Privacy Impact Assessment
for the

United Nations High Commissioner for Refugees (UNHCR) Information Data Share

DHS/USCIS/PIA-081

August 13, 2019

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

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

Abstract

On January 9, 2019, the Department of Homeland Security (DHS) entered into a Memorandum of Understanding (MOU) with the United Nations High Commissioner for Refugees (UNHCR) to share biometric and associated biographic data on refugees seeking to resettle in the United States. DHS and UNHCR entered into this MOU to expand the scope of the existing information shared through the State Department to support the U.S. Refugee Admissions Program (USRAP). Under the 2019 MOU, UNHCR is now directly sharing biometric and associated biographic information with DHS Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT) (soon to be replaced by Homeland Advanced Recognition Technology (HART)). The electronic transmission of data between UNHCR and IDENT/HART is facilitated by U.S. Citizenship and Immigration Services (USCIS) Enterprise Service Bus (ESB). USCIS is conducting this Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with collecting and using biometric and associated biographic UNHCR data for identity verification purposes. This PIA is limited to covering the collection and use of UNHCR data for identity verification purposes, as well as to identify any incident of potential identity fraud, by DHS and other entities authorized by the MOU. Any additional uses of UNHCR data will be addressed in a future PIA.

Introduction

Individuals outside the United States seeking admission as a refugee under Section 207 of the Immigration and Nationality Act (INA), as amended, are processed through the U.S. Refugee Admissions Program (USRAP).[1] From initial registration for refugee status until entry into the United States, a refugee interacts with many different agencies and organizations, including DHS,[2] the Department of State (DOS),[3] UNHCR,[4] the Resettlement Support Centers (RSCs),[5]

[1] Under the Immigration and Nationality Act (INA), a refugee is an alien who, generally, has experienced past persecution or has a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion. Individuals who meet this definition may be considered for either refugee status under Section 207 of the INA if they are outside the United States, or asylum status under Section 208 of the INA, if they are already in the United States.

[2] Within DHS, USCIS determines whether an individual is eligible for classification as a refugee; U.S. Customs and Border Protection (CBP) screens and admits refugees at the port of entry.

[3] DOS has USRAP management responsibility overseas and has the lead in proposing admissions ceilings and processing priorities.

[4] UNHCR refers cases to the USRAP for resettlement and provides important information with regard to the worldwide refugee situation.

[5] DOS's Bureau of Population, Refugees, and Migration (PRM) funds and manages seven RSCs around the world operated by non-governmental organizations (NGOs), international organizations, or U.S. embassy contractors. Under PRM's guidance, the RSCs prepare refugee applications for U.S. resettlement consideration.

Department of Health and Human Services (HHS),[6] International Organization for Migration (IOM)[7] and various non-governmental organizations. While each agency plays a unique role in the refugee resettlement process, they all use the same or similar identity information to differentiate individuals.

Many individuals seeking refugee resettlement register with UNHCR in the country to which they have fled. When an individual registers with UNHCR claiming to be a refugee, he or she is enrolled into UNHCR's respective IT case management systems.[8] During the registration process, UNHCR collects biometric and associated biographic information. This information is used to perform identity verification during UNHCR's subsequent interviews and encounters with the individual. If the individual is determined to be a refugee and that resettlement is the most viable permanent solution, UNHCR then begins the referral process. If the referral is made to the United States, UNHCR prepares and sends an electronic file with biographic data, case information, and the facial photo of each case member to DOS and, where applicable, directly uploads it to the Worldwide Refugee and Asylum Processing System (WRAPS).[9]

When UNHCR refers a refugee applicant to the United States for resettlement, the case is received and processed by a Resettlement Support Center (RSC). RSCs carry out administrative and processing functions, such as file preparation, data collection, and out-processing activities during the refugee admissions process. RSCs conduct the initial prescreening interview with refugee applicants and initiate biographic checks. RSCs collect biographic and other information from the applicants to prepare cases for security screening, interview, and adjudication by USCIS.

The USCIS Refugee, Asylum, and International Operations Directorate (RAIO) Refugee Affairs Division (RAD) is responsible for interviewing refugee applicants, receiving and reviewing results of all background checks, and adjudicating applications for refugee status.[10] Before conducting the interview, USCIS officers verify the refugee's identity by visually comparing the facial photo in the RSC-prepared documentation to that of the refugee appearing for the interview. In advance of or at the time of refugee interview, USCIS collects the refugee applicant's fingerprints (i.e.,10 flat and rolled for individuals within a certain age range), along

---

[6] HHS Office of Refugee Resettlement (ORR) administers domestic resettlement benefits for arriving refugees.
[7] IOM, DOS contractors, serve primarily as the travel agent for USRAP. DOS Contractors make travel arrangements for refugees eligible for resettlement and assist them with travel and processing at the port of entry in the United States.
[8] UNHCR is an international agency and is not required to adhere to the requirements of U.S. federal privacy laws about conducting PIAs for IT case management systems.
[9] WRAPS is the DOS case management database used for all refugee applicants processed for resettlement consideration to the United States. Please see the WRAPS PIA and SORN for more information on this system and the information it collects, uses, and maintains. Available at https://2009-2017.state.gov/documents/organization/262062.pdf. RPC, operated by DOS contractors, is the central data repository for all overseas and domestic resettlement operations. The RPC manages the WRAPS database.
[10] *See* DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting, *available at* www.dhs.gov/privacy.

with a signature and a photograph, which are automatically uploaded to Customer Profile Management System (CPMS).[11] Since the refugee's first encounter with the United States Government occurs during the resettlement process, the refugee's biometrics – obtained by USCIS – are frequently the first to be collected, retained, and used for identity verification and screening purposes by the U.S. Government. USCIS uses the biometric data it collects for biometric enrollment, identity verification checks, and for security checks.

USCIS uses the information from the application, security checks, interview, and supplemental evidence to determine whether the individual is eligible for refugee status. The application is either approved or denied. USCIS refers eligible applicants to RSCs for out-processing and issuance of a transportation letter. RSCs process approved cases for travel, including scheduling medical exams and arranging sponsorship by a domestic resettlement agency. RSC sends the paper documents to IOM and generates the Refugee Travel Packet.

After a refugee is authorized for travel to the United States, CBP receives a manifest of all individuals who have approved filings and have made reservations to travel to the United States by air. CBP receives this manifest before the scheduled travel date and performs initial vetting of the individuals before they arrive at a port of entry and then conducts background checks and inspection of these individuals upon arrival at a U.S. Port of Entry. CBP determines if the applicant is admissible to the United States and, if so, admits the individual as a refugee.[12]

Data Sharing with UNHCR

DHS entered into a Memorandum of Understanding (MOU) with UNHCR titled *Memorandum Of Understanding (MOU) between Department of Homeland Security (DHS) and United Nations High Commissioner for Refugees (UNHCR) on the Sharing of Personal Data*, effective January 9, 2019, to share biographic and biometric data on refugees seeking to resettle in the United States. The MOU expands the scope of information shared between the two agencies that has taken place through the State Department in support of the U.S. Refugee Admissions Program (USRAP). Under the terms of the MOU, DHS receives UNHCR refugee biometric data (e.g., fingerprints, photograph, and/or iris) along with associated biographic data[13] (e.g., name, date of birth, place of birth, and gender) upon referral and acceptance for access to USRAP. The biographic and biometric information establish an initial identity that allows DHS to later

[11] *See* DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), *available at* www.dhs.gov/privacy.
[12] Entry of refugees to the United States is limited to only six US International Air Ports of Entry: Chicago, Houston, Los Angeles, Miami, Newark, and New York.
[13] As listed in the MOU, the biographic, or personal, data elements include: name (including family name and all given names), date of birth, country of origin, gender, and unique identification number.

biometrically verify that the individual being processed by DHS for refugee resettlement is the same individual who was registered and referred by UNHCR.

As noted above, a refugee applicant to the United States is encountered and processed by various entities throughout the refugee resettlement process. This MOU allows the direct sharing of additional biometric data collected by UNHCR during refugee registration process with DHS. Biometric verification guards against substitution of individuals or identity fraud in the resettlement process. Many refugees live for long periods in asylum countries and the use of biometrics ensures that there is unbroken continuity of identity over time and between different locations. When resettlement is pursued, biometric verification helps provide assurance of identity through all steps of the process.

The information from UNHCR is stored in DHS IDENT/HART, which serves as a biographic and biometric repository for DHS.[14] When a referral from UNHCR is sent to DHS, the biometrics and associated biographic data originally collected by UNHCR will be sent to IDENT/HART for fingerprint-based enrollment. The transmission of information between UNHCR and DHS is facilitated by the USCIS Enterprise Service Bus (ESB) in an effort to connect and share data from different operating systems.[15] Serving as a conduit, ESB replaces all direct contact with applications and operates between the applications, so that all data exchanges take place through the ESB. The transfer of information is invoked by the end source systems. When exchanging data from one system to another, the ESB translates the message from one system format to another format to enable effective and secure synchronization and integration of data. ESB assists with the seamless and accurate exchange of information from disparate systems by facilitating the transfer of data.

UNHCR shares a specified amount of information with DHS to support the identity verification of the individual, as well as identify any incident of potential identity fraud.[16] Information sent to DHS from UNHCR may include the following: fingerprints, facial images, iris scans, full name, date of birth, gender, a uniquely assigned UNHCR identifier, and date and location of collection. The process of retaining fingerprint data provided to IDENT/HART is referred to as *enrollment*. Once an identity has been enrolled in IDENT/HART, additional collections of biometrics and biographics linked to that enrollment are called *encounters.*

---

[14] Please note that the Homeland Advance Recognition Technology (HART) system will be replacing IDENT. *See* forthcoming HART Increment 1 PIA *available at* www.dhs.gov/privacy.
[15] *See* DHS/USCIS/PIA-008 Enterprise Service Bus 2 (ESB), *available at* www.dhs.gov/privacy.
[16] USCIS will not be using the photograph to conduct automated facial recognition. USCIS will do a manual comparison of the photograph provided by UNHCR with the person who appears at the interview.

Encounters are accessible to IDENT/HART users based on filtering rules that are defined by the data owner and configured by the OBIM system administrators.[17]

Through IDENT/HART, DHS provides biometric encounter information to authorized users to verify the identity of individuals they encounter pursuant to their missions and determine whether those individuals are eligible to receive a benefit or should be subject to a law enforcement or intelligence action. DHS uses UNHCR data to verify that the individual being processed by USCIS personnel is the same individual who was registered and referred by UNHCR. The information shared by UNHCR and enrolled in IDENT/HART will be available to other DHS Components and external entities, in accordance with confidentiality provisions of 8 CFR § 208.6 as applied by policy to refugee information, to use for purposes that align with the purposes mentioned in the *MOU between DHS and UNHCR for Refugees on the Sharing of Personal Data*, effective January 9, 2019.[18] The MOU authorizes DHS to provide Department of Justice (DOJ), Department of Defense (DoD), DOS, and other federal agencies with a national security and counterterrorism responsibility to access UNHCR data in IDENT/HART.

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.

---

[17] The Homeland Advance Recognition Technology (*HART*) system will be replacing IDENT. *See* forthcoming HART Increment 1 PIA, *available at* www.dhs.gov/privacy.

[18] In addition to the regulatory confidentiality restrictions and the restrictions on sharing provided in the MOU, when persons who provide biometrics to UNHCR that are then enrolled in IDENT/HART become U.S. citizens or Lawful Permanent Residents, disclosure of those biometrics become protected by the Privacy Act and covered by the DHS/ALL-041 External Biometric Records System of Records Notice. *See* DHS/ALL-041 External Biometrics Records (EBR) System of Records, 83 FR 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208 and the Homeland Security Act of 2002, Section 222.This PIA examines the privacy impact of the UNHCR and DHS information sharing agreement as it relates to the FIPPs.

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.

DHS provides individuals general notice through the publication of PIAs and associated SORNs. This PIA provides the public with transparency about the sharing of UNHCR data with DHS. In addition to this PIA, DHS will mention the provision of biometrics from UNHCR in the forthcoming USCIS ESB 2 PIA and the forthcoming HART Increment 1 PIA. The forthcoming ESB 2 PIA covers the interconnection between UNHCR and DHS HART. The forthcoming DHS HART PIA lists UNHCR as a data source to HART. USCIS also provides notification about its participation in the refugee process in the Refugee Case Processing and Security PIA[19] and Refugee Case Processing and Security Screening Information System of Records.[20] Further, the External Biometrics Records SORN covers the maintenance of data from external sources like UNHCR.[21]

Privacy Risk: A privacy risk remains that UNHCR data will be shared with DHS or its partners even when an individual may never be encountered by DHS.

Mitigation: This risk is partially mitigated. The MOU with UNHCR stipulates that UNHCR may only share information of individuals who have been referred to the United States for resettlement. This makes it more likely that DHS will encounter those individuals at some time. However, it is possible that some of these individuals may drop out of the refugee resettlement process, so DHS may in those cases, continue to hold biometrics on individuals it may not encounter during the refugee resettlement process. It is possible, however, that DHS or other IDENT/HART users may encounter those individuals in a different context, for example during travel to the United States at a later point. In some cases, these individuals may seek refugee status

[19] *See* DHS/USCIS/PIA-068 Refugee Case Processing and Security, *available at* www.dhs.gov/privacy.
[20] *See* DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[21] *See* DHS/ALL-041 External Biometrics Records (EBR) System of Records, 83 FR 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

in a different country and then travel to the United States as citizens of a third country and be encountered by DOS or CBP.

DHS entered into the MOU with UNHCR prior to the sharing of information. The MOU between DHS and UNHCR fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. The MOU notes that DHS is to not share any personal data collected by UNHCR with agencies outside of DHS except for encounter data, which may be shared with DOJ, DOD, DOS, and other agencies tasked with national security and counterterrorism responsibilities. Through processes described in the HART Increment 1 PIA, OBIM configures access to records to be consistent with data owner rules and terms of information sharing and access agreements. DHS may only share encounter data with these external U.S. Government agencies when the fingerprints shared by UNHCR matches on the fingerprints of individuals already known to DHS, for whom there is also derogatory information.

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.

Under this program, it is not practical for DHS to directly seek individual consent prior to the collection and use of the personally identifiable information (PII) received from UNHCR. UNHCR is responsible for screening individuals and referring them to the United States and other countries. UNHCR collects the information directly from the individual seeking refugee benefits and may notify these individuals during the registration process that UNHCR may share their information with DHS and other participating members of USRAP as part of the referral process. The biographic and biometric data collected from UNHCR is used to determine whether they qualify as refugees and if they are in particular need of resettlement.

Under the terms of the MOU between DHS and UNHCR for Refugees on the Sharing of Personal Data, UNHCR sends the information of those applicants requesting U.S. resettlement to DHS IDENT/HART. The data will be a one-way transfer of refugee biometric data (e.g., fingerprints, facial image, and/or iris scans) along with associated biographic data (e.g., name, date of birth, place of birth, and gender) from UNHCR to OBIM IDENT/HART. The USCIS ESB facilitates the transfer of information from UNHCR to DHS IDENT/HART. The information stored in DHS IDENT/HART allows DHS to verify whether the individual being processed by DHS for possible refugee resettlement is the same individual who was registered and referred by UNHCR. An individual may seek access to his or her DHS records by filing a Privacy Act or Freedom of Information Act (FOIA) request.

Individual participation provides the government with the most accurate information about the public, while the public is given greater access to the information maintained by the government. The right for individuals to request amendments of their records under the Privacy Act of 1974 (5 U.S.C. §552a) (Privacy Act) is limited to United States citizens and lawful permanent residents. The President's Executive Order No. 13768, *Enhancing Public Safety in the Interior of the United States (EO 13768)* (January 25, 2017) reiterates that agencies, to the extent consistent with applicable law, will ensure that only PII relating to United States citizens and lawful permanent residents are covered by the protections of the Privacy Act.

The DHS Privacy Policy that implements *EO 13768*[22] makes clear that DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. DHS offers multiple avenues for individuals not covered by the Privacy Act to correct information maintained by DHS.

USCIS ESB is facilitating the transfer of UNHCR information to DHS HART and does not retain the information in its systems. Therefore, USCIS cannot provide individuals with the opportunity to access and correct their information with ESB. U.S. citizens, lawful permanent residents, and individuals who have covered records under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information in DHS HART by submitting a request to:

OBIM Privacy
Department of Homeland Security
245 Murray Drive, SW
Washington, D.C. 20598-0675

Individuals not covered by the Privacy Act or the Judicial Redress Act may access their records by filing a Freedom of Information Act (FOIA) request to the following address:

OBIM FOIA Officer,
Department of Homeland Security,
245 Murray Lane, SW
STOP-0628, Washington, D.C. 20528-0628

---

[22] DHS Memorandum 2017-01: *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 25, 2017) (DHS Privacy Policy), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01. As the DHS Privacy Policy notes, Executive Order 13768, does not affect statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. § 1367. These laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and aliens, regardless of a person's immigration status.

Requests for information are evaluated to ensure that any release of information is lawful, and do not disclose information which would cause a clearly unwarranted invasion of personal privacy or that would disclose techniques and/or procedures for law enforcement investigations or prosecutions.

If an individual is dissatisfied with the response to his or her redress inquiry, then he or she can appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted at Chief Privacy Officer, Attn: DHS Privacy Office, Department of Homeland Security, Mailstop 0655, 245 Murray Lane, SW, Washington, D.C. 20528; or by fax: 1-202-343-4010. As with access, amendments may be limited pursuant to applicable Privacy Act exemptions asserted by the Department of Homeland Security for IDENT/HART.

Privacy Risk: There is a risk that a refugee applicant may not be aware that information collected directly from him or her may be stored in IDENT/HART and shared with other IDENT/HART users.

Mitigation: DHS cannot fully mitigate this risk because DHS is not the original collector of the information and therefore not involved in the initial notification to the individual. As part of the referral process, UNHCR may inform individuals seeking refugee resettlement that it may share their data with other USRAP entities for the refugee resettlement process. To partially mitigate this risk, DHS is publishing this PIA to inform individuals that DHS maintains information originally collected by UNHCR in IDENT/HART for identity verification purposes, as well as national security and law enforcement purposes. The information maintained by IDENT/HART is used to perform identity verification during subsequent interviews and encounters with the individual. DHS provides DOJ, DOD, DOS, and other agencies tasked with national security and counterterrorism responsibilities to the refugee information maintained in IDENT/HART. The MOU stipulates that DHS is to not share any personal data collected by UNHCR except for encounter data, which may be shared with DOJ, DOD, DOS, and other U.S. Government agencies tasked with national security and counterterrorism responsibilities. Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. DHS may only share encounter data with these external entities when the biometrics shared by UNHCR matches data held on individuals known to DHS form whom there is derogatory information.

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.

Section 207 of the Immigration and Nationality Act (INA) as amended provides the legal authority for refugee admissions to the United States. The biometrics from UNHCR are used to help establish an initial identity that allows USCIS to later biometrically verify that the individual being processed by USCIS overseas for refugee resettlement is the same individual who was registered and referred by UNHCR, thus increasing efficiencies in the refugee resettlement process. It will assist USCIS to prepare for and inform the interview process, and to screen and vet the referred individual. This allows USCIS to check IDENT/HART for previous encounters and identities that might contain derogatory information on an individual. Many refugees live for long periods in asylum countries and the use of biometrics helps ensure that there is unbroken continuity of identity over time and between different locations. Where resettlement is pursued, biometric verification helps provide assurance of identity through all the steps of the process. The information shared by UNHCR and enrolled in IDENT/HART will be available to other DHS Components and external entities besides USCIS to use for purposes that align with the purposes mentioned in the MOU.

Privacy Risk: There is a risk that the UNHCR data will be used by DHS and other entities for purposes other than those stated in the MOU.

Mitigation: This risk is partially mitigated. Initially, only USCIS will have access to this data in IDENT/HART and will use it to verify that the individual USCIS is interviewing as part of the refugee resettlement process is the same individual that UNHCR referred to the United States. Once the individual's identity has been verified during the USCIS interview, the data will become a part of the individual's encounter history and will be available to other DHS Components as permitted by the MOU. In addition, when a biometric matches with one in the Terrorist Screening Center's (TSC) system, the Terrorist Screening Database,[23] IDENT/HART will send a message to the TSC informing them of a match. This is done via IDENT/HART's notification service.[24]

DHS has instructed OBIM to configure a robust filtering process in IDENT/HART based on the provisions of the MOU, as discussed above. As an Entity authorized to receive the data through IDENT/HART, DHS is responsible for using the information in an authorized manner.[25]

---

[23] For more information, please *see* DHS-ALL-PIA-027 Watchlist Service, *available at* www.dhs.gov/privacy.
[24] *See* https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf.
[25] The Homeland Advance Recognition Technology (*HART*) system will be replacing IDENT. *See forthcoming* HART Increment 1 PIA, *available at* www.dhs.gov/privacy.

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).

DHS seeks to minimize the collection and retention of biographic and biometric data of individuals seeking refugee resettlement to that which is necessary and relevant to biometrically verify that the individual being processed by USCIS overseas for refugee resettlement is the same individual who was registered and referred by UNHCR, as well as identify any incident of potential identity fraud. The MOU between DHS and UNHCR states that DHS will retain personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this agreement; and that UNHCR will ensure that inaccurate personal data is brought to the attention of DHS in order for appropriate corrective action to be taken in a timely manner. The records schedule requires DHS to maintain IDENT records in its custody for 75 years or when no longer needed for legal or business purposes, whichever is later (N1-563-08-34).

Privacy Risk: There is a risk that DHS will collect more information than necessary.

Mitigation: This risk is mitigated. For the purposes of this initiative, DHS and UNHCR worked together to ensure that UNHCR sends only the information necessary to support this initiative. DHS and UNHCR have entered into a MOU that outline the agreed upon data elements. DHS only requested data elements that are required to confirm that the individual DHS is interviewing is the individual that UNHCR referred to DHS for resettlement to the United States.

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

Mitigation: This risk is partially mitigated. The MOU stipulates that IDENT/HART will retain the information as outlined in the External Biometric Records SORN[26] and OBIM's current National Archives and Records Management (NARA) retention (DAA-0563-2013-0001).[27] OBIM will submit updates to the retention schedule thereafter to NARA for approval. USCIS will not retain the information in the ESB after retrieval and transmission from UNHCR to IDENT/HART.

---

[26] *See* DHS/ALL-041 External Biometrics Records (EBR) System of Records, 83 FR 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

[27] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

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.

IDENT/HART is the central DHS-wide system for the storage and processing of biometric and associated biographic information for the purposes of national security, law enforcement, immigration and border management, intelligence, and credentialing (e.g., background investigations for national security positions and certain positions of public trust), as well as for providing associated testing, training, management reporting, planning and analysis, or other administrative uses. IDENT/HART receives biometric and biographic data from DHS and external users to conduct biometric searches against IDENT/HART. Through the MOU, UNHCR has indicated the conditions for onward sharing. DHS has instructed OBIM to configure in IDENT/HART a robust filtering process based on the provisions of the MOU, as discussed above. OBIM encodes these data filtering authorizations through Data Access and Security Controls (DASC), which are the system configurations that reflect the permissions of each IDENT/HART authorized user. The information shared by UNHCR and enrolled in IDENT/HART is available to DHS Components and external entities to use for purposes that align with the purposes mentioned in the MOU. USCIS uses the information in IDENT/HART to biometrically verify that the individual being processed by USCIS for refugee resettlement is the same individual who was registered and referred by UNHCR.

Privacy Risk: There is a risk that collected information may be used for a purpose incompatible with the original purpose of collection.

Mitigation: The federal regulations at 8 CFR § 208.6 (a), govern confidentiality of asylum information, and by DHS policy, also govern the general prohibition against disclosing refugee information to third parties. Officers receive highly specialized training related to refugee processing and keep all information collected during refugee processing confidential. Additionally, standard operating procedures and policy guidance ensure that collected information is not used for a purpose incompatible with the original purpose of collection.

Privacy Risk: There is a risk that biometrics and biographics may be shared on individuals with external partners for a purpose that is not compatible with the purpose of the collection.

Mitigation: This risk is partially mitigated. Information related to refugee processing is kept confidential. The federal regulations at 8 CFR § 208.6 (a), govern confidentiality of asylum information, and by DHS policy also govern the general prohibition against disclosing refugee information to third parties. The MOU states that only encounter data, defined as biographic data and facial images can be shared with permitted entities (i.e., DOJ, DOS, DoD, and other entities with national security and counterterrorism responsibilities) only when derogatory information is

identified . OBIM has ensured that IDENT/HART has configured strong filtering mechanisms that incorporates UNHCR's data access permissions. Biographic data and facial images are shared with permitted entities. The inherent risks of biometric-based matching in IDENT/HART and sharing are documented in the forthcoming HART Increment 1 PIA. OBIM also maintains a log of all data transmitted and received, so these can be checked periodically to ensure that the sharing is taking place as envisioned.

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.

DHS and UNHCR entered into a MOU to preserve the integrity of USRAP. UNHCR is sharing biometric data along with associated biographic data of applicants upon referral to the United States for resettlement. This data will establish an initial identity that allows USCIS and other DHS Components to later biometrically verify, as well as identify any incident of potential identity fraud, that the individual being processed by USCIS overseas for refugee resettlement is the same individual who was registered and referred by UNHCR. Biometric verification helps guard against substitution or identity fraud in resettlement processes.

Privacy Risk: A risk exists that UNHCR will not inform DHS that data it provided was inaccurate.

Mitigation: This risk is partially mitigated. The DHS and UNHCR MOU stipulates that UNHCR intends to provide accurate, complete, and up-to-date data. In addition, it also states that UNHCR will promptly notify DHS of any data errors/inaccuracies that it discovers and take appropriate action on any requests from DHS for access, changes/additions, deletions, and corrections to the personally identifiable information. Ultimately, DHS cannot control the quality or accuracy of the data since UNHCR is the data provider.

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.

The MOU requires the Parties to ensure that the necessary technical and organizational measures are used to protect PII against accidental or unlawful destruction, accidental loss, unauthorized disclosure, alteration, access, or any unauthorized processing of the data. OBIM's strict access controls and system administrators for IDENT/HART ensure that only authorized

users with an operational need to know will have access to data.[28] Any recorded data, video, or still images that are saved to be used as evidence will be handled in accordance with DHS policy and as outlined in this PIA.

Privacy Risk: There is a risk that the transmission of data between UNHCR and DHS will be intercepted by a third party.

Mitigation: USCIS facilitates the data transfer between UNHCR and IDENT/HART via the ESB. The DHS/USCIS/PIA-008 ESB2 PIA covers this interconnection. As noted in the DHS/USCIS/PIA-008 ESB2, the data delivered by the ESB is protected by numerous security controls. ESB's security controls ensure that the data from UNHCR remains intact from when it is first queried from the original underlying source system until it is delivered to the consuming application or end user. The primary method of this control is the use of secure socket layer (SSL) processing between all components that do not reside on the same physical machine. SSL processing ensures that data may not be altered during communications. The SSL mechanisms involved are all Federal Information Processing Standard 140-2 compliant per DHS policy.[29]

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.

DHS ensures that practices stated in this PIA comply with internal DHS policies, including the DHS privacy policies, standard operating procedures, orientation and training, rules of behavior, and auditing and accountability. DHS and UNHCR have been indirectly sharing biographic information during the refugee resettlement process for many years. The *MOU between DHS and UNHCR for Refugees on the Sharing of Personal Data* expands that information sharing to include biometrics. All DHS employees and contractors receive annual privacy and security training to ensure their understanding of properly handling and securing PII, which includes biometrics as well as biographic information. DHS USCIS officers receive highly specialized training related to refugee processing and keep all information collected during refugee processing confidential. Additionally, standard operating procedures and policy guidance ensure that collected information is not used for a purpose incompatible with the original purpose of collection.

---

[28] The Homeland Advance Recognition Technology (*HART*) system will be replacing IDENT. *See forthcoming* HART Increment 1 PIA, *available at* www.dhs.gov/privacy.
[29] *See* https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards.

Conclusion

The DHS and UNHCR automated information sharing will assist DHS with biometrically verifying the identity of the individual in an effort to combat fraud and preserve the integrity of USRAP. DHS has implemented proper access controls, procedures, and protocols to ensure that the biographic and biometric data are properly handled and that proper protections and safeguards are in place to protect PII.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services

Approval Signature

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

_____

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