and Records Administration (NARA).[21] OIS is developing SOPs to ensure compliance. Although no practicable method exists for members of the public to query their records at OIS and correct erroneous information, these records are only used for statistical reporting purposes, so there is no personal harm to the member of the public if OIS's data are incorrect. Members of the public may reach out to data owners for this purpose as stated in relevant Privacy Act Statements/Notices or other notices at collection and applicable source system SORNs.

[21] Please *see* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-09-003_sf115.pdf.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and IT systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that OIS is an office rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This PIA examines the privacy impact of OIS operations as they relate to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

OIS does not collect information directly from individuals, and therefore does not provide any direct notice to individuals at the point of collection. All of the information OIS uses for reporting is extracted from other DHS and other federal immigration agencies' systems identified above. Depending on the source system, notice may have been provided by Privacy Act Statements/Notices or other notices or applicable source system SORNs and PIAs.

Privacy Risk: There is a risk that individuals providing information do not have notice that explains how their information is being transferred to OIS for use in statistical reporting and analysis.

Mitigation: This risk is partially mitigated. This PIA gives general notice to the public of how OIS uses such data. Additionally, OIS intends to publish a new OIS SORN, as it adjusts its methods for retrieving information by personal identifiers, to account for multiple data sets being linked by personal identifiers, in order to more clearly provide notice of how data are being used.

Otherwise, OIS must rely on the original collector of the information to properly notify at the time of collection with the appropriate Privacy Act Statements/Notices or other notices.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

OIS does not collect information directly from the individual. However, most of the information OIS receives was collected by an agency directly from or about the individual. OIS must rely on the original collector of the information to accurately enter the information and properly notify at the time of collection with the appropriate Privacy Act Statements/Notices or other notices informing individuals of whether they must consent to the collection of PII and how their data will be used, disseminated, and maintained. Individuals seeking to access or correct any record may notify the data owner of their query or correction, rather than OIS, who does not have access to and cannot correct the original data. Information within OIS originates with the source system. As a result, individuals can gain access to their information by following the access procedures outlined in the PIAs and SORNs of the source systems listed on the Privacy Act Statements/Notices or other notices that accompany the original information collection. Individuals may also follow the access/amendment procedures that will be outlined in the forthcoming OIS SORN.

In addition, individuals seeking notification of and access to any record contained in the source system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under Contact Information. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to:

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
245 Murray Drive, SW, Building 410, STOP-0655
Washington, D.C. 20528

Privacy Risk: There is a privacy risk that individuals will be unable to correct or amend information about them that is used by OIS.

Mitigation: This risk cannot be fully mitigated because there is not a process for individuals to amend erroneous information once it has been shared with OIS, and OIS cannot change records that have been stored for analytic purposes. This PIA provides notice to individuals whose information is used by OIS that redress procedures are outlined in the PIAs and SORNs of the source systems. Additionally, because of the law enforcement nature of a number of the source systems from which OIS receives data, DHS has exempted portions of the applicable systems of records from the notification, access, amendment, and certain accounting provisions of the Privacy Act.

However, even though individuals may not be able to correct or amend their information used by OIS, there is no direct impact to those individuals if the information is incorrect. No decisions are made about individuals based upon OIS's use of the data, so there is limited impact of erroneous data on the aggregate summaries produced or impact to individuals.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

OIS's core mission was established through legislative and administrative reporting mandates, including the Immigration and Nationality Act of 1965, as amended, the Homeland Security Act of 2002, and mandates from congressional appropriators and from the Secretary of Homeland Security. Presidential Executive Orders 13767, "*Border Security and Immigration Enforcement Improvements*," and 13768, "*Enhancing Public Safety in the Interior of the United States*," and the Memorandum for the Secretary of State, the Attorney General, the Secretary of Homeland Security (March 6, 2017) direct DHS to provide greater transparency in immigration enforcement. Additional authorities include: 8 U.S.C. 1103(d), Statistical Information System; 6 U.S.C. 341(b), Immigration; and the Consolidated Appropriations Act, 2016 (Pub. L. No. 114-113).

Furthermore, each PIA and SORN articulates the authority for the original data collection from the public as well as the intended purpose for maintaining the system of records. OIS receives the data for statistical purposes from Components through intra-agency transfer, and the "One DHS" policy, which ensures DHS Components and offices, including OIS, have access to data within the agency with a "need to know." Statistical analysis is compatible with the purposes for which the data are collected as it enables the agency and the Components collecting the information to improve operational effectiveness.

OIS expects to develop a sharing agreement covering DHS Components and put agreements in place with external agencies allowing sharing of records containing PII, dependent on identified authorities and compliance with the fair information practices as set out in the Privacy Act of 1974.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

OIS limits its requests for data to only those data elements or variables it requires to complete its statistical analysis and reporting. Though data owners have their own records retention schedules, OIS complies with its NARA-approved records retention schedule.[22] OIS is developing SOPs to ensure compliance with these requirements.

The retention schedule classifies OIS records into several categories of records. Records containing PII that OIS uses to complete its statistical analyses and reporting fall into Section 6: "Research and background material used to produce the Yearbook of Immigration Statistics." The scheduled disposition provides for the data to be evaluated for remaining business need or destruction three years following the end of the fiscal year in which the yearbook is produced. However, the schedule authorizes longer retention periods if records are needed for business use beyond this period. Many tables in the Yearbook of Immigration Statistics and accompanying reports contain tabulations of ten years, and in some cases OIS must compare new records with records going back several decades.

Due to this need to keep records dating back several decades, OIS retains PII for a significant period of time.

Privacy Risk: There is a risk that OIS will retain this information for longer than is necessary.

Mitigation: This risk is not fully mitigated. OIS has an established NARA-approved records retention schedule that it will follow and will ensure that records are destroyed after the business use of the data is no longer valid. However, due to unknown future requests and data required for future comparisons, a large portion of the data OIS maintains is kept for longer than three years.

Although this presents additional risk, access to the data within OIS is limited to those with "need to know" and available only to OIS personnel. Additionally, moving to SAS PME provides greater technical security for ensuring this is the case. SAS PME has technical safeguards, including access controls and auditing capabilities, which provide greater security for securing the large quantities of data that will be held in the OIS storage instance.

[22] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-09-003_sf115.pdf.

Data that are copied to the OIS storage container from the SFTP server[23] will be deleted from the SFTP server once the copy completes. In the OIS storage container, the data will not be overwritten or merged when copied. This data is required to be kept to in order to provide an accurate accounting of immigration records over time. OIS is responsible for managing and organizing the data once in the dedicated storage. USCIS will capture and store a daily log of the transaction for future auditing, but not the data itself.

DHS Privacy Office Recommendation: OIS should review its data holdings on a yearly basis to ensure that it is still required for business purposes.

Privacy Risk: There is a risk that OIS will retain more information than is necessary to perform its mission.

Mitigation: This risk is mitigated. OIS limits its requests for data to only those data elements or variables that it requires to complete its statistical analysis and reporting. If OIS receives data that it did not request or does not need, it deletes the data from its holdings. OIS limits its requests to identifiers necessary to determine or match unique individuals across data sets, to information indicating immigration-related events or status changes, and to other demographic or biographical information required to inform the public, Congress, and Department policy makers on immigration trends.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Each source system SORN articulates the purpose for the original data collection. While these SORNs do not currently specify the use of the information downstream for statistical purposes, OIS receives the data for statistical purposes from DHS Components through intra-agency transfer, and the "One DHS" Policy, which ensures access within the agency with a "need to know." Statistical analysis is compatible with the purposes for which the data are collected as it enables the agency to improve operational effectiveness. Reports released to the public do not contain PII, but rather contain tabulations based on characteristics such as demographics, broad geographical information, or being the subject of an immigration action. This data is aggregated and not re-identifiable.

Currently OIS does not share data in an identifiable form with agencies outside DHS. While an exception to the Privacy Act applies to sharing data for statistical purposes in non-identifiable form, there is currently no exception, exemption, or routine use allowing OIS to share PII with non-DHS statistical agencies. Therefore, OIS intends to publish an OIS-specific SORN that will

[23] The SFTP server is a separate service that SAS PME leverages to facilitate the safe transfer of data by components for OIS reporting and analytics. Data will be uploaded to the SFTP server according to each agency's existing and established protocols. However, the information is copied from the SFTP server daily.

describe OIS sharing information with external statistical agencies.[24] While PII is not released in final products, PII allows more accurate record linkage across agencies, improving data quality and integrity of reporting.

<u>Privacy Risk</u>: There is a risk that the data used to produce OIS reports may be used for unauthorized purposes.

<u>Mitigation</u>: This risk is mitigated. Only authorized OIS personnel have access to the data used to produce OIS reports. The OIS Principal Director determines who requires access for authorized purposes, and such personnel receive annual IT security and privacy training.

These controls ensure that OIS information is not used for a purpose other than why it was shared with OIS in the first place (*e.g.*, not used for making a benefit determination on an individual).

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

When OIS receives data into its dedicated storage space attached to SAS PME, it first reviews the data to ensure to the extent possible that the data are complete and accurate, and that OIS personnel properly understand the meaning of the data. These checks generally catch issues such as non-standard variable codes (*i.e.*, variable values that are not approved for use and so do not have a clear meaning) or subsets of the population that may not have made it into the data extract submitted to OIS. In some cases, OIS requests more than one extract to look for inconsistencies. As the data are never used to adjudicate a benefit or in considering the disposition of a case, errors in a specific record do not affect the individual in the record. Data integrity checks do ensure, though, that the data are suitable for the kinds of statistical analysis and reporting which OIS conducts, as well as point to appropriate caveats OIS should append to reports and tabulations.

OIS is conducting research to enable it to more accurately link record across datasets, but again, errors in linking do not affect the subjects of any of the involved records on an individual level. The data linking procedures OIS are developing and improving are to ensure an overall quality to the data that allow statistical - and not operational - use.

[24] DHS will issue an updated PIA once the OIS SORN is published to indicate that identifiable information will be shared outside of DHS.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

OIS has developed IT solutions such as SFTP with partners to ensure data are protected in transit, and moved away from physically transporting data on CDs.

OIS currently does not operate an IT system, and so is not covered under an Authority to Operate (ATO). In the interim, it expects to host its data within OIS's own dedicated storage space attached to USCIS's SAS PME environment, and will be incorporated under its ATO as either a Subsystem or Minor Application. Data within that environment will be covered by an OIS security plan to which the security plan covering SAS PME will point.

Within OIS, and prior to the use of SAS PME, the data resided on a shared drive, accessible only to OIS personnel. The OIS Principal Director determined who required access to which data. OIS will migrate its datasets from current holding in its shared network drive to its own storage attached to SAS PME. OIS will remove this historic data from its shared drive, and no longer use it to store the data long term.

As updated datasets are received, OIS will ingest the information directly into SAS PME through SFTP rather than store it on a shared drive internally at OIS. In the event OIS requires data from Components or other federal agencies with which SFTP is not established, physically transporting data on CDs may be necessary. Where this is the case, OIS and partners use appropriate encryption. This data will then be manually uploaded into SAS PME.

In the longer term, OIS may, with the Immigration Data Integration Initiative (IDII),[25] develop its own IT system to store and process its data and will then have its own ATO.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

OIS currently does not operate its own IT system, and so has limited IT auditing solutions available, but expects to build these mechanisms into any system that it may develop with the IDII.[26] Current safeguards include limiting access to OIS personnel with a need to know, and

[25] Launched in September 2016, the DHS Immigration Data Integration Initiative (IDII) aims to ensure uniform Department-wide immigration data standards, to give the Department's data stakeholders real- or near real-time access to relevant data from across the Department, and to ensure that immigration records are fully linkable across DHS data systems. An integrated immigration data system will strengthen immigration operations by allowing officers to more easily track individuals through immigration enforcement and benefits systems and will strengthen DHS's ability to analyze and report on immigration policies and policy outcomes.

[26] The future state of the OIS program and IDII will be subject to additional privacy compliance documentation and requirements.

mandatory IT and privacy training for those personnel. Personnel with a need to know may not use PII for unauthorized purposes. Any requests for PII outside the office are subject to review in consultation with the Privacy Point of Contact. OIS is developing SOP solutions to track any disclosures of PII outside the office. All personnel with access to the data take mandatory IT security and privacy training.

SAS PME administrators will regularly monitor the system for compliant and authorized use of OIS data. This is achieved through SAS's Audit, Performance, and Measurement (APM) utility. APM is able to audit administrative modifications, user and group access updates, user level usage patterns, authentication failures, and data usage reports. Results of such reports will be made available to the OIS Principal Director on an as needed or recurring basis.

Responsible Officials

Gary Lukowski
Principal Director, and Director, Standards and Operations Division
Office of Immigration Statistics (OIS)
Office of Policy
Department of Homeland Security

Approval Signature

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

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Source system SORNs from which OIS receives data

- U.S. Citizenship and Immigration Services, Immigration and Customs Enforcement, and Customs and Border Protection Alien File, Index, and National File Tracking System of Records;[27]
- U.S. Citizenship and Immigration Services Asylum Information and Pre-Screening System of Records;[28]
- U.S. Citizenship and Immigration Services Benefits Information System;[29]
- U.S. Customs and Border Protection Border Crossing Information;[30]
- U.S. Customs and Border Protection Border Patrol Enforcement Records;[31]
- U.S. Customs and Border Protection TECS;[32]
- U.S. Immigration and Customs Enforcement Criminal Arrest Records and Immigration Enforcement Records (CARIER);[33]
- U.S. Department of Justice (Executive Office for Immigration Review) Records and Management Information System;[34] and
- U.S. Department of State Refugee Case Records.[35]

[27] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).

[28] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015).

[29] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).

[30] DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016).

[31] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).

[32] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

[33] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016).

[34] EOIR-001 Records and Management Information System, 69 FR 26179 (May 11, 2004) and 72 FR 3410 (January 25, 2007).

[35] STATE-59 Refugee Case Records, 77 FR 5865 (February 6, 2012).