Privacy Impact Assessment
for the

Homeland Advanced Recognition Technology System (HART) Increment 1 PIA

DHS/OBIM/PIA-004

February 24, 2020

Contact Point
Shonnie R. Lyon
Director
Office of Biometric Identity Management
DHS Management Directorate
(202) 298-5200

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

Abstract

The Homeland Advanced Recognition Technology System (HART) replaces the legacy Automated Biometric Identification System (IDENT) as the primary 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 uses. The Office of Biometric Identity Management (OBIM) will implement HART in 4 incremental phases. This Privacy Impact Assessment (PIA) only focuses on Increment 1. OBIM will publish an update to this PIA prior to the release of each Increment.

Overview

The legacy Immigration and Naturalization Service (INS) developed IDENT in 1994 as a law enforcement system for collecting and processing biometrics from individuals apprehended by border security or immigration officials. In 2004, after the creation of the Department of Homeland Security, 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 OBIM.[1] In 2015, OBIM began planning for the replacement of IDENT with the HART, a more robust system that will provide OBIM with flexible and more efficient biometric data that supports 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 information. OBIM's mission partners include internal DHS Components, other Federal Government agencies, and international partners. OBIM's mission partners capture biometric data and submit it to HART in order to carry out the 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 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 is using this information in concert with

[1] *See* Public Law 113-6, Homeland Security Appropriations Act, Public Law 115-31, Div. F., Section 301. *See also* see 8 U.S.C. § 1379(1), which provides authority to match biometric information by requiring the use of biometrics 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.

external partners to facilitate the screening of refugees in an effort to combat terrorist travel consistent with DHS's and Components' authorities.

HART, IDENT's replacement IT system, is a centralized DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context. The information 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 access agreements (ISAA). OBIM and the DHS Office of Strategy, Policy, and Plans (PLCY), in collaboration with the Component data owner facilitate HART-based DHS ISAAs with external partners.[2] OBIM is the system owner and the data steward for IDENT, and for the successor HART system. Once OBIM completes HART development and technical configurations, HART will replace IDENT as the biometric system of record. HART will store and process biometric data (digital fingerprints, iris scans, facial images (including a photo)[3]) and link these biometrics with biographic information pursuant to the data owner's authorities and policies for use, retention, and sharing of information. Deoxyribonucleic acid (DNA) retention is not included in Increment 1.

The migration from IDENT to HART operations occurs in phases to minimize impact to OBIM's mission partners. 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 (FY) 2020.

HART Features and Capabilities

HART will provide mission partners with accurate and timely biometric-based identity services that advance informed decision making. OBIM will deploy this replacement system in four incremental phases in order to enhance security and privacy protections, augment interoperability, reduce unsustainable costs, and improve performance and availability. OBIM will provide an updated PIA that describes any new features and capabilities prior to the launch of each Increment.

[2] An ISAA may include a Memorandum of Agreement (MOA), a Memorandum of Understanding (MOU), an Implementing Arrangement, or other formal document.
[3] A facial image may include a photo or video capture that can be used for biometric matching purposes. OBIM is currently working with the National Institute of Technology (NIST) to develop a facial image quality capture standard.

Increment 1

HART Increment 1 development is focused on delivering the core foundational infrastructure and baseline existing functionality in IDENT that ensures continuity of services without disruption to existing IDENT users. HART Increment 1 implements a new data architecture, which includes conceptual, logical, and physical data models, a data management plan, and physical storage of records where each associated record may have multiple associated biometric modality[4] images. HART Increment 1 will include migration to the Amazon Web Services (AWS) GovCloud, and will provide mission partners a biometric matching capability based on multiple biometric modalities (fingerprint (including latent prints), face (including a photo), and iris), and additional means by which to identify an individual such as a unique identifier (e.g., Social Security number (SSN), Alien Number (A-Number)). The data and system architecture have been designed for scalability to address projected growth in identity and image data volumes and to accommodate any needs associated with larger files.[5] HART Increment 1 includes OBIM's design and acquisition of the physical infrastructure for HART. HART Increment 1 will also include existing internal reporting functionality needed to provide reports to our users, monitor redress requests, and support administrative tasks.[6]

Future Increments

Increment 2 will provide additional biometric capabilities to HART to meet customer needs and provide increased interoperability with agency partners and improved reporting features. Increments 3 and 4 will include a web portal and user interface capability, support for additional modalities, and improved reporting tools. OBIM will provide an updated PIA that describes any new features and capabilities prior to the launch of each Increment.

Amazon Web Services (AWS)

HART is housed in the FedRAMP-approved AWS GovCloud environment, at a high confidentiality that allows OBIM to host PII.[7] All existing records will be extracted from the legacy database (IDENT) using a database backup and recovery tool and transferred to the AWS GovCloud environment hosting HART. The migration from IDENT to HART operations occurs in phases to minimize impact to OBIM stakeholders. Under oversight from DHS Security teams,

[4] A biometric modality, for example, face, fingerprint, and iris, is "any measurable biological or behavioral characteristic". *See* biometric modality definition *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf.
[5] Retaining multiple modalities will result in the need for additional storage capacity to accommodate the larger file types. For example, face photos may have larger files size.
[6] OBIM's administrative and reporting functions including information sharing coordination and reporting to provide information in response to queries from external agencies and foreign data providers charged with national security, law enforcement, immigration, or other DHS mission-related functions; provide information in response to redress inquiries and HART user requests; and provide internal reporting and other administrative tasks to OBIM.
[7] *See* additional FedRAMP information *available at* https://aws.amazon.com/compliance/fedramp/.

OBIM will load data and transfer secure encrypted data to the FedRAMP-approved AWS GovCloud environment. Housing HART in the AWS GovCloud environment increases security against cyber threats, improves control over identity and access management, and enables more control over network and firewall configurations.

AWS is a multi-tenant public cloud designed to meet a wide range of regulatory requirements, including Government compliance and security requirements.[8] FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. The cloud service provider selected for this initiative is required to adhere to the security and privacy controls required by the National Institute of Technology (NIST) Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing,"[9] and the DHS Chief Information Officer.

HART Users and Data Providers

OBIM's mission partners include internal DHS Components, other Federal Government agencies, and international partners. OBIM's partners are considered authorized users and data providers. All HART authorized users may query HART. HART authorized users that also upload and store biometric information in HART are called "data providers." Data providers own the data contained in HART. HART authorized users that do not store biometric information have "search only" access, meaning they can search HART pursuant to their mission needs, but do not enroll (or maintain) data in HART. Not all data providers are authorized users. In certain instances, data providers that are not authorized users have provided historical data such as gang affiliations. HART authorized users are U.S. Federal Government, foreign, or international governmental agencies, as well as state, local, tribal, and territorial law enforcement agencies that have entered into ISAAs with DHS for biometric identification and analysis services. DHS Component HART authorized users memorialize the technical security and data transfer specifications through technical and operational documents. Transparency into information sharing programs, including any associated privacy risks and mitigations, may be found in an authorized user's PIA.

HART has two settings for submission of data:[10]

- *Search and Enroll:* When a HART data provider initially enrolls an individual's fingerprint and basic biographic information, HART creates a Fingerprint Identification Number (FIN) for that individual. The user as data provider provides data to conduct a HART search, and if there is no match, the encounter is enrolled as a new HART identity and new FIN assigned. If the search

[8] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[9] *See* additional information *available at* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.
[10] HART users can also search HART but that does not entail contributing data via the search and enroll or the search and assign functions.

matches an existing identity the encounter is added to the FIN.[11] For HART Increment 1, search and enroll is for fingerprints only and does not include face or iris.

- *Search and Assign:* The data provider provides data to conduct a HART search. If there is a match, the encounter is added to the matching FIN. If there is no match, HART will not save the inbound encounter.

OBIM *does not* own the biometrics or biographic data in HART. OBIM owns unique numbers or sequence of numbers and characters, also known as enumerators, that HART generates to link individuals with encounters, biometrics, records, and other data elements. These enumerators are used for OBIM's execution of administrative functions of HART such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.

Data providers determine with which HART authorized users their data may be shared or may not be shared through data provider rules. These data sharing rules are defined in ISAAs, privacy compliance documents, and by DHS policy. Within the HART system, the data sharing rules are called data configuration rules. HART data providers include:

- U.S. Customs and Border Protection (CBP);
- Federal Emergency Management Agency (FEMA);
- U.S. Immigration and Customs Enforcement (ICE);
- Transportation Security Administration (TSA);
- U.S. Coast Guard (USCG);
- U.S. Citizenship and Immigration Services (USCIS);
- DHS Under Secretary for Management (USM);
- U.S. Secret Service (USSS);
- Department of Defense (DOD);
- Department of Justice (DOJ);
- Department of State (DoS);
- Intelligence Community;
- State / local / tribal / territorial law enforcement, federal, state, local investigative agencies,

[11] OBIM retains latent prints in HART's Unsolved Latent File (ULF) that are not initially identified for future searches against known prints to support the DHS mission, unless the latent print contributor requests that the prints not be retained. See Latent Fingerprint Identification section below for more information on latent prints being enrolled and retained in HART.

in coordination with the DOJ;

- Migration 5 partners: Canada, New Zealand, Australia, and the United Kingdom, through agreements negotiated by the DHS Office of Strategy, Policy, and Plans; and

- Other with international partners such as Guatemala, Greece, Italy, and Mexico through bilateral agreements negotiated by the DHS Office of Strategy, Policy, and Plans.

DHS Component System of Record Notices (SORN) and ISAAs govern the function and use of the biometrics records collected by each Component. As a result, OBIM coordinates with DHS Components on privacy compliance documentation that details how information is collected, used, and shared, retained, and disposed of per relevant retention schedules.

OBIM Security manages user access to HART through AWS GovCloud identity access management tools. OBIM Security determines a requestor's security clearance through established procedures that may include the DHS Integrated Security Management System (ISMS).[12] OBIM Security will continuously monitor account inactivity. Upon an authorized request, a specified user account will be completely deleted from system access. To mitigate concerns of unauthorized access, foreign entities are allowed to query HART and can receive Identity eXchange Messaging (IXM)[13] responses, but do not get direct access to the HART system.

OBIM will provide HART users and data providers with OBIM's Biometrics Guidelines, which provide basic expectations on accuracy and the responsible use of identification and analysis activities provided by OBIM.

HART Biometric Modalities & Services

Identity and Encounter Creation

HART stores and processes biometric data. Once a fingerprint and basic biographic information is enrolled in HART, it can be linked with additional biographic information and other biometric modalities, as well as matched in the event of a new encounter. DHS and its Components consider fingerprints to be unique biometric identifiers. For example, data providers may enroll individuals' fingerprints encountered in the context of criminal or civil law enforcement or from an application for an immigration benefit. They may subsequently assign other biometric modalities, such as a facial image or iris, for future identity verification.

An identity in HART can be made up of one or multiple encounters. Adding encounters to an already existing identity is referred to as an assignment. Matching thresholds for fingerprints

[12] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.
[13] IXM is method of communicating with HART in Extensible Markup Language (XML) message format. The XML-based format is designed to perform specific operations (HART Services as described below) for the HART user or data provider. This allows the HART user or data provider to send or receive information to HART.

and iris are determined based on algorithms tuned to specific NIST matching technology.[14] OBIM is working with NIST on establishing an image quality capture standard to ensure consistency in data definition and accuracy for its facial recognition services.

When a HART authorized user initially enrolls an individual's fingerprint and basic biographic information, HART creates a FIN for that individual. While the fingerprint and basic biographic information establish an identity, every subsequent encounter receives a new HART-generated Encounter Identification Number (EID). If the biometrics in the new encounter matches to existing biometrics in the system with a FIN, HART adds a HART-generated EID to that FIN, thereby assigning the new encounter to the identity. HART stores both the FIN, the EID, and the biometric record. In certain circumstances as discussed below, HART will only store the encounter and not the biometric record.

Fingerprint Matching

The fingerprint service provides a high-assurance, positive identification response to a fingerprint request by a HART authorized user for either identification or verification. Fingerprint data sets may include submissions related to visa applicants and other individuals seeking immigration benefits, credentials to secure facilities, submissions from law enforcement actions, or fingerprints associated with national security.[15] After searching the entire fingerprint gallery during an identification request, HART returns the identity with the best match to the fingerprint submitted.

HART can also perform a 1 to 1 verification of fingerprint data with an EID to verify the identity of an individual whose fingerprints were formerly submitted and are stored in HART. Identification requests are solely fingerprint-based and do not use biographic information, such as name and date of birth, as biographic information may be incomplete, incorrect, fraudulent, or otherwise unreliable. Verification requests compare submitted biometric data to a known or asserted identity within the HART system.

Facial Recognition Services

HART provides the following facial recognition service, pursuant to written agreement between OBIM and authorized users, including ISAAs, and as documented in component-specific compliance documentation.[16] OBIM is supporting NIST in the development of a variety of types of standards, including 1) data formats; 2) data transmission/exchange; 3) face image quality standards; and 4) performance testing standards. NIST does not develop "matching standards."

[14] OBIM also leverages the NIST Fingerprint Image Quality standard formalized in ISO/IEC 29794-4:2017 for fingerprints and the ANSI/NIST Type 17 Iris transmission format, *available at* https://www.nist.gov/programs-projects/iris-exchange-irex-overview for iris.
[15] *See* Appendix A for list of authorized users.
[16] *See* Appendix A for list authorized users.

HART users accept risk of the accuracy of match or no match responses from HART based on metrics provided by OBIM, which reflect the contextual factors identified by the program.[17] NIST may assist OBIM by providing recommendations regarding algorithm selection, threshold, and procedures in making match or no match decisions.[18] NIST standards and recommendations[19] will be incorporated into applicable ISAAs and component-specific compliance documentation once finalized. OBIM will distribute OBIM Biometrics Guidelines (currently under development) to provide basic expectations and clarifying information to HART authorized users on accuracy and the responsible use of HART's services, including OBIM's facial recognition service.

The DHS Privacy Office requires OBIM and DHS Components to submit privacy compliance documentation prior to using the facial recognition capability.

***Facial 1 to 1 (Verification)*:** Facial 1 to 1 verification allows a HART authorized user to match a single facial image to an existing facial image associated with a known identity in HART. An authorized user submits a facial image and EID that asserts an identity. HART then provides a response indicating if the face submitted with the asserted identity matches the face of the same identity on file. The threshold for matching is set by OBIM through testing and measuring error rates and statistical representations of matching accuracy to reduce errors and potential bias. OBIM continuously monitors industry research and analysis on biometric performance improvements. OBIM's Biometric Support Center (BSC) reviews specific situations in which the submitted image does not correctly match to a known identity in HART. This scenario is called a mismatch. OBIM leverages the Facial Identification Scientific Working Group (FISWG) guidelines for photo image capture comparisons.[20] OBIM's BSC consists of highly trained employees and contractors that provide expert manual biometric verification and identification services.

***Facial Comparison (2-Photo Submission)*:** The facial comparison feature allows a HART authorized user to submit two photos in a single transaction to determine if the submitted images match at or above a given threshold, as established by OBIM. The capability does not involve searching for or matching against any images in HART. HART will receive two photos, perform the comparison, and provide a match or no-match response to the requestor. The threshold for matching is set by OBIM through testing and measuring error rates and statistical representations of matching accuracy to reduce errors.[21] OBIM leverages the FISWG guidelines for photo

[17] Contextual factors may include the demographic of the population (e.g., age, sex, race), camera quality, the rate of throughput, lighting, distance, and size of the database, as well as other factors.
[18] OBIM has a forthcoming OBIM NIST Biometric Study PIA to discuss the transfer of biometrics to NIST for facial recognition, fingerprint, and iris biometrics applications testing.
[19] OBIM will continue to work and collaborate with DHS components including the DHS Science & Technology to continually improve HART's biometric services.
[20] OBIM leverages guidelines from the FISWG for photo facial image capture comparison *available at* https://fiswg.org/index.htm.
[21] OBIM is working with NIST to develop a face-quality capture standard to support OBIM's facial recognition program to ensure consistency in data definition and accuracy.

comparison.[22] Having been informed of the accuracy metrics through the OBIM Biometric Guidelines and based on the program's contextual factors, the submitting official retains discretion as to any action resulting from a match or no match response. Facial Comparison photos are not compared against HART data and will not be enrolled or stored in HART—only a record of the encounter is enrolled or stored; these photos and the resulting response will be immediately deleted from the system.

***Facial 1 to Many (Identify Candidates)*:** Facial 1 to Many biometric search allows an authorized HART user to submit a face image and request a search of facial images held in one or more specified HART face galleries. Submitted face images may come from a photo or video capture and must follow the American National Standards Institute (ANSI)/NIST Type 10[23] record format for data exchange.

OBIM's Biometrics Guidelines will provide basic expectations for accuracy and clarifying information to HART authorized users on the responsible use of HART's biometric services, including facial recognition services. OBIM is working to determine the optimal 1 to Many face threshold through testing and measuring error rates and statistical representations of matching accuracy for best performance and to reduce potential bias. HART does not provide a single match for 1 to Many searches. It returns candidate lists, devoid of biographic data. The numbers of candidates returned and the threshold for candidate identification is specified per written agreement for the 1 to Many service.

As with other facial recognition services, DHS Components and other HART authorized users, prior to using the 1 to Many service, will have in place written agreements with OBIM, including ISAAs. DHS users will have Component-specific privacy compliance documentation to describe specific projects that will use the 1 to Many capabilities.

Iris Matching Capability

HART currently has an operational iris gallery, allowing 1 to Many iris matching capability. As with facial images, all iris enrollments are associated with fingerprints and basic biographic information. The 1 to Many service searches a submitted iris against the iris gallery in HART. If there is no match above an OBIM-selected threshold, then OBIM's BSC will review and provide a hit/no hit response. If the iris matches to an iris in HART (discussed as a "hit"), then HART will only return the identity of the fingerprint associated with the iris. HART will not provide any iris-only responses. OBIM leverages the ANSI/NIST Type 17[24] format for iris

[22] OBIM leverages guidelines from the FISWG for photo facial image capture comparison *available at* https://fiswg.org/index.htm.
[23] ANSI/NIST ITL 1-2011, Update 2015, Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, https://www.nist.gov/programs-projects/ansinist-itl-standard.
[24] OBIM uses ANSI/NIST Type 17 Iris transmission format, *available at* https://www.nist.gov/programs-projects/iris-exchange-irex-overview.

biometric transmission and the NIST Iris Exchange (IREX) I Interagency Report for Interoperability standard. HART has the capability to store the iris image and shares the matching in accordance with ISAAs, National Archives and Records Administration (NARA)-approved retention schedules, and approved DHS Component documentation.

The DHS Privacy Office requires OBIM and DHS Components to submit privacy compliance documentation prior to using the iris matching capability.

Latent Fingerprint Identification

Latent fingerprints ("latent prints") refers to prints deposited on a surface from a person whose identity is unknown. These prints or impressions result from the patterns of friction ridges, which are the raised portions of a fingerprint. The prints are collected by federal, state, local, tribal, territorial, foreign, and international agencies for investigative and national security purposes. In the case of domestic law enforcement entities, OBIM accepts such prints only after it has been determined that they do not match prints in Federal Bureau of Investigation's (FBI) Next Generation Identification System (NGI). OBIM may also receive latent prints through submissions from partners pursuant to certain international agreements (e.g., Preventing and Combatting Serious Crime Agreements) and treaties (e.g., Mutual Legal Assistance Treaties).

Authorities collect latent prints at crime scenes, terrorist incidents, or other similar locations of law enforcement interest, including from deceased individuals when conditions of the decedent's fingerprints do not allow for a 10-print search.[25] Authorities then transmit digitized images of these latent print impressions to OBIM. OBIM searches these records against identities in HART.

For each image compared, HART assigns numerical values that indicate the similarity between known fingerprints in HART and the latent fingerprint submitted. HART returns a candidate list to the submitter with the top twenty (or less, if twenty do not exist) unique highest-scoring candidates authorized by HART data owners for automated sharing with the associated EID. HART applies its filtering protocols to comply with existing law and policy. Candidates not authorized by HART data owners for automated sharing are adjudicated manually; OBIM will seek consent from the data owners prior to sharing those candidates. If an authorized user determines the IDENT/HART candidate conclusively matches the submitted latent print, the authorized user may use the EID to request additional biographic data (e.g., name, date of birth,

[25] *See Memorandum of Understanding among the Department of Homeland Security, the Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, the Department of State, Bureau of Consular Affairs and the State of Texas, Department of Public Safety for Latent Fingerprint Interoperability,* August 2016, *and Memorandum Of Understanding Between And Among the U.S. Department Of Homeland Security, the U.S. Department Of Justice, Federal Bureau Of Investigation, Criminal Justice Information Services Division and the U.S. Department Of State Bureau Of Consular Affairs For Improved Information Sharing Services And Enhanced Biometric Interoperability* expected to be signed February 2020.

and fingerprint identification number) about the candidate.

DHS data owners derive mission value from investigative actions that establish a derogatory nexus to DHS populations (e.g., law enforcement, travel and immigration benefits, and travel/access privileges). Latent fingerprints that do not match to any existing fingerprints in HART may be stored in HART's Unsolved Latent File (ULF) when requested by the latent print owner. Depending on the requesting user's needs and written agreements, the latent prints may be enrolled or used as search-only data and stored in a sub-system separate from fingerprint data. Latent prints from individuals who were deemed victims, bystanders and/or law enforcement personnel, and those handling the evidence at criminal or terrorist incidents are immediately deleted from HART once they are reported as such to OBIM by the providing agency. If further law enforcement action is taken (e.g., warrant issued, arrest), OBIM will be notified of the encounter. OBIM will destroy submitted latent prints with conclusive matches within five (5) business days of DHS or Department of State (DoS) data owner notification. The majority of latent prints in the ULF come from Department of Defense (DoD) and FBI, while the remaining come from DHS, state and local law enforcement, and foreign and international agencies for investigative and national security purposes.[26] All fingerprints submitted by HART users from individuals whose identities are known are searched against the ULF to determine if there is a match. This is known as a "reverse latent search." OBIM notifies the submitter when a reverse search results in a match.

HART Identity Services

HART authorized users may request a service or provide information to the HART system. Authorized users have the ability to determine which services they need based on mission needs and technical capabilities and in accordance with DHS Component-specific compliance documentation, ISAAs, and DHS and NARA-approved retention schedules that delineate the terms of use and any information sharing restrictions. HART services are used in accordance with an authorized user's ISAA with OBIM and in compliance documentation as referenced in Appendix A. Appendix B provides additional information on the HART services.

HART Data Filtering

HART data providers and users have mission-based access limitations. HART implements access control through robust filtering capabilities, implemented through code, that can remove access to information at the organizational, encounter, and identity/person level based on purpose or activity type. Filtering can also be conducted based on Derogatory Information (DI).[27] OBIM

[26] See *Memorandum of Understanding among the U.S. Department of Homeland Security the Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division the U.S. Department of State Bureau of Consular Affairs and the State of Texas Department of Public Safety for Latent Fingerprint Interoperability*, October 2016.

[27] Derogatory Information is information which potentially justifies unfavorable suitability, fitness, or security

encodes these data filtering authorizations through business rules, which are the system configurations that reflect the permissions of each HART authorized user as agreed to in ISAAs with OBIM or DHS and as described in DHS Component-specific privacy compliance documentation, as applicable.[28] Filtering can also be done at the request of the data provider. The different types of filtering are described below.

Organizational filtering, also called Organization/Unit/Subunit (O/U/S) filtering, uses configuration settings within the HART system to remove information about encounters that are not permissible to share from responses to the authorized user's query. Each HART authorized user has an O/U/S account for their specific agency or organization, and their account receives information in accordance with defined filtering rules as determined by statues and DHS policies, and in ISAAs and as described in component compliance documentation. Since HART is only a repository and OBIM does not own the data, authorized users who upload and store biometric information HART are considered "data providers," as well as the "data owners." HART has the ability to either filter or share HART data from an O/U/S in accordance with permissions set by the data owner at the request of the user requesting the data. Filtering can also be done at the request of the data provider. Each O/U/S is configured to receive or filter out certain types of information based on data owner-set permissions, ISAAs, and other technical specification documents with DHS partners. The filtering restrictions, risks, and mitigations are captured in DHS or DHS Component-user's privacy compliance documents.

Identity level flagging and filtering establishes the capability for an O/U/S to submit a flag indicating that an individual belongs to a defined population, either during the process of encounter enrollment or separately to add or update an existing encounter. This flag acts to filter an individual's entire identity, including every encounter that exists for that individual in HART, from a requesting O/U/S that is unauthorized from receiving information on (including the existence of) identities belonging within that population. Unauthorized requestors typically receive a response indicating that there was no match to the identity, as determined by applicable law and policy.

Encounter filtering (also referred to as activity type filtering) uses configuration settings within the HART system to filter encounters from responses being returned using the designated activity category stored in the Activity Type field. Encounter filtering considers both the O/U/S and Activity Type of the requestor and data provider when making a sharing determination.

---

adjudication and such information may prompt a request for additional investigation or clarification for resolution of an issue. *See* DHS Instruction 121-01-007-01 for Personnel Security, Suitability and Fitness Program (August 2016). HART users will have the ability to Add or Deactivate DI. Deactivating a particular DI demotes the DI. HART will not include that deactivated DI element in the response to the Authorized user. DI may include information submitted from the Department of Defense (DoD), the Federal Bureau of Investigations (FBI), the Department of State, INTERPOL, international country partners, and DHS Components, specifically ICE, and CBP. See Section 2.1 below for a list of DI data elements.

[28] *See* Appendix A for a list of authorized users.

Because all HART users are not authorized to receive all types of DI, HART can either filter or share DI data according to O/U/S. DI Filtering implements access rules, based on the applicable agreement, and internal technical and operational documents, by removing a predetermined DI type from the response to the HART authorized user. It is important to note that the encounter containing the filtered DI is not impacted by this particular filtering layer, meaning that the user receives all information contained in that encounter that he or she is authorized to receive.

The DHS Privacy Office's statutory mission is to "assure that the use of technology sustains, and does not erode, privacy."[29] Due to the privacy risks associated with the collection, retention, use, and dissemination of biometrics, the DHS Privacy Office has included additional recommendations throughout the "Privacy Impact Analysis" section of this PIA to better mitigate the privacy risks. In addition, the DHS Privacy Office will initiate a Privacy Compliance Review (PCR) of HART's governance within one year of this PIA's publication. The PCR will evaluate how OBIM is protecting privacy as described in this PIA and will also determine if OBIM is following the DHS Privacy Office recommendations provided in the "Privacy Impact Analysis" section of this PIA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The data in HART is collected, processed, and stored consistent with the applicable authorities of the agencies that originally collected the data, as expressed in ISAAs with OBIM or agreements or arrangements with DHS. When the agency is internal to DHS, these authorities are also described in applicable PIAs and SORNs. OBIM identifies each collection by data provider and implements the provider's authority to use, retain, and share the information according to the terms of the applicable ISAA, which may include a MOA, MOU, or other formal, data sharing policy. HART enables sharing with authorized users after the data provider has approved the sharing through an approved ISAA and as described in component SORNs.[30]

The statutory and other authorities pertaining to the establishment and mission of the OBIM program for the operation and maintenance of HART, include the following statutes and authorities:

[29] *See* 6 U.S.C. § 142.
[30] See Appendix A for additional information.

- Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000, Public Law 106-215, codified at 8 U.S.C. § 1365a;
- Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106-396 codified at 8 U.S.C. § 1379;
- Section 403(c) and 414 of the USA PATRIOT ACT, Public Law 107-56 codified at 8 U.S.C. § 1379, 8 U.S.C. § 1365a, 8 U.S.C. § 1365a note;
- Section 202, 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002, Public Law 107-173 codified at 8 U.S.C. §§ 1722, 1731;
- Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458 codified at 8 U.S.C. § 1365b;
- Section 711(d) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53 codified at 8 U.S.C. § 1187; and
- Other authorities can be found at: 6 U.S.C. §§ 202, 481-485, 8 U.S.C. §§ 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1379, and 1732; 19 U.S.C. § 1589a.

Additionally, OBIM operates the HART system to support partner agencies, which carry out their authorities pursuant to applicable law and regulation. Specific authorities are referenced in applicable privacy compliance documentation listed in Appendix A, updated as appropriate.

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

The information in HART is covered by the source system DHS, DHS Component, and partner SORNs, which govern the function and use of the biometrics records collected by each Component. DHS information in HART relies on the DHS/ALL-041 External Biometric Records (EBR) System of Records Notice[31] to govern the maintenance and use of biometrics and associated biographic information received from non-DHS entities. The forthcoming Enterprise Biometric Administrative Records (EBAR) SORN will cover administrative records maintained in HART.[32]

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

No. OBIM is in the process of obtaining the Authority to Operate (ATO) for HART,

[31] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (May 24, 2018).
[32] The forthcoming EBAR SORN will support OBIM's existing and future administrative and reporting functions including information sharing coordination and reporting to provide information in response to queries from external agencies and foreign HART data providers charged with national security, law enforcement, immigration, or other DHS mission-related functions; provide information in response to redress inquiries and HART user requests; and provide internal reporting and other administrative tasks to OBIM.

expected in 2020. The authority to operate is pending publication of this PIA. OBIM will publish updates to this PIA prior to operationalizing additional Increments and functionalities.

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

A records schedule was approved by NARA, which requires OBIM to maintain HART records in its custody for the various retention periods outlined in the Biometric with Limited Biographic Schedule (DAA-0563-2013-0001).[33] OBIM is re-evaluating the current retention policy to determine variable retention periods for latent fingerprints and international records and will publish a PIA update for any change in retention periods.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

OBIM currently has no collections that would trigger the PRA. DHS, however, requires certain aliens who cross the borders of the United States to provide fingerprints, photographs, and/or other biometric identifiers upon their arrival and departure at designated ports. Additionally, HART contains information on DHS personnel,[34] individuals applying for credentials and opt-in enrollments (e.g., Global Entry[35] and TSA Precheck).[36] These requirements constitute an information collection under the PRA. All information stored in HART is collected by HART data providers and stored under the data provider agency's regulatory notices and authorities.

Section 2.0 Characterization of the Information

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

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

HART authorized users will have acess to the business rules configurations that reflect the permissions of each HART authorized user as agreed to in ISAAs with OBIM or DHS and as described in DHS Component-specific privacy compliance documentation, as applicable.

---

[33] *See* Biometric with Limited Biographic Schedule, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.
[34] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS) and subsequent updates, *available at* www.dhs.gov/privacy.
[35] *See* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* www.dhs.gov/privacy.
[36] *See* DHS/TSA/PIA-041 TSA Pre✓™ Application Program, *available at* www.dhs.gov/privacy.

HART maintains biometric and associated biographic information collected by DHS and non-DHS entities.

A record stored in HART may contain the following data elements:

- Biometric data, including: facial images, fingerprints, and iris images;
- Biometric-associated biographic data including full name (i.e., first, middle, last, nicknames, and aliases); date of birth (DOB); gender; personal physical details (e.g., height, weight, eye color, and hair color); signature; assigned number identifiers (e.g., A-Number, Social Security number (SSN), 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, when available);
- DI,[37] which may consist of wants and warrants, known or suspected terrorist (KST) designation, sexual offender registration, foreign criminal convictions, and immigration violations, when available. Specifically, the data elements include the following: KSTs, wanted persons, sex offenders, state and local 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; aliens with criminal history, known or suspected gang members, enforcement actions taken at CBP Ports of Entry; expedited ICE immigration removals; and law enforcement community alerts;
- Miscellaneous officer comment information, when available;
- Encounter data, including location and circumstance of each instance resulting in biometric collection; and
- Unique machine-generated identifiers (e.g., fingerprint identification number (FIN), EID, and Transaction Control Number (TCN)) that link individuals with their encounters, biometrics, records, and other data elements. These data elements enable the execution of administrative functions of the biometric repository such as redress operations, testing,

[37] Each HART user may use authorized DI received from a HART response in accordance with mission needs and as defined in ISAA or as defined in DHS component compliance documentation.

training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.

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

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

- Directly from the individual applying for a credential, through opt-in enrollments (e.g. Global Entry[38] and TSA Precheck);[39] an immigration benefit, pursuant to a background investigation;
- Via military and law enforcement direct encounters or forensic operations according to the data provider's authority; or
- Through records shared by foreign governments according to written agreement or cooperative arrangement.

External DHS data providers include DoS; DOJ; DOD; other federal, state, local, tribal, territorial law enforcement organizations, foreign governments, and international agencies. Foreign government data providers include the Five Eyes/Migration Five Partners, namely Canada, United Kingdom, Australia, and New Zealand, certain Visa Waiver Program (VWP) countries under the Protecting and Combatting Serious Crime Agreements, and other allied nations providing information pursuant to an agreement or arrangement. International agency information can include Office of the United Nations High Commissioner for Refugees (UNHCR) collected biometrics for refugees who are referred to the United States for resettlement.

DHS data provider sources include PLCY via the Program Manager for information sharing with international partners, CBP, ICE, USCG, USCIS, TSA, FEMA, the DHS Office of the Chief Security Officer (OCSO), and the Intelligence Community. For example:

- The USCG interdicts and refers for prosecution illegal immigrants and 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; and
- TSA collects information to support the vetting and adjudication of their current credentialing populations which may include workers seeking access to secure facilities,

[38] *See* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* www.dhs.gov/privacy.
[39] *See* DHS/TSA/PIA-041 TSA Pre✓™ Application Program, *available at* www.dhs.gov/privacy.

and TSA Precheck applicants.

Each DHS data provider is responsible for documenting their own data collections in a SORN and PIA. 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 HART user such as the site of a terrorist incident. The data is then securely transmitted to HART and accessed by mission need.

A more detailed accounting of DHS data provider collections and external sources can be found in the collector's privacy compliance documents.[40]

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

HART may use information from publicly available sources, collected according to the data provider's authority. Specific publicly available sources are discussed in more detail in the appropriate data provider's privacy compliance documentation.

2.4 Discuss how accuracy of the data is ensured.

Fingerprint Identification and Verification

OBIM leverages existing industry standards, including the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 19795-1:2006 Biometric performance testing and reporting. OBIM is aware of efforts by individuals to provide a fraudulent or fake identity including using morphing techniques. OBIM recommends that data providers use liveness detection[41] tools to counteract and mitigate any efforts or provide a fake identity. OBIM participates in various forums including the Intelligence Advanced Research Projects Activity (IARPA), FBI, NIST, DoD, and private sector groups, that look into countermeasures to understand new applications to biometrics and how agencies can counteract individuals that try to compromise biometric accuracy. OBIM will position itself with HART to evaluate the best biometric alteration detection tools in order to protect the system's data integrity.

OBIM monitors and maintains the accuracy and integrity of the fingerprint data in HART through fingerprint tuning. Fingerprint tuning involves testing false match rates and false non-match rates,[42] and then making sure those data results are performing optimally with the matcher

[40] *See* list of DHS component and external source compliance documentation in Appendix A of this PIA.
[41] Liveness detection is any technique used to detect a spoof attempt by determining whether the source of a biometric sample is a live human being or a fake representation. This is accomplished through algorithms that analyze data collected from biometric sensors to determine whether the source is live or reproduced.
[42] A false non-match rates measures the probability that the system fails to detect a match between the input and a

algorithm. OBIM tunes fingerprint matchers to optimize accuracy according to existing business rules. Depending on the matcher algorithm, there are tuning parameters that can optimize accuracy rates for a specific gallery and application. While OBIM makes efforts to promote accuracy, the data provider shares responsibility for the accuracy, completeness, and quality of the data uploaded to the system.

Latent Prints

Additional accuracy processes are built in to the process for matching HART records against latent fingerprints. Because these prints may be partial, incomplete, or oriented differently than in controlled collection settings (in addition to many other possible anomalies), accurate identification is less reliable. To ensure accurate matches for latent prints, HART returns a limited number of possible matches to trained and experienced fingerprint examiners in its BSC. BSC latent-print examiners make a final determination on whether the submitted print matches any of the fingerprints currently retained in HART. If BSC examiners confirm that there is a match in HART, the submitting agency can request additional information on the individual.

Face

For Increment 1, OBIM currently offers the following facial recognition services:

- ***Facial 1 to 1 (Verification)*:** Facial 1 to 1 verification allows a HART authorized user to match a single facial image to an existing facial image associated with a known identity in HART;
- ***Facial Comparison (2-Photo Submission)*:** The facial comparison feature allows a HART authorized user to submit two photos in a single transaction to determine if the submitted images match at or above a given threshold, as established by the authorized user. The capability does not involve searching for or matching against any images in HART; and
- ***Facial 1 to Many (Identify Candidates)*:** Facial 1 to Many biometric search allows an authorized HART user to submit a face image and request a search of facial images held in one or more specified HART face galleries. Specifically, OBIM currently uses BSC Examiners for manual verification prior to returning a candidate list to the requester for adjudication for the 1 to Many service as described above.[43]

OBIM is continually working to improve facial recognition accuracy. OBIM leverages ANSI/NIST Type 10 for biometric transmission formats.[44] The transmission formats are

matching biometric in the database.
[43] See Biometrics Modalities and Services section on pg.7 for additional information.
[44] See additional information on NIST/ANSI Type 10 face transmission format *available at* https://www.nist.gov/programs-projects/ansinist-itl-standard.

recognized throughout United States government and industry. Users follow the biometric transmission formats when submitting images to HART.

OBIM is currently working directly with NIST to develop a facial image quality capture standard. OBIM also conducts testing to measure match errors and select thresholds and configure business rules (i.e., how the system implements sharing and restrictions in accordance with applicable agreements) to reduce error rates. OBIM is aware of efforts by individuals to provide a fraudulent or fake identity using morphing techniques including deep fakes. A deep fake is a type of presentation attack that involves the modification of an image or video using an algorithm to make that image or video appear authentic. OBIM participates in various forums including with IARPA, FBI, NIST, DoD, and private sector groups, that look into countermeasures to understand new applications to biometrics and how agencies can counteract individuals that try to compromise biometric accuracy. OBIM will position itself with HART to evaluate the best biometric alteration detection tools in order to protect the system's data integrity. Data provers should also consider using tools to detect deep fake use at the point of collection.

HART users accept risk of the accuracy of match or no match responses from HART based on metrics provided by OBIM, which reflect the contextual factors identified by the program. As OBIM implements future HART increments, OBIM will continue to provide additional transparency including the limits, risks, and mission benefits of our facial recognition services in a future PIA update.

Iris

Increment 1 will offer a 1 to Many iris service that searches a submitted iris against the iris gallery in HART. In Increment 1, if there is no match above an OBIM-selected threshold, then OBIM's BSC will provide no-hit response. If the iris matches to an iris in HART (described as a "hit"), then HART will only return the identity of the fingerprint associated with the iris. HART will not provide any iris-only responses. Every iris in HART will have an associated fingerprint. OBIM leverages the ANSI/NIST Information Technology Laboratory (ITL)-2011 Type 17 format for iris transmissions.[45]

OBIM also conducts testing to calculate match error rates and statistical representations of matching accuracy. OBIM will position itself with HART to evaluate the best biometric alteration detection tools in order to protect the system's data integrity. HART users make match/no match decisions based on acceptance of risk and OBIM's accuracy metrics. OBIM will include any updates or changes to the iris recognition services in a subsequent PIA update.

[45] See additional information on NIST/ANSI ITL Type 17 transmission format and the NIST/IREX I iris matching standard *available at* https://www.nist.gov/programs-projects/iris-exchange-irex-overview.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that HART facial image matching results may be inaccurate or result in a disproportionate impact to certain populations.

Mitigation: OBIM mitigates this risk by conducting face matcher tuning in order to optimize accuracy and system performance. The face matcher tuning evaluates face algorithms for biographic, biometric, and contextual factors. Contextual factors may include the demographic of the population (e.g., gender, race, and age), camera quality, the rate of throughput, lighting, distance, and size of the database, among other factors. OBIM uses protocols to evaluate test plans and is currently reviewing those test plans with NIST. OBIM leverages the ANSI/NIST Type 10 biometric transmission format for facial images.[46] To promote accuracy in HART's facial recognition service, OBIM has limited the automated capability to 1 to 1 and two photo comparison and deploys BSC examiners to assist when the technology cannot return a Match/No Match response. Specifically, OBIM currently uses BSC Examiners for manual verification prior to returning a candidate list to the requester for adjudication for the 1 to Many service.

OBIM, DHS Components, and other authorized users will complete ISAAs with OBIM and other privacy compliance documentation, as needed, to describe specific projects that will use this capability.

Privacy Risk: There is a privacy risk that non-matching facial images are disclosed to HART authorized users.

Mitigation: In the case of the 1 to 1 facial recognition service, if the match does not return a match/no-match result, the facial images are reviewed by OBIM's facial examiners in the BSC and non-matching faces are not disclosed to HART users. HART may generate candidate list as an investigative lead as part of a 1 to Many service. OBIM's BSC may review candidate lists and provide them to authorized HART users for use as an investigative lead only and not the sole basis for any law enforcement action.

DHS Privacy Office Recommendation: When drafting the OBIM Biometric Guidelines, OBIM should consider content that will assist data users and data providers when determining accuracy, the parameters for providing candidate lists, a description of BSC examiner services, the requirements and retention period for probes (e.g. latent prints and facial images), any prohibitions on intentional alteration of an original biometric, any required training for HART system use, responsibilities for adherence to the applicable records retention schedule, and OBIM's audit schedule for HART. The OBIM Biometrics Guidelines should also describe the tuning and

[46] Additional NIST Biometric Transmission information is *available at* https://www.nist.gov/programs-projects/ansinist-itl-standard.

business rules process as it applies to all biometric modalities.

Privacy Risk: There is a risk that the quality and integrity of information collected and maintained in HART may not have sufficient quality required to serve its purpose of biometric and biographic verification and matching, thus potentially causing misidentification.

Mitigation: HART mitigates this risk by requiring fingerprints, which are unique identifiers, and basic biographic information, to establish an identity in HART. HART offers manual fingerprint comparisons, fingerprint quality checks by the data provider, and 10-print matching. Additionally, HART performs certain quality checks (e.g., determining the quality of a captured fingerprint and its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness. HART conducts face and fingerprint matcher tuning to monitor and maintain the accuracy[47] and integrity of biometric data.

To ensure accuracy in facial image recognition, OBIM has the capability for 1 to 1 and two photo comparison and deploys BSC examiners to assist when the technology cannot return a Match/No Match response. OBIM is currently coordinating with NIST to develop a facial image capture quality standard. This will ensure consistency in data definition and conformance interoperability between systems.

The original data owner, whether an organization external or internal to DHS, is also responsible for ensuring the accuracy, completeness, and quality of the data submitted to OBIM. OBIM recommends that data providers follow best practices and guidelines of the Facial Identity Scientific Working Group including the Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems.[48]

OBIM provides a redress process for individuals who believe the data held on them in HART is inaccurate, as detailed in Section 7 of this PIA.

Privacy Risk: There is a risk of collecting and sharing more information than is required for the purposes of the system, because HART cannot filter by biometric modality and collects biographic data that details the subject's encounters, which are not strictly necessary for identity verification or identification.

Mitigation: This risk is partially mitigated. HART shares different types of responses with

[47] Testing also includes testing the True Acceptance Rate (TAR) and the False Acceptance Rate (FAR). The TAR is the probability that a biometric system will correctly verify an individual's true claim of identity. This statistic is expressed as a percentage and is used to measure biometric performance of verification. The FAR is the probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. This statistic is expressed as a percentage and is used to measure biometric performance of verification or identification. OBIM may modify terms based on new industry research and analysis.

[48] *See FISWG Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems*, https://fiswg.org/FISWG_Guide_for_Capturing_Facial_Images_for_FR_Use_v2.0_20190510.pdf.

different users based on a specifically articulated purpose as determined in information sharing agreements. For certain data providers, the full encounter history of an individual's biometric interactions with the Department is required to meet the mission of the agency. For example, a data provider may determine whether non-derogatory information should be shared with HART authorized users. When that data provider determines that the user does not need and/or is not authorized to receive this data, that data is withheld from the response provided to the HART user through the business rules. The business rules can also be configured to block sharing of biometric data in response to a query. HART responses are appropriately scoped to the purpose of each authorized user, as memorialized in an ISAA with OBIM and applicable DHS Component privacy compliance documentation.

Privacy Risk: In a limited number of instances, the automated biometric match process will result in biometric information that does not correctly map to one individual. This can occur, for example, when an individual has low quality fingerprints, which increases the likelihood of a matching error and causes the system to establish two identities for one person. This can also occur if a facial image does not correctly match to one individual.

Mitigation: This risk is mitigated in two ways. Internally, HART can merge records when the same person has two different identities in HART, usually because of poor fingerprint quality. The process works when a new encounter matches to two identities in the system, indicating that the two identities are in fact one person. When the new encounter is tied to two separate identities, the OBIM BSC examiners review the identities before merging them into one identity as part of the matching process.

In other instances, the identities can be separated if the wrong biographic information has been assigned to them, either because of an error in automation or because of a human error such as an inspector transposing the traveler's biometrics with the traveler's travel companion's biographic information. HART will not automatically merge or separate identities. All merge or separation request will require BSC examiner review.

In the case of the 1 to 1 facial recognition capability, if the match does not return a match/no-match result, the facial images are reviewed by OBIM's facial examiners in the BSC and non-matching faces are not disclosed to HART users. In the case of the 1 to Many face service, OBIM's expert facial examiners may return a candidate list to the user for investigative leads only. As with fingerprints, OBIM will not automatically merge any facial image to an identity without human review and authorized HART user requests. OBIM is working closely with NIST to develop facial image quality capture standards to improve matching accuracy.

Privacy Risk: There is a privacy risk that a Pre-Verify or biographic-only search will return inaccurate responses, as there could be multiple responses for the same person.

Mitigation: This risk is mitigated through the follow up Pre-Verify request process. If

HART finds multiple identities and not a single, usable identity, HART will request the user return biometrics, including fingerprints and facial images, for identification. OBIM will not automatically merge any facial images to an identity without human review and authorized HART user requests. As mentioned above, OBIM is working closely with NIST to develop facial image quality capture standards to improve matching accuracy and participates in the multi-agency Facial Identification Scientific Working Group to monitor best practices and guidelines for facial recognition services.

Privacy Risk: There is a privacy risk that data quality will not be maintained since HART users have the ability to manually apply derogatory and disposition information.

Mitigation: This risk is not mitigated. OBIM cannot ensure accuracy since the information is not automatically pulled from the source system. OBIM does coordinate with users to determine what derogatory information they are authorized to share. Additionally, OBIM will train HART users on how to use HART's derogatory services in accordance with the user's source system mission and business rules.

Privacy Risk: There is a risk that the use of deep fake images will impact the quality of iris and facial recognition services.

Mitigation: OBIM collaborates with IARPA, FBI, NIST, DoD, and the private sector, to look into deep fake usage and countermeasures to understand new applications to biometrics and how agencies can counteract individuals that try to compromise biometric accuracy using deep fake images. The OBIM Biometric Guidelines will recommend that data collectors use liveness detection devices[49] at the point of collection in order to minimize the impact of deep fakes. OBIM will also position itself with HART to evaluate the best biometric alteration detection tools in order to protect the system's data integrity.

Privacy Risk: There is a risk that retaining the fingerprint, face, or iris biometric for juveniles may result inaccurate results due to factors including growth and image quality.

Mitigation: This risk is not mitigated. OBIM is currently retaining juvenile biometrics received from data providers in accordance with the memorandum titled "DHS Biometrics Expansion for Improved Identification and Encounter Management," signed by Secretary Kelly in May 2017.[50] This memorandum augments existing DHS policy to use biometric identification across all screening missions and to collect multimodal biometrics at the time of application or encounter, beyond the 14 and 79 years age range, when and where it is technically and operationally feasible. OBIM is in the process of working towards isolating all juvenile biometrics

[49] Liveness detection is any technique used to detect a spoof attempt by determining whether the source of a biometric sample is a live human being or a fake representation. This is accomplished through algorithms that analyze data collected from biometric sensors to determine whether the source is live or reproduced.
[50] *Available at* https://www.dhs.gov/publication/dhs-biometrics-expansion.

in a separate gallery to minimize any impacts to matching accuracy. Additionally, OBIM is following and monitoring industry best practices including the Center for Identification Technology Research (CITeR)[51] as it continues to conduct studies and evaluate biometric modalities and matching for children under 14.

DHS Privacy Office Recommendation: OBIM should establish a baseline quality for enrollment of all biometric modalities and provide guidance as to reliability of the modalities according to the age of the subject at the time of collection.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

HART's authorized users typically carry out their missions by capturing biometric data and submitting the biometric data to HART. OBIM uses the transmitted data to match, store, and share results as permitted by the data owner's authorities and documented in information sharing agreements. OBIM shares the information with users in support of their national security, credentialing, law enforcement, immigration, and intelligence. Each authorized user documents the data collections and uses in their respective PIAs, SORNs, and ISAAs.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, currently HART does not have advanced analytics capabilities. OBIM will coordinate with the DHS Privacy Office and other appropriate DHS Components on any future advanced analytics capabilities.

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

The following DHS Components may provide and receive information through HART:

- CBP;
- DHS Office of Intelligence & Analysis;
- DHS OCSO;

[51] *See* information on Center for Identification Technology Research (CITeR), *available at* https://citer.clarkson.edu/affiliates/.

- FEMA;
- ICE;
- TSA;
- USCG;
- USCIS; and
- USSS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that HART users may use information for purposes inconsistent with the purpose of the original collection.

Mitigation: ISAAs between OBIM and data providers and OBIM and data users will ensure the business rules implement compatibility of collection and use. Moreover, HART records audit trails of changes made to service request processing priorities and changes made to system operating parameters and thresholds. More specifically, HART tracks and logs changes made to business processing rules, Service Level Agreements (SLA), accounting of disclosures of PII, all outgoing transaction data (excluding biometric images) sent as part of an outgoing identity message, authorized and unauthorized actions, deletions, modifications, errors, exceptions, and actions performed by users accessing the data. Quality assurance audits will be available to all HART authorized users and oversight offices.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

HART does not provide individuals notice prior to the collection of information, as it is merely a service provider and data repository. This PIA and the EBR SORN and forthcoming EBAR SORN provide general notice that an individuals' personal information may reside in HART. Notice is also provided through the publication of PIAs and SORNs on the underlying systems of original collection and the information shared from those systems.[52] If required by law

[52] *See* Appendix A for a list of authorized users and associated privacy compliance documents.

or policy,[53] DHS Components, as well as external partners that submit information to HART and other DHS systems, provide notice to the individual at the point of collection related to storage and retention of information, including whether it is retained initially in IDENT or currently in HART.

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

Because HART operates as the DHS back-end biometric identification system and repository, individuals should consult other DHS programs' Privacy Impact Assessments[54] for specifics on opportunities to opt-out and consent. Some biometric enrollments in HART are non-consensual (e.g., an arrest by law enforcement), which do not generally provide individuals the opportunity to opt out. On the other hand, consensual enrollments (e.g., Global Entry or TSA Pre-Check) often offer the opportunity to opt out or consent to certain uses. Information received from outside DHS may or may not offer the opportunity to opt out or consent to uses.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may not be aware that information collected directly from him or her (e.g., provided during an application for a benefit or credential) may be stored in HART and shared with other HART users.

Mitigation: OBIM cannot fully mitigate this risk because OBIM is not the original collector of the information. OBIM partially mitigates this risk through publication of this PIA.

Privacy Risk: There is a risk that individuals are not aware that their information is indirectly collected (e.g., latent fingerprints and facial images).

Mitigation: HART cannot fully mitigate this risk because HART is not the original collector of the latent prints or facial images. Although individuals may not be aware that their fingerprints or facial images were extracted from crime scenes or terrorist incidents, such prints are not retained in HART once they are linked to a biographic and that individual has been identified as a bystander or victim, as memorialized in data provider information sharing agreements that cover latent prints.

[53] *See* Privacy Policy Guidance Memorandum: 2017-01 (April 2017), *available at* https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.
[54] *See* Appendix A for a list of authorized users.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

HART maintains records for a variable period of time in accordance with National Archives and Records Administration (NARA)-approved records schedules. Through the Delete Encounter service, data owners can schedule the deletion of biometric records in accordance with their NARA-approved retention schedule. Data owners may need to recalibrate retention schedules in consideration of the different modalities.

OBIM, in coordination with DHS, is identifying other data that may not match to an existing retention schedule and will provide an update in a subsequent PIAs.

The latent fingerprint biometric retention schedule is currently in development with OBIM and will be submitted thereafter to NARA for approval.

The transactional record systems retention schedule is currently in development with OBIM and will be submitted thereafter to NARA for approval.

OBIM currently keeps international records for 75 years. DHS is re-evaluating the current retention policy to determine whether a new retention period or combination of retention periods is appropriate. DHS will publish a PIA update for any change in the retention period.

OBIM's current Record Schedule DAA-0563-2013-0001 covers DHS biometric and biographic records used for national security, law enforcement, immigration, and other functions consistent with DHS authorities has been approved by National Archives and Records Administration (NARA). EBR records include:

- Law Enforcement Records: Identification, investigation, apprehension, and/or removal of aliens unlawfully entering or present in the United States and facilitate legal entry of individuals into the United States, which must be destroyed or deleted 75 years after the end of the calendar year in which the data is gathered.
- Records related to the analysis of relationship patterns among individuals and organizations that are indicative of violations of the customs and immigration laws including possible terrorist threats from non-obvious relationships and specific leads and law enforcement intelligence for active and new investigations. These records must be destroyed or deleted 15 years after the end of calendar year of last use of individual's data.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the system will retain biometrics for longer than

necessary to assist a user's mission need.

Mitigation: This risk is partially mitigated. HART data owners review, publish, and manage their own retention schedules. OBIM is in the process of identifying and negotiating any additional retention schedules for facial images and fingerprints.

DHS Privacy Office Recommendation: As a service provider, OBIM should provide expert guidance to data owners regarding the length of time a particular biometric remains valid for comparison. For example, a facial image of a young child may not provide a good match for the same individual when he or she is an adult. OBIM may be able to provide perspective to data owners on how to properly propose retention schedules.

Privacy Risk: There is a risk that latent prints collected at a crime scene from individuals who are not perpetrators may be inappropriately retained.

Mitigation: ISAAs provide that latent prints of individuals who were deemed victims, bystanders, and/or those handling the evidence at criminal or terrorist incidents are not to be retained in HART once they have been identified as such by the providing agency to OBIM.

Privacy Risk: There is a risk that data owners may not delete their records in a timely manner or in accordance with their respective retention schedule.

Mitigation: This risk is not mitigated. Data providers are responsible for deleting their information from HART in accordance with the applicable data retention schedule, using the Delete Encounter Service. OBIM provides training and guidance to HART data providers prior to submitting information to HART, so that they understand how to use the Delete Encounter Service. In addition, DHS oversight offices and data providers may use HART auditing capabilities to ensure implementation of the data retention schedules.

DHS Privacy Office Recommendation: When onboarding a new O/U/S or making changes to an O/U/S, part of the onboarding process should be setting the retention period so records are automatically deleted according to their approved retention period.

DHS Privacy Office Recommendation: OBIM should annually review and document the retention periods (i.e., scheduled) when creating an O/U/S or adding and deleting users to HART and coordinate with Component Privacy Offices on component-specific retention requirements.

DHS Privacy Office Recommendation: OBIM should coordinate with applicable HART users and technical teams to analyze and determine if a separate O/U/S for minors should be maintained and how to effectively include validation checks with the data owners to ensure appropriate access controls.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OBIM shares information as permitted by the data owners and in accordance with the data owners' authorities. 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, intelligence purposes, national defense, 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 ISAAs. DHS Component system-to-system HART users also address HART sharing in their specific privacy compliance documentation.[55]

ISAAs set out the terms for HART users according to their authorities and mission needs. Some HART users may receive a full response to a biometric search request while others receive a limited response. Data providers make the final determination on the type of response and the amount of data a HART user should receive. The content of HART response messages is derived from individual encounters submitted by a variety of HART data providers and is based on agreements to share by those HART data owners.

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

DHS Component SORNs govern the function and use of the biometrics records collected by each Component. Each data owner must determine whether sharing is compatible prior to permitting HART to release the information. DHS/ALL-041 External Biometric Records (EBR) System of Records governs the maintenance and use of biometrics and associated biographic information received from non-DHS entities that are not covered by an existing DHS Component SORNs. Any sharing pursuant to the DHS/ALL-041 EBR System of Records must be pursuant to an ISAA or Arrangement that sets out the terms for sharing and only for specified for 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.

[55] *See* HART Appendix A for additional information on HART authorized users and component specific privacy compliance documentation.

6.3 Does the project place limitations on re-dissemination?

External data owners sign ISAAs that govern the sharing of data retained in HART. ISAAs may include Memorandums of Agreement, Memorandums of Understanding, Implementing Agreements, or other formalized letters describing the purpose, use, and scope of sharing. Those ISAAs include limitations and restrictions on re-dissemination and third-party sharing. These limitations are discussed in Component privacy compliance documentation.[56] As the data steward, OBIM configures HART according to the data owner instructions provided in ISAAs with OBIM and DHS and as described in DHS Component compliance documentation.

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

OBIM retains an accounting of records disclosed outside of the Department. The accounting includes disclosures of both paper-based and electronic records and includes the date, nature, and purpose of each dissemination and disclosure, along with the name and address of the individual or agency to which the disclosure is made. This list of disclosures is retained as part of the accounting requirements for the HART system in order to demonstrate compliance.

HART maintains an audit record in the database for each system message sent to an external agency. Audit logs are maintained by OBIM. Access to audit logs is limited strictly to core O&M personnel. The audit log data is backed up regularly as part of the overall HART database backup and archiving process. OBIM will also share applicable audit records to relevant data owners upon request.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a potential risk that sensitive data may be shared with groups not authorized to receive the data.

Mitigation: This risk is partially mitigated because it is possible unauthorized sharing may still occur with OBIM or DHS Component knowledge. HART incorporates a code-based filtering process according to the data owners' requirements for all information sharing. Prior to using HART, OBIM requires that data providers inform OBIM of all limitations on dissemination in an information access agreement. However, HART does not apply caveats to alert users to special protected class (SPC),[57] refugee, or asylee records, so it is possible that a user permitted to receive SPC information may wrongfully share it. HART employs code to filter information at the organizational, encounter, purpose, or activity types, the person level, or based on DI.

[56] *See* HART Appendix A for additional information on HART authorized users and component specific privacy compliance documentation.
[57] Special protected classes include T, U, and VAWA nonimmigrants, Asylee and Refuges, and Temporary Protected Status. These individuals receive special confidentiality through statute, regulation, or DHS policy.

Configuration settings based on O/U/S filters encounters from responses being returned to the requesting organization.

HART has the ability to either filter or share data from an O/U/S at the request of the data provider or the requestor. Identity level flagging allows a HART authorized user to submit a flag or indicator identifying an individual belonging to a HART defined population, either during the process of encounter enrollment or separately to add/update an existing encounter. This flag acts to filter an individual's entire identity from a requesting O/U/S that is prohibited from receiving identities belonging within that population.

Privacy Risk: There is a risk of sharing HART data with foreign partners, where it is more difficult for DHS to externally impose the same controls that govern the data internally.

Mitigation: These risks are currently not mitigated because HART does not employ caveats. Foreign partners' audit and redress provisions, however, may be used to detect wrongfully shared information and provide redress. DHS PIAs[58] related to sharing with foreign partners lend additional transparency to those external partners' provisions. Additionally, OBIM will audit information sharing in HART to ensure consistency with the ISAAs and other related documentation.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that HART implement caveats on data shared with foreign partners to ensure that they are aware of any restrictions that apply regarding use of the data.

Privacy Risk: There is a risk that HART users who have not been approved will gain access to HART data through third party sharing.

Mitigation: The potential for unauthorized sharing is mitigated by implementing access controls to ensure that only authorized HART users can access the data. HART places limitations on third-party sharing by limiting the amount of data shared based on specific circumstances described in information sharing access agreements.

Privacy Risk: There is a risk of information about special protected class of identities being shared inappropriately.

Mitigation: HART contains information provided by USCIS on millions of applicants and petitioners seeking immigration benefits. Some of the individuals who have applied for and received immigration benefits belong to groups of individuals, referred to as SPCs, because their information is subject to heightened confidentiality provisions by statute or regulation. These confidentiality provisions generally prohibit the disclosure or use of any information about applicants for, and beneficiaries of, certain victim-based immigration benefits, including those

[58] *See* HART Appendix A for additional information on HART authorized users and component specific privacy compliance documentation.

applied for those under 8 U.S.C. § 1367 and other provisions. DHS policy requires SPC records be affixed with caveats so that those organizations that are authorized to receive information protected by 8 U.S.C. § 1367 are aware of the special handling requirements. OBIM does not currently employ caveats but will work with technical teams and DHS Components to implement this requirement in HART and will address progress in subsequent updates to this PIA.

HART shares SPC data only with HART users authorized to receive the information per statute and Department policy. OBIM's business rules prevents the sharing of SPC data with HART users unauthorized to receive that information. Updated configurations to identity level flagging and filtering will allow HART to affix caveats in the future, as appropriate, and filter all encounters associated with an identity. To ensure protection of 8 U.S.C. § 1367 data, HART will filter the entire identity from HART users not authorized to receive the data.

OBIM's policy requires that HART remain updated as those identities that should receive 1367 protections to ensure full compliance with the law. Currently, OBIM receives SPC identities from USCIS through daily encrypted files. OBIM loads the identities into the system and flags the identities as protected to prevent information sharing to unauthorized users. USCIS and OBIM are currently working to automate the transfer of SPC information between systems for real time accuracy.

Privacy Risk: There is a risk that HART may share more data elements than is required for the recipient's purpose for receiving the information.

Mitigation: This risk is partially mitigated. HART has the capability to filter biographic information by data element, and to block biometric responses. However, HART cannot filter by individual biometric modality. Prior to a user using HART services, the user will negotiate an ISAA with OBIM or DHS, as appropriate, and document a common understanding of what information the user can receive from HART and what data HART is allowed to share based on that user's applicable authorities and policies. For internal users, OBIM documents this analysis through the Data Access Request Analysis' (DARA), similar to a Privacy Threshold Analysis (PTA), completed by OBIM and the relevant Component Privacy Office to provide information to the DHS Privacy Office documenting how data is collected, shared by the data owner, will be shared by the data owner and the data manager, and how data protection within HART will be accomplished. OBIM's dedicated privacy analysts also attend technical and operational meetings to discuss or resolve any potential information sharing issues and questions in order to prevent sharing more information than is required for the recipient purpose.

Additionally, OBIM has robust filtering capabilities, implemented through code, that can filter information at the organizational, encounter, and identity/person level based on purpose or activity type in order to only share information that is approved and authorized. OBIM encodes these data filtering authorizations through business rules. This data filtering capability reduces the

likelihood of sharing more data than the user is authorized to receive.

HART also has audit logging capabilities to track data transmission. If HART incorrectly sends more data than is required, OBIM will contact the authorized HART user to request that the HART user delete the information and confirm that the information was deleted. OBIM will also request confirmation that no onward sharing occurred with those specific data elements. In addition, OBIM will immediately notify the relevant Component Privacy Officer or Privacy Point of Contact that data was inadvertently shared, and all relevant information regarding the inappropriate sharing.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that OBIM implement a review cycle to regularly confirm the filters placed on the data with the data owner. This will ensure that information is being shared consistent with the data owner's requirements.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends OBIM implement technology that allows authorized users to read caveats that indicate a record contains special protected class information.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

U.S. citizens, lawful permanent residents, and covered individuals who have covered records under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. All individuals, regardless of citizenship, may obtain access to records consistent with the Freedom of Information Act (FOIA) unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Requesters may indicate the modality for the basis of the search. Individuals may submit a request to OBIM Freedom of Information Act Office: 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.

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

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

U.S. citizens and lawful permanent residents, as well as other covered persons with records covered by the JRA may seek to amend inaccurate records by filing a Privacy Act amendment request under the Privacy Act. Those individuals covered under by the JRA or Privacy Act may direct all requests to contest or amend information to OBIM Privacy, Department of Homeland Security, 245 Murray Lane S.W., Washington, DC 20598-0675. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment.

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 S.W., Washington, DC 20528, USA; 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 the HART system.

Additionally, travelers who wish to file for redress can complete an online application through the through the DHS Traveler Redress Inquiry Program (DHS TRIP)[59] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF). For more information about the types of services DHS TRIP can provide, please visit https://www.dhs.gov/step-1-should-i-use-dhs-trip.

Completing the form online saves processing time and helps prevent data entry errors. After an individual submits a redress form, the individual will receive notification of receipt from DHS TRIP. DHS TRIP will review the redress form and will determine which component/agency will be able to respond most effectively to the submission. When a redress request is related to records maintained in HART, DHS TRIP will coordinate with OBIM. OBIM will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request.

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

Individuals are advised of the procedures for correcting their information in this PIA, or by contacting OBIM Privacy, Department of Homeland Security, 245 Murray Lane S.W., Washington, DC 20598-0675. The redress procedures for travelers are established and operated

[59] *See* DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* www.dhs.gov/privacy.

by DHS through DHS TRIP, which can be accessed at www.dhs.gov/trip.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals, particularly non-U.S. persons, may not be able to correct inaccurate or erroneous information about themselves in HART.

Mitigation: This risk is partially mitigated. For travelers, DHS TRIP provides a redress process through a website that facilitates the submission and processing of redress requests. Any individual can request access to or correction of his or her PII regardless of nationality or country of residence. This process has been described in the DHS TRIP PIA and information is available in multiple places on DHS's public website. Redress requests that come to TRIP in which a traveler encountered difficulties at the point of entry due to information in HART that needs to be modified or updated, are assigned via TRIP to OBIM. OBIM then makes appropriate corrections to the HART record if warranted and makes that notation in TRIP.

Alternatively, any person may submit a request to have a record corrected by contacting OBIM Privacy, Department of Homeland Security, 245 Murray Lane S.W., Washington, DC 20598-0675.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

HART secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. HART is periodically evaluated by OBIM Security to ensure that it complies with these security requirements. HART reviews and provides audit trail logs to monitor, and analyze system transactions, as well as actions and system accesses of authorized HART users. External connections must be documented and approved with both parties' signatures in an ISAA, which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed.

As HART contains data from a variety of sources, collected for a variety of uses, it is necessary to institute controls so that only those individuals with a need to know can access that data. HART has a robust set of access controls, including role-based access and interfaces, which limit individual access to the appropriate discrete data collections. Misuse of the data in HART

is mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity. External connections must be documented and approved with both parties' signatures in an ISAA, which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed.

Additionally, HART records audit trails of changes made to service request processing priorities and changes made to system operating parameters and thresholds. More specifically, HART tracks and logs changes made to business processing rules, accounting of disclosures of PII, all outgoing transaction data, (excluding biometric images) sent as part of an outgoing identity message, authorized and unauthorized actions, deletions, modifications, errors, exceptions, and actions performed by users accessing the data.

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

DHS provides comprehensive privacy training that all DHS personnel are required to attend in person within the first 30 days of their assigned entry on duty. This follows the high-level overview privacy training provided by DHS as part of new-employee orientation. HART users and all employees and contractors supporting its systems, have limited access based on their roles and need to know, and they are trained in the handling of personal information and PII for mission- and non-mission-related data (e.g., human capital and employment data). Annual refresher training is also provided online for existing employees and contractors**.** All DHS and OBIM system users must complete annual refresher training to retain system access.

Additional HART training will be conducted for HART authorized data providers prior to submitting information to HART; system administrators and hardware maintenance personnel; BSC biometric examination personnel; contractor staff providing technical support and HART operations maintenance; and OBIM staff that maintain business rules and system configurations. The OBIM Biometrics Guidelines will also provide basic expectations for accuracy and clarifying information to HART authorized users on the responsible use of HART's biometric services.

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

OBIM has documented standard operating procedures to determine which users have approved access. The minimum requirements for access are documented in the ISAAs between and among DHS and specific users, and in security, technical, and business documentation. In particular, individuals with system access must satisfy suitability requirements based on a need to

know the information based on their job responsibilities and must participate in security and privacy training. Individuals external to DHS must submit a form to OBIM Security in order to gain access to the system. Also, data is filtered based on the HART user, so that one user that has access may have access to more or less data than another user. The HART data provider decides who may have access to the data it provides.

Some contractors may have access to HART data. The extent of access will vary based on the need to fulfill the requirements of the contract under appropriate nondisclosure and use limitations, in addition to requirements enumerated in section 8.1 of this document, and in Component source system compliance documentation. HART ensures that all employees and contractors supporting its systems have limited access based on their roles and that they are trained in the handling of PII.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

DHS Policy requires that ISAAs, including MOUs, MOAs, and Implementing Agreements, are reviewed and approved by DHS oversight offices, including the DHS Privacy Office, as well as the relevant Component Privacy and Security Offices and Component System Owner.[60] DHS Component Privacy Offices, including OBIM Privacy, are required to review technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts, and advise DHS leadership and DHS components on implementing corresponding privacy protections.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: If the security controls for HART are incorrectly configured in the AWS Cloud, then information could be accessible to those not authorized to access it.

Mitigation: OBIM mitigates the risk because OBIM is responsible for all PII associated with HART, whether the information is held in data centers or in a cloud infrastructure, and it therefore imposes strict requirements for safeguarding PII. This includes adherence to the DHS 4300A Sensitive Systems Handbook,[61] which provides implementation criteria for the rigorous requirements mandated by the DHS Information Security Program. Additionally, OBIM requires AWS to segregate HART data from all other third-party data. All contracted cloud service providers must follow DHS privacy and security policy requirements and must follow FedRAMP's

[60] *See* DHS Instruction 047-01-001 Privacy Policy and Compliance (July 2011), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.
[61] *See* 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

strict configurations, security assessments, authorizations, and continuous monitoring requirements.

Privacy Risk: There is a risk that PII may be impacted during the data migration to the AWS U.S. West.

Mitigation: OBIM mitigates this risk through a several key procedures in order to prevent any compromise of data during the migration process. The data migration is continuously monitored by the DHS Chief Information Security Officer and by other security offices within DHS. OBIM uses a secure database backup and recovery enterprise software to migrate data to the AWS cloud.

To ensure data integrity and accuracy during the IDENT-to-HART system migration, parallel operations[62] shall be kept in synchronization and updates shall be made to both systems' data stores in accordance with DHS Fair Information Practice Principles, especially data integrity and accuracy. OBIM will conduct continuous monitoring and analysis to reconcile any discrepancies with the system data. This process involves technical data mapping activities prior to migration and post migration activities and monitoring, which may include identity deduplication, identity consolidation, or data correction.

Additionally, production implementation of HART shall be preceded by the delivery of comprehensive procedures for system operation, maintenance, system administration, data conversion, system transition, and help desk support. The progression of HART from development through integration, testing, and implementation of production operation includes contingency planning, which includes disaster recovery procedures in the unlikely event that reversion to IDENT becomes necessary.

DHS Privacy Office Recommendation: OBIM should report annually on the number and O/U/S source of matches to the HART latent print and probe facial recognition services.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends OBIM develop additional privacy-specific training and material based on a HART user's mission need and job function.

DHS Privacy Office Recommendation: OBIM should provide a mandatory modality-specific training prior to permitting access to HART.

DHS Privacy Office Recommendation: OBIM should establish a governance board made up of OBIM, DHS authorized users and providers, and DHS oversight offices (i.e., DHS Privacy Office, DHS Office of Civil Rights and Civil Liberties, Office of the General Counsel) to ensure that internal and external collection and dissemination of HART records is aligned with the data

[62] Parallel operations are database updates to legacy IDENT and HART that will keep both systems updated and accurate.

owner authorities and policies as set out in the business rules. The governance board should also review whether business rule configurations align with ISAAs with OBIM or agreements or arrangements with DHS that contemplate sharing from the HART system

Responsible Officials

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

Approval Signature

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

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

Appendix A: Authorized Users and Privacy Compliance Documentation

U.S. Customs and Border Protection (CBP)

CBP PIAs: https://www.dhs.gov/privacy-impact-assessments.

- DHS/CBP/PIA-002 Global Enrollment System (GES) and *subsequent updates*;
- DHS/CBP/PIA-006 Automated Targeting System (ATS) and *subsequent updates*;
- DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) and *subsequent updates*;
- DHS/CBP/PIA-012 CBP Portal (e3) to EID/IDENT and *subsequent updates*;
- DHS/CBP/PIA-021 TECS System: Platform;
- DHS/CBP/PIA–024 Arrival and Departure Information System and *subsequent updates*;
- DHS/CBP/PIA-026 Biometric Exit Mobile Program and *subsequent updates*;
- DHS/CBP/PIA-051 Automated Passport Control (APC) and Mobile Passport Control (MPC); and
- DHS/CBP/PIA-056 Traveler Verification Service.

CBP SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/CBP-002 Global Enrollment System, 78 FR 3441 (Jan. 16, 2013);
- DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012);
- DHS/CBP-007 Border Crossing Information (BCI), 81 FR 89957 (Dec. 13, 2016);
- DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 73 FR 77753 (Dec. 19, 2008);
- DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008);
- DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (Nov. 18, 2015); and
- DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (Oct. 20, 2016).

Immigration and Customs Enforcement (ICE)

ICE PIAs: https://www.dhs.gov/privacy-documents-ice.

- DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) and *subsequent updates*;
- DHS/ICE/PIA-003 electronic Travel Document System;
- DHS/ICE/PIA-009 Fugitive Case Management System (FCMS);
- DHS/ICE/PIA-011 Visa Security Program Tracking System and *subsequent updates*;
- DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and *subsequent updates*;
- DHS/USCIS/PIA-020 Alien Criminal Response Information Management System (ACRIMe) and *subsequent updates*;
- DHS/ICE/PIA-049 ICE Parole and Law Enforcement Programs Unit Case Management Systems;
- Forthcoming Biometric Identification Transnational Migration Alert Program (BITMAP) PIA.

ICE SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/ICE 001 Student and Exchange Visitor Information System, 75 FR 412 (Jan. 5, 2010);
- DHS/ICE-006 Intelligence Records System (IIRS), 75 FR 9233 (March 1, 2010);
- DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records, 83 FR 20844 (May 8, 2015);
- DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010);
- DHS/ICE-010 Confidential and Other Sources of Information, 78 FR 7798 (Feb. 4, 2013);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016); and
- DHS/ICE-014 Homeland Security Investigations Forensic Laboratory, 81 FR 45523 (July 14, 2016).

U.S. Coast Guard (USCG)

USCG PIAs: https://www.dhs.gov/privacy-documents-us-coast-guard.

- DHS/USCG/PIA-002 USCG "Biometrics at Sea" System (BASS) and *subsequent*

updates.

USCG SORNs:

- DHS/USCG-031 USCG Law Enforcement (ULE) System of Records, 81 FR 88697 (Dec. 8, 2016).

U.S. Citizenship and Immigration Services (USCIS)

USCIS PIAs**:** https://www.dhs.gov/uscis-pias-and-sorns.

- DHS/USCIS/PIA-007 Domestically Filed Intercountry Adoptions Applications and Petitions and *subsequent updates*;
- DHS/USCIS/PIA-008 Enterprise Service Bus 2 (ESB 2) and *subsequent updates*;
- DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems and *subsequent updates*;
- DHS/ALL/PIA-027 USCIS Asylum Division and *subsequent updates*;
- DHS/USCIS/PIA-045 Deferred Action for Childhood Arrivals (DACA) and *subsequent updates*;
- DHS/USCIS/PIA-048 USCIS International Biometric Processing Services and *subsequent updates*;
- DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS) and *subsequent updates*;
- DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS) and *subsequent updates*; and
- DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting.

USCIS SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017);
- DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016);
- DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016);
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015);
- DHS/USCIS–017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct.19, 2016); and

- DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36950 (July 31, 2018).

Transportation Security Administration (TSA)

TSA PIAs:

- DHS/TSA/PIA-012 Transportation Worker Identification Credential (TWIC) Program;
- DHS/TSA/PIA-020 Security Threat Assessment for Airport Badge and Credential Holders and *subsequent updates*;
- DHS/TSA/PIA-022 Maryland Three (MD-3) Airports;
- DHS/TSA/PIA-026 Alien Flight Student Program;
- DHS/TSA/PIA-041 TSA Pre-Check Application Program and *subsequent updates*; and
- DHS/TSA/PIA-046 TSA OIA Technology Infrastructure Modernization Program and *subsequent updates*.

TSA SORNs:

- DHS/TSA-001 Transportation Security Enforcement Record System, 83 FR 43888 (Aug. 28, 2018);
- DHS/TSA 002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014); and
- DHS/TSA-021 TSA Pre✓™ Applications Program System of Record, 78 FR 55274 (Sept. 10, 2013).

Office of the Chief Security Officer (OCSO)

OCSO PIAs

- DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System (PIV/IDMS) and *subsequent updates*; and
- DHS/ALL/PIA-038 Integrated Security Management System (ISMS) and *subsequent updates*.

OCSO SORN

- DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (Feb. 23, 2010); and

- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

Federal Emergency Management Agency (FEMA)

FEMA PIAs: https://www.dhs.gov/privacy-documents-fema.

- DHS/FEMA/PIA-034 Electronic Fingerprint System and *subsequent updates*.

FEMA SORNs:

- DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (Feb. 23, 2010); and
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

Office of Intelligence and Analysis (I&A)

I&A PIAs

- DHS/ALL-054 Identity Intelligence Biometrics (I2B) Pilot

Department of State (DOS)

- STATE-26 Passport Records, 76 FR 34966 (July 6, 2011);
- STATE-36, Security Records, 83 FR 28058 (Jun. 15, 2018); and
- STATE-39 Visa Records, 83 FR 28062 (Jun 15, 2018).

Department of Defense (DOD)

- A0025-2 SAIS DoD Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009).
- A0025-2 PMG (DFBA) DoD Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015).

Department of Justice (DOJ) and state / local / tribal / territorial law enforcement, Federal, state, local investigative agencies, and

- JUSTICE/INTERPOL-001 INTERPOL-United States National Central Bureau (USNCB) Records System, 75 FR 27821 (May 18, 2010) [Note: records shared with DHS include: law enforcement, intelligence, and national security records];
- JUSTICE/DOJ-005 Nationwide Joint Automated Booking System, 72 FR 3410 (Jan. 25, 2007), 71 FR 52821 (Sept. 7, 2006); and
- JUSTICE/FBI-009 Next Generation Identification (NGI) System of Records (pending DOJ release).

- JUSTICE/FBI-019 Terrorist Screening Records System of Records, 76 FR 77847 (Dec. 14, 2011).

DHS Officer of Policy (PLCY), Program Manager for information sharing with international partners, including Migration 5 partners Canada, New Zealand, Australia, and the United Kingdom. DHS also shares information with Greece and Mexico.

PIAs: https://www.dhs.gov/privacy-documents-department-wide-programs and https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

- Canada – DHS/OBIM/PIA-001 IDENT Appendix B;
- New Zealand - DHS/OBIM/PIA-001 IDENT Appendix B;
- Australia - DHS/OBIM/PIA-001 IDENT Appendix B;
- United Kingdom - DHS/OBIM/PIA-001 IDENT Appendix B;
- Mexico - DHS/OBIM/PIA-001 IDENT Appendix CC; and
- DHS/ALL/PIA-064 Preventing and Combating Serious Crime (PCSC) Agreements - Greece and Italy.

Appendix B: Services

Biometric Services

- **Identify Service** – This service allows a HART authorized user to conduct a biometric search of the full or subset of HART for the purpose of identifying an individual based on submission of a fingerprint, iris, or facial image. In the event of a match, the requestor receives a response that may be filtered to only provide the data that the requestor is authorized to receive, as established by DHS policies, statutes, and regulations and as reflected in ISAAs with OBIM and as described in DHS component-specific compliance documentation.[63] Responses may include biographic information only or all of the biometric modalities associated with the identity.

- **Verify Service** – This 1:1 confirmation service allows a HART authorized user to conduct a biometric search of the full or subset of HART for the purpose of determining whether an individual whose identity is being confirmed is the same person that was previously enrolled in HART with fingerprints and possibly other biometric modalities. The modalities used for confirmation include fingerprints, irises, and face images.

- **External Identify Service** – This service allows a HART authorized user to conduct a biometric fingerprint search of one or more external biometric systems with which HART has established connectivity. HART creates a search request of an external system with the required data in the external biometric systems' specified format. Currently, external systems include DOJ's Next Generation Identification (NGI)[64] system and international Migration5 (M5) partner countries, pursuant to Visa and Immigration Information Sharing Agreements.[65] OBIM is also working with DoD to use this service with DoD's Automated Biometric Information System (ABIS).[66]

- **Compare Service** – This service allows a HART authorized user to confirm a match between a captured biometric image and a biometric image retrieved from a document or a system not currently enrolled in HART. This allows a customer to determine whether an individual whose identity is being confirmed is the same person as the person associated with a document or previously captured biometric. The modalities that could be used for biometric comparison

---

[63] *See* Appendix A for list of authorized users.
[64] See *Memorandum of Understanding among the Department of Homeland Security the Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division and the Department of State Bureau of Consular Affairs for Improved Information Sharing Services*, Jul 1, 2008.
[65] Migration Five (M5) partner countries include Canada, Australia, New Zealand, United Kingdom, and the United States. Additional discussion on DHS international information sharing, *available at* www.dhs.gov/privacy.
[66] See *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activates*, January 2016 Update.

currently include fingerprints and face images but could be expanded in the future to additional biometric modalities.

- **Latent Search Service** – This service allows a HART authorized user to submit latent fingerprints to be searched against the HART full gallery and the ULF in order to identify potential candidates for comparison. Top scoring candidates that are shareable per HART's data filtering rules are returned either to the BSC or the user for manual review and adjudication.

Biographic Services

- **PreVerify** – The service allows a service requestor to submit a personal identifier[67] to determine if HART has previously encountered the individual. This occurs when the authorized user does not know if HART has record of an encounter with the individual. If HART has not encountered the individual, then the system will send a response to the authorized user requesting biometric information. If HART does find a previous encounter, then the service will suggest the type of HART service to perform in the additional encounter. The HART user can also decline to provide additional information on the user based on the HART user's operational protocol and authority. If permitted by established ISAAs, the PreVerify Service will also indicate any derogatory information (DI) pertaining to the matched identity. Facial images may also be returned in the response, if appropriate under the collector's legal authority, policies, and rules for sharing.

- **Retrieve Identity** – This service allows a HART authorized user to verify that the biometric collected matches the biometric in HART for that particular person. For example, an authorized user may submit a biometric and unique identifier (may include A-Number, Fingerprint Identification Number (FIN), Known Traveler Number (KTN)) to match against an identity in HART. HART then searches the database and returns a response in accordance with an ISAA and as described in DHS component specific compliance documentation.[68] This service may return biographic and biometric images in the match response.

- **Retrieve Encounter** – This service allows a HART authorized user to retrieve a specific encounter from HART using one or more HART encounter unique identifiers.[69]

- **External Retrieve Identity** – This service allows a HART authorized user to retrieve

[67] Personal Identifiers in HART may include: A-Number; Australian Certificate of No Impediment to Marriage (CNI), Canadian Unique Client Identifier (UCI), Civil Record Number (CRN), Foreigner Identifier (FRI); Great Britain Unique Person Identifier (GBR-UID), HART EID, Individual Identifier (IID), New Zealand - Claimed Identity ID (CIID); Social Security number (SSN/SOC); State Identification (SID); USCIS Account Number (USCISACCT); USCIS Z Number (Z-Number); USPass Identifier (USP); and Known Traveler Number (KTN).
[68] *See* Appendix A for a list of authorized users.
[69] Encounter Unique Identifiers in HART may include: A-Number; Australian Certificate of No Impediment to Marriage (CNI), Canadian Unique Client Identifier (UCI), Civil Record Number (CRN), Foreigner Identifier (FRI); Great Britain Unique Person Identifier (GBR-UID), Individual Identifier (IID), New Zealand - Claimed Identity ID (CIID); Social Security number (SSN/SOC); State Identification (SID); USCIS Account Number (USCISACCT); USCIS Z Number (Z-Number); USPass Identifier (USP); and Known Traveler Number (KTN).

identity data from an external system using a unique identifier that exists in that system. HART will return the external system's matching identity or encounter information.

- **Retrieve Referrals** – This service allows a HART authorized user to receive information on individuals referred to Secondary Inspection[70] for additional screening at designated ports of entry.

Identity Management Services

- **Add New Biometric Modality** – This service allows a HART authorized user to add a new biometric modality to an existing identity or encounter. For example, irises can be added to a fingerprint-only identity upon a successful verification of fingerprints.

- **Add Disposition** – This service allows a HART authorized user to indicate the result of a particular encounter. For example, this could occur when a traveler is admitted at a U.S. Customs and Border Protection Primary entry point or referred to Secondary Inspection for further screening.

- **Adjudicate Derogatory Information** – This service allows a HART authorized user to indicate whether a piece of DI should be added or removed (demoted) based on a Component's authorized demotion rules and procedures. The demotion rules and procedures are established and outlined in the applicable ISAA or other technical specification documentation.

- **Add and Delete Identity Flag** – An identity flag is used to filter the identity of an individual belonging to a population defined under law[71] or by an authorized user as requiring specialized treatment, either during the process of encounter enrollment or at a later date. This Add and Delete Identity Flag Service allows a HART authorized user to add or delete an identity flag to an existing biometric encounter in HART. OBIM uses the Identity Flag to assist in satisfying the legal requirement that prohibits the disclosure of certain identities under certain circumstances about applicants for, and beneficiaries of, certain victim-based immigration benefits.

- **Delete Encounter** – This service allows a HART encounter owner, or other authorized HART user, to delete one or more biometric encounters owned by that HART user. This service is predominantly used by HART users to adhere to National Archive Records (NARA) records retention schedules.[72]

---

[70] Secondary inspection is the interview area at a Port of Entry where U.S. Customs and Border Protection (CBP) officers conduct additional research on an individual traveler in order to verify information without causing delays for other arriving individuals to the United States. For additional reference, see Appendix A for additional CBP compliance documentation.

[71] DHS prohibits this disclosure of certain identities under certain circumstances for defined populations including about applicants for, and beneficiaries of, certain victim-based immigration benefits, including those applied for those under Title 8 U.S.C. § 1367 and other provisions. *See* Section 6.5 for additional discussions.

[72] The National Archives and Records Administration (NARA) is charged with providing guidance and assistance

- **Add Encounter Comments** – This service allows a HART authorized user to add a comment to an encounter.

- **Record Issuance** – This service allows a HART authorized user to associate a travel document, benefit, or credential with an existing biometric encounter. This also allows other authorized users that subsequently encounter the same individual to see that the issuing organization granted the individual a travel document, credential, or benefit.

- **Latent Maintenance** – This service allows a HART authorized user to submit a request to OBIM to add to or delete a latent fingerprint from the ULF.

- **Derogatory Information Management Services:**
    - **Add Derogatory Information** – This service allows a HART authorized user to add DI to an existing biometric encounter.
    - **Deactivate Derogatory Information**[73] – This service allows a HART authorized user to indicate whether a piece of DI should become inactive or be demoted based on authorized demotion rules and procedures. Deactivating a particular DI demotes the DI.
    - **Delete Derogatory Information** – This service allows a HART authorized user to permanently delete a piece of DI associated with an existing biometric encounter in HART.
    - **Confirmations -** The HART system will generate confirmations back to the authorized user once HART completes these automated requests based on the HART user's defined business rules. Note that only an authorized user can request to delete their own DI.

OBIM Internal Services

- **Internal Management Request** –This service is comprised of the Identity Merge and Identity Separation requests. It allows a HART authorized user to submit a request to HART and based on an examiner's review, the examiner will separate two or more biometric identities that have either been erroneously commingled by the system as a single identity, or merge two or more biometric identities that have erroneously enrolled as separate identities. HART will not automatically merge or separate identities.

---

with respect to records management within the Federal Government. *See* Section 1.4 and Section 5.1 for additional discussion on data retention.

[73] DI may include information submitted from the Department of Defense (DoD), the Federal Bureau of Investigations (FBI), the Department of State, INTERPOL, international country partners, and DHS Components, specifically U.S. Immigration and Customs Enforcement (ICE), and CBP. See Section 2.1 for list of DI data elements.

In addition, HART data providers may submit requests to HART to separate or merge biometric identities to enable accuracy of the information. Upon the data provider's request, BSC examiners review the information, and if appropriate, the examiner will separate two or more biometric identities that have either been erroneously commingled by the system as a single identity, or merge two or more biometric identities that have erroneously enrolled as separate identities.

- **Image Management** – This service allows a HART authorized user to request an OBIM examiner make corrections to labeling or enhance images. Corrections include adjust mirrored images and correcting image reversals. Image labeling includes labeling finger position, documenting the left or right iris, or documenting missing biometrics. An examiner makes the requested change and provides the result back to the service requestor.

Notification Services

- **Notification Subscription Services** – The Notification Subscription Service includes the ability for an authorized HART user to receive permissible notifications about specific activity pertaining to a specific biometric identity. Notifications are sent when there are changes to an identity's history or status, or for enrollment changes due to system maintenance. HART users may subscribe to the following notification services:
    - **Encounter Notification** – Encounter notification informs a subscriber that a new encounter has been assigned to an identity stored in HART.
    - **DI Update Notification** – This service informs a subscriber whenever DI changes on a subscribed identity.
    - **Identity Flag Update Notification** – The identity flag notification informs a subscriber when an identity flag changes on a subscriber's identity.
    - **Person Identifier Notification** – This service notifies a subscriber when a unique identifier ((e.g., A-Number) in HART has changed.
    - **Document Issuance Notification** – This service informs a subscriber when a document was issued (e.g., US visa) by the United States and is associated to an existing encounter.
    - **Encounter Assignment Notification –** This service informs a subscriber that a new encounter is assigned in HART.[74]

[74] Encounter Assignment Notification may occur when an encounter is created as the result of a person entering the country; an encounter created as the result of a person exiting the country; an encounter created as the result of a person applying for a document (such as a visa).

APPENDIX C: OBIM HART Inc. 1 PIA Glossary

American National Standards Institute / National Institute of Standards and Technology, Information Technology Laboratory (ANSI/NIST- ITL)	"A private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The mission of ANSI is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and safeguarding their integrity."- International Biometrics and Identity Association (IBIA)[75] "The Information Technology Laboratory (ITL), one of six research laboratories within the National Institute of Standards and Technology (NIST), is a globally recognized and trusted source of high-quality, independent, and unbiased research and data. As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, ITL's research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology."- NIST[76]
Biographic Information	*See Characterization of the Information section of this PIA for listing of biographic data elements in HART.*
Biometric	• "measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual"- DHS[77] • "A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris can samples are all examples of biometrics."- NIST[78]

[75] See IBIA glossary *avaliable at* https://www.ibia.org/biometrics/glossary.
[76] See NIST/ITL website *avaliable at* https://www.nist.gov/itl/about-itl.
[77] See DHS Lexicon Terms and Definitions, *available at* https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf.
[78] See NIST glossary, *available at* https://csrc.nist.gov/glossary/term/biometric.

Biometric Match/Matching	• "Biometric matching is the process of comparing biometric information against a previously stored template(s) and scoring the level of similarity." - NIST[79] • "A determination that two samples correspond to the same source based on some level of computer-evaluated similarity. Does not inherently imply that the probe and candidate are the same person." - FISWG[80]
Biometric Modality	Biometric modality is the type or class of biometric that is the subject of measurement, i.e., face, fingerprint, iris, voice, etc. *See HART Features and Capabilities section for additional reference.* "This is a type or class of biometric system. Any measurable biological or behavioral characteristic can be a biometric modality."- NIST[81]
Business Rules	System configurations that reflect the permissions of each HART authorized user as agreed to in ISAAs with OBIM or DHS and as described in DHS Component-specific privacy compliance documentation. Business rules can also be configured to block sharing of biometric data in response to a query. *See HART Data Filtering section for additional reference.*
Contextual Data (Factors)	Contextual factors may include the demographic of the population (e.g., age, sex, race), camera quality, the rate of throughput, lighting, distance, and size of the database, as well as other factors determined by a user's operational mission. *See HART Biometrics Modalities & Services section for additional reference.*
Derogatory Information	Information which potentially justifies unfavorable suitability, fitness, or security adjudication and such information may prompt a request for additional investigation or clarification for resolution of an issue. Each HART user determines which information may be derogatory for their specific purposes. *See HART Data Filtering section for additional reference.*

[79] *See* NIST glossary *available at* https://csrc.nist.gov/glossary/term/match-matching.
[80] *See* FISWG glossary *available at* https://fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[81] *See* biometric modality definition *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf.

Presentation Attacks	"Also commonly known as spoofing, is the"[p]presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system." - NIST[82]
Encounter Identification Number (EID)	While the fingerprint and basic biographic information are initially enrolled and assigned a Fingerprint Identification Number (FIN), every subsequent encounter receives a new HART-generated Encounter Identification Number. *See HART Biometric Modalities & Services section for additional reference.*
Encounter	Collection of biometrics, biographics, and associated data collected at a given place and time. *See HART Biometrics Modalities & Services section for additional reference.*
Enrollment	• "The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison." -IBIA[83] • The first time an individual is registered in a biometric system. During the enrollment, the system captures and stores an individual's biometric information. *See HART Biometrics Modalities & Services section for additional reference.*
Facial Image	Facial images in HART are limited to those captured from a photo or video that can be used for biometric matching purposes. S*ee HART Biometric Modalities and Services section for additional reference.*
False Acceptance Rate (FAR)	• The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. This statistic is expressed as a percentage and is used to measure biometric performance of verification or identification. The FAR is used during testing and tuning the biometric algorithm. Both the FAR and TAR (see definition below) must be considered and tested in relation to each other. *See Footnote 53 for additional reference.* • "Proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed."- NIST[84]

[83] *See* IBIA glossary *available at* https://www.ibia.org/biometrics/glossary.
[84] *See* NIST glossary *available at* https://csrc.nist.gov/glossary/term/false-accept-rate.

False Rejection Rate (FRR)	"Proportion of verification transactions with truthful claims of identity that are incorrectly denied." -NIST.[85]
HART Data Provider	HART data providers upload and store biometric information in HART. *See Users and Data Providers section for additional reference.*
HART Users	HART authorized users are U.S. Federal, foreign, or international governmental agencies, as well as state, local, tribal, and territorial law enforcement agencies that have entered into ISAAs with DHS for biometric identification and analysis services. All HART authorized users can query the HART database. *See Users and Data Providers section for additional reference*.
IXM	A method of communicating with HART in Extensible Markup Language (XML) message format. The XML-based format is designed to perform specific operations (HART Services as described below) for the HART user or data provider. This allows the HART user or data provider to send or receive information to HART. *See Footnote13 for additional reference.*
Latent Print	• "An impression or image of friction ridge skin left on a surface." - NIST[86] • "A fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger." - IBIA[87]
Liveness Detection	"A technique used to ensure that the biometric sample submitted is from an end user. A liveness detection method can help protect the system against some types of spoofing attacks."- IBIA[88]
One-to-Many	"Of or relating to biometric identification in which submitted feature data is compared with that of all enrolled identities." - NIST[89]

[85] *See* NIST glossary *available at* https://csrc.nist.gov/glossary/term/false-reject-rate.
[86] *See* latent print definition *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf.
[87] *See* IBIA glossary *available at* https://www.ibia.org/biometrics/glossary.
[88] *See* IBIA glossary at https://www.ibia.org/biometrics/glossary.
[89] *See* NIST glossary *available at* https://csrc.nist.gov/glossary/term/One_to_Many.

One-to-One	"Of or relating to biometric verification in which submitted feature data is compared with that of one, claimed, identity." NIST[90]
Query	An automated or manual search against OBIM's biometric holdings. HART users can submit automated searches via system-to-system connections. Manual searches, by contrast, require users to submit queries to the OBIM Biometric Support Center for processing. *See Users and Data Providers section for additional reference.*
Special Protected Class (SPC)	Individuals whose information is protected by Title 8, United States Code (U.S.C.), Section 1367, confidentiality and prohibited source provisions (relating to applicants for and beneficiaries of Violence Against Women Act (VAWA), T visa, or U visa protections in accordance with 8 U.S.C. 1367(d) and Section 810 of the Violence Against Women Reauthorization Act of 2013, including VAWA self-petitioners and VAWA cancellation or removal applicants.
Spoofing	"In a biometric system, the process by which an imposter intentionally attempts to be recognized as another person or intentionally attempts to be missed as an existing identity in the gallery." - FISWG[91]
Threshold	"Values used to establish concrete decision points and operational control limits to trigger management action and response escalation." - NIST[92]
True Acceptance Rate (TAR)	"This is the probability that a system will verify the identity of a legitimate claim. The performance statistic for verifying the identity is the probability of correct verification or true acceptance rate (TAR)." - NIST[93]

[90] *See* NIST glossary *available at* https://csrc.nist.gov/glossary/term/One_to_one.
[91] *See* FISWG gallery *available at* https://fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[92] *See* NIST glossary *available at* https://csrc.nist.gov/glossary/term/Thresholds.
[93] https://www.govinfo.gov/content/pkg/GOVPUB-C13-1ba4778e3b87bdd6ce660349317d3263/pdf/GOVPUB-C13-1ba4778e3b87bdd6ce660349317d3263.pdf.