Privacy Impact Assessment

for the

Homeland Advanced Recognition Technology System (HART)

DHS Reference No. DHS/OBIM/PIA-004(a)

August 14, 2024

Homeland Security

Abstract

When it reaches operational capability, the Homeland Advanced Recognition Technology (HART) will replace the legacy Automated Biometric Identification System (IDENT) as the primary U.S. Department of Homeland Security (DHS) system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, development of new technologies, and other administrative use.

While HART is not yet operational, the Department is issuing this Privacy Impact Assessment (PIA) update to (1) enhance transparency about the anticipated categories of individuals whose data will be stored in HART (foreign nationals and U.S. citizens); (2) broadly describe HART's anticipated users and information sharing partners and identify new HART information sharing partners; (3) describe how the HART system is now expected to be developed —HART no longer has four increments as previously envisioned—HART will consist of Increment 1 and Future Capabilities; and (4) clarify that DHS Components may use certain other DHS Component collected fingerprints maintained in HART to query foreign partners with which it has an Information Sharing and Access Agreement (ISAA), consistent with DHS policy, and under broader DHS authorities or its own authorities.

Overview

The legacy Immigration and Naturalization Service (INS) developed IDENT in 1994 as a law enforcement system for collecting and processing biometric data from individuals apprehended by border security or immigration officials. After its creation in 2003, DHS established the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program as the first large-scale biometric identification program to support immigration and border management. In 2013, US-VISIT transitioned to become the Office of Biometric Identity Management (OBIM).[1] In 2015, OBIM began planning to replace IDENT with HART, a more advanced system that is expected to provide OBIM with more efficient biometric data to support DHS core missions.

OBIM's mission is to provide identity services to DHS and its mission partners that enable informed decision making by producing accurate, timely, and high assurance biometric identity

[1] *See* Public Law 113-6, Homeland Security Appropriations Act, Public Law 115-31, Div. F., Section 301. *See* also 8 U.S.C. § 1379(1), which provides authority to match biometric information by requiring the use of biometric data for conducting background and identity checks; 8 U.S.C. § 1365b(f), which provides authority to store biometric information by requiring the Secretary to make procedures for "additions" to the entry and exit data system; 8 U.S.C. § 1365a(f), which provides authority to share biometric information by allowing access to government personnel.

information. OBIM's mission partners include internal DHS Components, other federal government agencies, and international partners. OBIM's partners capture biometric data and will submit it to HART to carry out their missions and functions, including law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, background investigations relating to national security positions, and credentialing consistent with applicable DHS authorities. DHS also maintains this information to support its Information Sharing and Access Agreements and arrangements with foreign partners. Such sharing augments the law enforcement and border control efforts of both the United States and its partners. Additionally, DHS uses this information in concert with external partners to facilitate the screening of refugees, visa applicants, and other immigrants to combat terrorist travel consistent with DHS and Component authorities.

HART, IDENT's replacement system, is a centralized DHS-wide biometric database that will also contain limited biographic and encounter history information needed to place the biometric information in proper context. Like IDENT, the information to be maintained in HART is collected by, on behalf of, in support of, or in cooperation with DHS and its Components, consistent with applicable laws, rules, regulations, and Information Sharing and Access Agreements. OBIM and the DHS Office of Strategy, Policy, and Plans (PLCY), in collaboration with Component data owners, facilitate biometrics-based Information Sharing and Access Agreements with external partners. OBIM is the system owner and the data steward for IDENT, and the successor HART system. HART will store and process biometric data (e.g., digital fingerprints, iris scans, and face images (including photographs)), and link the biometric data to biographic information pursuant to the data owner's authorities and policies for use, retention, and information sharing.

Migration from IDENT to HART will be performed to minimize impact to OBIM's mission partners' operations. The migration will occur without unscheduled interruption of service delivery to OBIM's mission partners, with minimal scheduled service outages, and without degradation in service levels (response time) to those partners. Once OBIM completes HART development and technical configurations, HART will replace IDENT as the biometric system of record. Pending any development or program changes, OBIM anticipates that this will occur in Fiscal Year 2026.

Reason for the Privacy Impact Assessment Update

In February 2020, DHS published the original HART Privacy Impact Assessment[2] to assess and mitigate any potential privacy risks associated with the then-anticipated four-phased

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVACNED RECOGNITION

incremental development and roll out of HART. Traditionally, Privacy Impact Assessments are completed on finished technologies, systems, programs, operations, and activities that may impact individual privacy. With respect to HART, while not yet developed and implemented, the Department anticipated potential privacy risks associated with the privacy sensitive system and sought to proactively develop appropriate privacy safeguards to be implemented throughout its development. Unfortunately, while a novel, forward looking approach, the resulting Privacy Impact Assessment inadvertently caused confusion regarding the forward-looking nature of the Assessment and corresponding safeguards. Accordingly, this Privacy Impact Assessment update is being published to clarify and address points raised by external oversight bodies and accomplish the following:

1. enhance transparency about the categories of individuals' information whose data is anticipated to be stored in HART;
2. broadly describe HART's anticipated users and information sharing partners and identify new HART information sharing partners;
3. clarify and further describe how the HART system is expected to be developed; and
4. clarify that a DHS Component may use certain other DHS Component collected fingerprints maintained in HART to query foreign partners with which it has an Information Sharing and Access Agreement, under broader DHS authorities or its own authorities.

DHS will issue an updated Privacy Impact Assessment for HART when it is fully developed and before it is operational.

Categories of Individuals to be in HART

HART will contain information collected by DHS Components, as well as other domestic and foreign mission partners. HART will contain personally identifiable information, including biometric data and associated biographic information, on U.S. citizens, lawful permanent residents, and foreign nationals.

DHS Mission Partners that will be HART Users or Information Sharing Partners

DHS mission partners will provide biometric and associated biographic information from individuals from whom they collect information to HART. HART, in turn, may also share information with these partners.

DHS HART users are expected to include DHS Components and Offices: U.S. Citizenship and Immigration Services (USCIS), U.S. Coast Guard (USCG), U.S. Customs and Border

TECHNOLOGY (HART), DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Secret Service (USSS), DHS Office of the Chief Security Officer (OCSO), Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), and the Office of Strategy, Policy, and Plans (PLCY); external domestic partners: Department of State (DOS), Department of Justice (DOJ), Department of Defense (DOD), Office of Personnel Management (OPM), and elements of the Intelligence Community (IC); and state, local, tribal, and territorial law enforcement agencies.

International users of HART anticipated to provide data to and use data maintained in HART are expected to include foreign governments such as Canada, the United Kingdom, Australia, New Zealand, Mexico, and Greece. Since the last HART Privacy Impact Assessment in February 2020, HART has added the following expected foreign partners: Bulgaria, Croatia, Guatemala, and Panama. International users of HART will also include international organizations such as the UN High Commissioner for Refugees (UNHCR), also known as the UN Refugee Agency.

Use of DHS Component Fingerprints to Query Foreign Partners

Under DHS Policy Statement 262-173, DHS Components may use fingerprints collected by another DHS Component and maintained in IDENT (eventually to be transitioned to HART) to initiate queries of a foreign partner's biometric holdings. This policy authorizes Components that lack their own fingerprint collections in individual cases to disclose certain fingerprints collected by other Components to initiate information requests under the International Biometric Information Sharing Program (IBIS), in accordance with the terms of applicable agreements and arrangements and to the extent permitted by, and consistent with, those Components' authorities and any restrictions imposed by statute, executive order, or other directive or policy.[4] Information obtained through the International Biometric Information Sharing Program is now maintained in IDENT, eventually to be maintained in HART.

HART Development

HART is now expected to consist of Increment 1 and Future Capabilities. Increment 1 is expected to include the core foundational infrastructure necessary to operate HART and fully

[3] DHS Policy Statement 262-173 authorizes any DHS Component participating in the International Biometric Information Sharing Program to use certain categories of fingerprints, submitted to or collected by another DHS Component, to initiate a fingerprint-based query against a foreign government's biometric holdings under the conditions outlined in the Policy. This authority is provided on the condition that such queries are made pursuant to, and consistent with, the terms of formal information sharing agreements or arrangements that exist with foreign governments and conform to the purposes of the International Biometric Information Sharing Program, when there is an official need to conduct a query consistent with the requirements outlined in the Policy.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTERNATIONAL BIOMETRIC INFORMATION SHARING PROGRAM (IBIS), DHS/ALL/PIA-095 (2022), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

replace IDENT. Future Capabilities may be developed after the HART Program reaches Initial Operational Capability (IOC) and consist of technical and functional enhancements to the system that will be prioritized and executed at the direction of the HART lead business authority, as operational needs arise.

HART Increment 1

Initial HART system capabilities will be developed in Increment 1. The scope of Increment 1 is limited to development work, which includes the core foundational infrastructure necessary to operate HART and fully replace IDENT. This structure will consist of the system infrastructure, database re-architecture, business workflow, business rules management capabilities, biometric middleware, data management, additional biometric capabilities, and baseline (existing IDENT) system functionality. Increment 1 is required to establish the framework and system architecture, system components, and baseline system functionality. Increment 1 will include production-scaled fingerprint, latent fingerprint, iris, and face biometric modalities as well as the completion of the full Performance Test Environment (PTE). Once HART Increment 1 capabilities are fully developed and tested, the HART system will be delivered as a single unit and is expected to become the Department's biometric system of record, supporting the decommissioning of IDENT.

At HART Program Initial Operational Capability, HART will replace the legacy IDENT system with a modular application. HART is expected to provide business workflow and business rules management, an interface to biometric matching services, feature an authentication and authorization web service, and fully integrate with DHS enterprise system security. HART is also expected to have a modular biometric matching subsystem interface architecture that will enable the application to communicate with multiple biometric matching subsystems concurrently and that isolates the transaction and business processing components of HART from the internal details of individual biometric matching subsystems.

HART Future Capabilities

Once HART Program Initial Operational Capability is achieved, HART Future Capabilities will be assessed, developed, and delivered. At this time, Future Capabilities are comprised of the post-Increment 1 technical and functional enhancements to the system which will be prioritized and executed at the direction of the HART lead business authority as operational needs arise. In addition to operational capabilities, HART would then undergo technical updates and expansion, necessary to meet operational and capacity requirements. HART Future Capabilities and their prioritization will be periodically reviewed and adjusted based on evolving needs and requirements. The prioritization of capabilities may be impacted by such factors as cost, OBIM and customer priorities, and Department-wide initiatives. Some of the capabilities may be identified for accelerated development or potentially revised or even descoped. The lead business authority will provide direction for prioritization of the capabilities based on evolving operational

and legislative priorities.

Privacy Impact Analysis

Authorities and Other Requirements

There are no changes to OBIM's statutory and other authorities pertaining to the establishment and mission of the OBIM program for the operation and maintenance of HART. The IDENT System of Record Notice (SORN)[5] and DHS Component System of Records Notices and Information Sharing and Access Agreements govern the function and use of the biometric records collected by each Component. As a result, OBIM coordinates with DHS Components on privacy compliance documentation that details how information is collected, used, shared, retained, and disposed.

The DHS/ALL-041 External Biometric Records (EBR) System of Records Notice[6] governs the maintenance and use of biometric and associated biographic information from non-DHS entities (not already covered by a DHS Component System of Records Notice), both foreign and domestic, for the following purposes pursuant to formal or informal information sharing agreements or arrangements ("external information"), or with the express approval of the entity from which the Department received biometric and associated biographic information: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. Additionally, the DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records Notice[7] covers DHS' collection and maintenance of administrative and technical records associated with IDENT and its successor information technology system, HART.

The HART Security Plan is completed. HART has an active Authority to Operate. The National Archives and Records Administration (NARA) approved a records schedule that requires OBIM to maintain HART records in its custody for the retention periods outlined in the Biometric with Limited Biographic Schedule (DAA-0563-2013-0001). There is no update regarding the *Paperwork Reduction Act* information discussed in the 2020 HART Privacy Impact Assessment. All information stored in HART is collected by HART data providers and stored under the data provider agency's regulatory notices and authorities.

---

[5] *See* DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT), 72 Fed. Reg. 31080, (June 5, 2007), *available at* https://www.dhs.gov/system-records-notices-sorns.
[6] *See* DHS/ALL-041 External Biometric Records (EBR), 83 Fed. Reg. 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[7] *See* DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR), 85 Fed. Reg. 14955 (March 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

Characterization of the Information

While there is no change in the type of information that is expected to be maintained in HART, DHS is publishing this Privacy Impact Assessment update to clarify the categories of individuals whose data may be maintained in the system. HART maintains biometric and associated biographic information on U.S. citizens, lawful permanent residents, and foreign citizens, initially collected by DHS and non-DHS entities.

As discussed in the 2020 HART Privacy Impact Assessment, a record stored in HART may contain the following data elements:

- Biometric data, including face images, fingerprints, and iris images;
- Biographic data associated with the biometric data including full name (i.e., first, middle, last, nicknames, and aliases); date of birth; gender; personal physical details (e.g., height, weight, eye color, and hair color); signature; assigned number identifiers (e.g., A-Number, Z-number, Social Security number; state identification number; civil record number; other agency system-specific fingerprint record locator information, Federal Bureau of Investigation (FBI) Number (FNU)/Universal Control Number (UCN), Encounter Identification Number (EID), DOD Biometric Identifier (DOD BID), National Unique Identification Number (NUIN); document information and identifiers (e.g., passport and visa data, document type, document number, country of issuance, when available); and identifiers for citizenship and nationality, including person-centric details (e.g., country of birth, country of citizenship, and nationality);
- Derogatory Information may consist of wants and warrants, known or suspected terrorist (KST) designation, sexual offender registration, foreign criminal convictions, and immigration violations. Specifically, the data include derogatory information relevant to: KSTs, wanted persons, convicted sex offenders, State and local convicted criminals flagged by State/local law enforcement from the FBI; subjects who have violated U.S. immigration laws or who have been denied a biometric visa by DOS; individuals encountered by the DOD during military operations; international criminal data provided by INTERPOL, DOD, FBI, and our international partners; noncitizens with criminal history, known or suspected gang members, enforcement actions taken at CBP Ports of Entry; expedited U.S. Immigration and Customs Enforcement (ICE) immigration removals; and law enforcement community alerts;
- Miscellaneous officer comment information;
- Encounter data, including location and circumstance of each instance resulting in biometric collection; and
- Unique machine-generated identifiers (e.g., fingerprint identification number (FIN), Encounter Identification Number (EID), and Transaction Control Number (TCN)) that link

individuals with their encounters, biometric data, records, and other data elements. These data elements enable the execution of administrative functions of the biometric repository, such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.

HART data providers will collect the information according to their authorities and mission. Collection methods will include:

- Directly from the individual according to the data providers' authorities and mission. This could include biometric data collected from individuals while applying for a credential, through opt-in enrollments (e.g., Global Entry and TSA PreCheck®), an immigration benefit, or pursuant to a background investigation, at ports of entry, or at the borders;
- Via military and law enforcement direct encounters or forensic operations according to the data providers' authority; or
- Through records shared by foreign governments according to written agreements or cooperative arrangements.

External DHS data providers include DOS, DOJ, DOD, OPM, other federal, state, local, tribal, territorial law enforcement, foreign governments, and international agencies. Foreign government data providers include Five Eyes/Migration Five Partners, namely Australia, Canada, New Zealand, and United Kingdom; certain Visa Waiver Program (VWP) countries like Bulgaria, Croatia, Greece, and Italy under Protecting and Combatting Serious Crime Agreements; and other allied nations providing information pursuant to an agreement or arrangement, including Guatemala, Honduras, Mexico, and Panama. A complete list of data providers and users will be included in the HART Privacy Impact Assessment update to be issued when HART is completed and ready to use operationally. International agency information can include biometric data collected by the UN High Commission for Refugees for refugees who are referred to the United States for resettlement.

DHS data provider sources include CBP, ICE, USCG, USCIS, TSA, FEMA, and the DHS OCSO. For example:

- The USCG interdicts and refers for prosecution undocumented migrants and suspected migrant smugglers off the coast of the United States;
- USCIS may collect information to establish and verify the identities of individuals applying and being adjudicated for immigration benefits, including asylum or refugee status;
- TSA collects information to support the vetting and adjudication of its current credentialing populations, which may include workers seeking access to secure facilities and individuals applying for trusted traveler programs, such as TSA PreCheck®.

Each DHS data provider is responsible for documenting its own data collections in its respective System of Records Notice and Privacy Impact Assessment. The data may be collected by HART data providers through an online application, a paper-based application, a mobile biometric device, a fixed platform, or in-person interviews. Latent prints may be manually collected at a crime scene or another site relevant to the work of a HART user, such as the site of a terrorist incident. The data will then be securely transmitted to HART and accessed by mission need.

There are no updates on how the project will use information from commercial sources or publicly available data or on how the accuracy of the data will be ensured, and there are no new risks related to the characterization of the information.

Uses of the Information

There are no new anticipated uses of the information with this Privacy Impact Assessment update.

Notice

HART will not provide individuals notice prior to the collection of information, as OBIM is a service provider and does not collect data directly from individuals. This Privacy Impact Assessment update, the DHS/US-VISIT-004 IDENT Records System of Records Notice, DHS/ALL-041 External Biometric Records System of Records Notice, and DHS/ALL-043 Enterprise Biometric Administrative Records System of Records Notice provide general notice that an individual's personal information may reside in HART. Notice will be provided through the publication of Privacy Impact Assessments and System of Records Notices for the underlying systems of original collection and the information shared from those systems, a list of which will be completed (and updated as needed) when the updated Privacy Impact Assessment is completed upon HART reaching operational capability. If required by law or policy, DHS Components, as well as external partners that submit information to HART and other DHS systems, will provide notice to the individual whose information is collected and retained related to maintenance and retention of information, including whether it is retained in HART, at the point of collection.

DHS/ALL/PIA-095 International Biometric Information Sharing Program (IBIS),[8] published in November 2022, lists HART's anticipated partner countries including Australia, Bulgaria, Canada, Cabo Verde, Croatia, El Salvador, Guatemala, Greece, Honduras, Italy, Israel, Mexico, New Zealand, Panama, Poland, Qatar, and United Kingdom. As noted previously,

[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTERNATIONAL BIOMETRIC INFORMATION SHARING PROGRAM (IBIS) – APPENDIX B, DHS/ALL/PIA-095 (2022), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

information obtained through the International Biometric Information Sharing Program is now maintained in IDENT, eventually to be maintained in HART.

Data Retention by the Project

There is no change to the retention period with this Privacy Impact Assessment update.

Information Sharing

HART's anticipated Users and Information Sharing Partners: As previously mentioned in the 2020 HART Privacy Impact Assessment, OBIM shares information as permitted by data owners and DHS and in accordance with DHS and the data owners' authorities and requirements. Information may be shared with federal agencies; state, local, tribal, and territorial law enforcement agencies; and foreign and international agencies for national security, law enforcement, criminal justice, immigration screening and border management, national defense, and intelligence purposes, as well as to conduct background investigations for national security positions, credentialing, and certain positions of public trust consistent with applicable DHS authorities. These information sharing relationships are documented in Information Sharing and Access Agreements. DHS Component HART users will also address HART sharing in their specific privacy compliance documentation. Federal agencies like DOJ, DOS, and DOD, with which HART is expected to share information, also have their own privacy compliance documentation, policies, and requirements. DHS has biometric interoperability with DOJ and DOD, which means many entities may send queries to HART via DOJ's Next Generation Identification System (NGI)[9] or DOD's Automated Biometric Identification System (ABIS).[10] This includes OPM, which now queries IDENT via the Next Generation Identification System under the terms of the DHS, DOJ, and DOS Interoperability Memorandum of Understanding (2008). Many other federal, state, local, and territorial agencies may also exchange information with HART through DOJ and DOD interoperability.

International Sharing – Querying foreign partners' databases with fingerprints collected by a different DHS Component: Since the publication of the 2020 HART Privacy Impact Assessment, DHS published the DHS/ALL/PIA-095 International Biometric Information Sharing Program (IBIS) Privacy Impact Assessment and subsequent updates. This Privacy Impact Assessment series describes the International Biometric Information Sharing Program, which enhances cooperation between DHS Components and foreign partners in assessing the eligibility or public security risk

[9] *See* U.S. DEPARTMENT OF HOMELAND JUSTICE, FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE NEXT GENERATION IDENTIFICATION SYSTEM (NGI), *available at* https://www.fbi.gov/file-repository/pia-next-generation-identification-biometric-interoperability.pdf/view.

[10] *See* A0025-2 PMG (DFBA) DoD - Defense Biometric Identification Records System, 80 Fed. Reg. 8292 (Feb. 17, 2015), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/581425/a0025-2-pmg-dfba-DoD/. *See* A0025-2 SAIS DoD - Defense Biometric Services, 74 Fed. Reg. 48237 (Sept. 22, 2009), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569938/a0025-2-sais-DoD/.

of individuals seeking an immigration benefit or encountered at the border (or its functional equivalent) or during a law enforcement investigation related to immigration or border security. Appendix B of the original International Biometric Information Sharing Privacy Impact Assessment lists the countries with which DHS exchanges information. That Privacy Impact Assessment, and its updates, provide enhanced transparency on DHS sharing and use of biometric and associated biographic data with foreign partners. After DHS concludes an appropriate information sharing agreement or arrangement that includes privacy safeguards, foreign partners' records can be vetted or compared against information held in IDENT or, eventually, HART. DHS Components may share information with foreign partners as authorized by broader DHS authorities and policies, pursuant to their own authorities. As noted previously, information obtained through the International Biometric Information Sharing Program is now maintained in IDENT, eventually to be maintained in HART.

Privacy Risk: There is a risk that individuals may not know that non-DHS entities/agencies may exchange information on them, and that information may be maintained in and processed by HART.

Mitigation: This risk is mitigated. In many instances, the biometric and biographic information to be maintained in and processed by HART is collected directly from the individual, so the individual knows their fingerprints are being captured at the time of collection. HART data providers who collect this information, such as DOD, DOJ, and DOS, may provide notice through publication of their own Privacy Impact Assessments and by other methods. OBIM also provides notice through publication of this Privacy Impact Assessment. DHS/NPPD/PIA-002 IDENT and DHS/ALL/PIA-095 International Biometric Information Sharing (IBIS), and subsequent updates, list additional non-DHS entities/agencies and foreign partners that are expected to exchange data with HART. The DHS/ALL/PIA-077 Biometric Interoperability Privacy Impact Assessment between DHS and DOJ, and subsequent updates, describe how DOJ and authorized users exchange information with IDENT (eventually HART). As part of the Biometric Interoperability Agreement between DHS and DOJ, users of DOJ/FBI's Next Generation Identification System[11] will also have access to and may query HART, including federal, state, and local law enforcement users.

Redress

In addition to the original HART Privacy Impact Assessment, the DHS/ALL/PIA-095 International Biometric Information Sharing (IBIS) Privacy Impact Assessment and updates, published in 2022 and 2024, include information related to redress as it relates to biometric and biographic information sharing with foreign partners. As noted previously, information obtained

[11] *See* U.S. DEPARTMENT OF HOMELAND JUSTICE, FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE NEXT GENERATION IDENTIFICATION SYSTEM (NGI), *available at* https://www.fbi.gov/file-repository/pia-next-generation-identification-biometric-interoperability.pdf/view.

through the International Biometric Information Sharing Program is now maintained in IDENT, eventually to be maintained in HART.

Privacy Risk: There is a risk that individuals may not be able to correct inaccurate or erroneous information about themselves eventually maintained in HART.

Mitigation: This risk is fully mitigated. U.S. Persons (i.e., U.S. citizens and lawful permanent residents) may file a Privacy Act request to access or amend their information. In addition, U.S. Persons who are travelers and have experienced difficulty while traveling may use the DHS Traveler Redress Inquiry Program (DHS TRIP)[12] to pursue redress requests. Moreover, any individual may request access to or correction of their personally identifiable information (PII) regardless of nationality or country of residence through TRIP. This process is described in the TRIP Privacy Impact Assessment and information is available on the DHS public website. Redress requests that come to TRIP in which a traveler encountered difficulties at the point of entry due to information maintained in HART that needs to be modified or updated will be assigned via TRIP to OBIM. OBIM will then take appropriate actions to the HART record, if warranted, and make that notation in TRIP.

Alternatively, any person may submit a request to have any record maintained by OBIM and/or in an OBIM system corrected by contacting OBIM Privacy, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, D.C. 20598-0675.

Further, U.S. citizens, lawful permanent residents, and covered individuals covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. Additionally, all individuals, regardless of citizenship, may request access to records consistent with the Freedom of Information Act (FOIA) unless disclosure is subject to a statutory exemption. Requesters may indicate the biometric modality for the basis of the search. Individuals may submit a FOIA request to: The Privacy Office, Office of Biometric Identity Management, U.S. Department of Homeland Security, 245 Murray Lane SW, STOP-0655, Washington, D.C. 20528-0655, or online at https://www.dhs.gov/foia-contact-information.

Auditing and Accountability

There are no updates to Auditing and Accountability because of this update. However, OBIM and the DHS Privacy Office are working to address the 13 privacy recommendations in the 2020 HART Privacy Impact Assessment. In addition, in the Privacy Office is working to complete the Privacy Compliance Review (PCR) noted in the 2020 HART Privacy Impact Assessment.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM (TRIP), DHS/ALL/PIA-002 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

Contact Official

Craig Kelly
Branch Chief, Privacy and Policy
Office of Biometric Identity Management
DHS Management Directorate
obim_icmd_privacy_and_policy@hq.dhs.gov

Responsible Official

Shonnie R. Lyon
Director
Office of Biometric Identity Management
DHS Management Directorate

Approval Signature

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

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy@hq.dhs.gov