Privacy Impact Assessment

for the

Office of Biometric Identity Management (OBIM) - National of Institute Standards and Technology (NIST) Data Transfer

DHS Reference No. DHS/OBIM/PIA-005

May 16, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS or the Department) Office of Biometric Identity Management (OBIM), through the Automated Biometric Identification System (IDENT), which will be replaced with the Homeland Advanced Recognition Technology System (HART), is the Congressionally designated lead provider of biometric identity services for the Department. The National Institute of Standards and Technology (NIST)[1] is a non-regulatory federal agency within the U.S. Department of Commerce that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. DHS and NIST, in support of efforts to increase the accuracy of OBIM's biometric matching, entered into an Interagency Agreement (IAA or Agreement) for research, development, testing, and evaluation activities. Through engagement with NIST, OBIM can address, focus, and enhance its internal biometric test and evaluation capabilities, techniques, and methodologies. OBIM is conducting this Privacy Impact Assessment (PIA) to discuss the privacy risks and mitigations surrounding the transfer of operational data to NIST.

Introduction

OBIM's mission is to provide DHS and its mission partners with biometric identity services that enable informed national security and public safety decision making by producing accurate, timely, and high assurance biometric identity information. OBIM's mission partners capture biometric data and submit the biometrics and associated biographic records to IDENT[2]/HART[3] to support DHS missions and functions. IDENT (and its replacement, HART) is a centralized DHS-wide biometric database that also contains limited biographic and encounter history information. Once OBIM completes HART development and technical configurations, HART will replace IDENT as the Department's biometric system of record. HART will store and process biometric information (e.g., fingerprints, iris scans, facial images (including a photo)) and link these biometrics with biographic information pursuant to the data owner's authorities and policies for use, retention, and sharing of information.

NIST supports the government-wide effort to increase the collection of good quality biometrics, to see that the data collected is appropriately shared with other agencies, and to make

[1] *See* https://www.nist.gov/.
[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/NPPD/PIA-002 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.
[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR HOMELAND ADVANCED RECOGNITION TECHNOLOGY (HART), DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

sure biometric systems are accurate and interoperable. NIST's activities include research on the various biometric modalities: fingerprint, face, iris, voice, DNA, and multimodal; standards development at the national and international level; and technology testing and evaluation. NIST research provides state-of-the-art technology benchmarks and guidance to industry and U.S. Government agencies that depend upon biometrics recognition technologies.

Seeking to improve the collection and use of biometrics, DHS and NIST entered into an Interagency Agreement for research, testing, evaluation, and development activities to enhance the accuracy of OBIM's biometric matching. NIST scientists and technicians will support IDENT/HART's future facial recognition capability and fingerprint, iris, and other biometrics applications through the development of biometric standards for transmission and quality evaluation, which ensures consistency in data definition and conformance interoperability between systems.[4] Data definition and interoperability between biometric systems will support and enhance the Department's national and international operations, including more effective enforcement of U.S. immigration laws.

Assuring accuracy in IDENT/HART biometric matching is one of the core goals of OBIM. By identifying and minimizing matching errors in day-to-day transactional processing, OBIM can provide integrity assurance to users of IDENT/HART. From previous studies and biometric evaluations, NIST has established that the collection and use of high-quality biometric data will result in accurate matching against biometric repositories.[5] The sharing of data stored in IDENT allows NIST scientists and statisticians to conduct tests and evaluations for data quality and accuracy across a broad set of statistically significant sub-groups, based on such phenotypes as age, race, and gender, as well as contextual conditions of the collection, such as the country of document issuance from which the biometric was collected and the location, date, and time of collection, which may affect matching reliability. These tests and evaluations will provide insight to DHS on positive matching configurations and identify areas for improvement in optimal face capture technology, face and fingerprint matcher tuning,[6] and DHS current and future algorithms.[7] The continual improvement of OBIM's biometric matching will result in lower risk of errors and is essential both for mission operators and compliance with DHS privacy policies.

Per the Interagency Agreement, NIST will use DHS collected facial images to evaluate available and emerging facial recognition technology for potential use by DHS Components. This

[4] Relevant systems and applicable Privacy Compliance Documentation are listed in Appendix A.
[5] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, BIOMETRIC PROJECTS AND PROGRAMS, *available at* https://www.nist.gov/programs-projects/biometrics.
[6] Tuning involves testing false match rates and false non-match rates, and then making sure those data results are performing optimally with the matcher algorithm.
[7] An algorithm is a clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result. *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, COMPUTER SECURITY RESOURCE CENTER GLOSSARY, *available at* https://csrc.nist.gov/glossary/term/Algorithm.

effort is being initiated to develop a face image quality standard and provide technical support for biometric matcher tuning, with NIST providing the expertise to assist OBIM in obtaining reliable match results.

In addition, OBIM plans to work with NIST to assess fingerprint matching accuracy. NIST will evaluate fingerprint related algorithms and match performance, conduct fingerprint quality analysis, and examine effects and mitigation of fingerprint overlap on matching accuracy. The continual improvement of OBIM's biometric matching will result in lower risk of errors for mission operators, who rely on the accuracy of OBIM's matching services. Decision making by mission operators based on more accurate matching also results in improved privacy, civil rights, and civil liberties protections for individuals.[8]

Per the Statement of Work (SOW), NIST will assess, evaluate, and inform test environment and test set design plans and approaches to ensure that overarching biometric performance evaluations follow best practices and generate repeatable results. NIST routinely performs evaluations of facial recognition technologies. One of the evaluations, the Face Recognition Vendor Test (FRVT),[9] provides independent evaluations of commercially available and prototype face recognition technologies. These evaluations are designed to provide U.S. Government and law enforcement agencies with information to assist them in determining where and how facial recognition collection technology can best be deployed. NIST will perform the Face Recognition Vendor Test on DHS information provided from IDENT. Face Recognition Vendor Test results can inform DHS in creating optimal face image collection guidelines.

This project involves the transfer of operational DHS information from IDENT to the controlled NIST Biometric Research Laboratories BRL. NIST will evaluate how biometric algorithms ("matchers") perform against DHS information from IDENT in the Biometric Research Laboratories environment. NIST will test and report on the overall quality of facial images and fingerprints in IDENT; how various algorithms perform with information maintained in IDENT using repeatable and generally accepted accuracy measurements;[10] and the strengths and weaknesses that may exist in IDENT's current or developmental algorithms. Per the Statement of Work, NIST will deliver two types of reports: (1) Reports on specific OBIM tasks supporting internal evaluations; and (2) Reports related to interagency studies. NIST will suggest updates to OBIM on relevant industry biometric standards and best practices for DHS adoption. NIST will also assist with the development of facial image, fingerprint, and iris quality capture standards.[11]

---

[8] Currently, OBIM does not plan to have NIST conduct iris or other biometric modality testing.
[9] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FACIAL RECOGNITION VENDOR TEST QUALITY ASSESSMENT, *available at* https://pages.nist.gov/frvt/html/frvt_quality.html.
[10] An Introduction to Evaluating Biometric Systems *available at* https://www.nist.gov/publications/introduction-evaluating-biometric-systems. Additionally, ISO/IEC 19795 Biometric Performance Testing and Reporting has information regarding Biometric testing.
[11] *See* supra note 9.

The DHS Privacy Office has recommended that OBIM develop Biometrics Guidelines to provide basic expectations for accuracy and clarifying information to HART authorized users on the responsible use of HART's biometric services.[12] This work is being undertaken to fulfill that recommendation.

OBIM will inform DHS Components of specific face image quality vectors impacting face recognition, such as pose, illumination, and expression, via the DHS Face Image Quality Standard (FIQS) Working Group (WG) and the IDENT/HART onboarding process. OBIM's Biometrics Guidelines will provide basic expectations on accuracy and the responsible use of OBIM's identification and analysis activities to both users and data providers. OBIM's biometrics experts will develop a Face Image Capture Guideline with DHS Component representatives and coordinate through the Face Image Quality Standard Working Group. OBIM has invited interagency partners to participate in the DHS Face Image Quality Standard Working Group and will be coordinating with DHS Science & Technology (S&T) to disseminate Face Image Capture Guidelines.

NIST will provide OBIM information from the Face Recognition Vendor Test matcher performance analysis and image quality assessment study. Both resources are relevant for OBIM and DHS Components because the results are based on DHS face images maintained in IDENT. NIST is providing performance accuracy measurement results that are from a commercial matcher. While NIST does not have the same commercial matcher that DHS Components use in production, the results are the closest representation of the OBIM matcher face recognition performance. The NIST Face Recognition Vendor Test study provides analysis results of face image quality tools submitted to NIST for evaluation. The results of this analysis are based on production DHS face images. This analysis will help with the selection of face image quality assessment tools for use by DHS. Both performance accuracy data and image quality assessment data will assist in the development of future face image capture technologies.

Transfer of Data

In April 2019, OBIM transferred facial images, anonymized unique identifiers (Encounter Identification (EID) only), year of birth, country of birth, nationality, citizenship, gender, and other metadata to NIST to support evaluation efforts. The facial images included in this data transfer were captured by DHS Components, specifically, U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS).[13] During this data transfer, OBIM sought to minimize risk by only including the associated biographic data elements that were needed for the testing and evaluation, such as gender, year of birth, and nationality. Names and several other personal identifiers were excluded

[12] *See* supra note 3.
[13] *See* Appendix A for users and additional information on DHS Component compliance documentation.

from the data transfer. The Encounter Identification number that would tie the data back to the data in IDENT was included, however, it was anonymized. Additionally, before sending the data to NIST, OBIM filtered out special protected class (SPC)[14] data using OBIM's identity level filtering. OBIM encrypted the data during the transfer to NIST.

OBIM plans to transfer fingerprints, anonymized unique identifiers (Encounter Identification only), year of birth, country of birth, nationality, citizenship, gender, and other metadata to NIST to support the fingerprint evaluation efforts mentioned above. The fingerprints will include those captured by DHS Components; specifically, ICE, USCIS, CBP, and Transportation Security Administration (TSA). OBIM will not send any data collected by foreign partners to NIST. During this data transfer, OBIM will minimize the risk by only including the associated biographic data elements that are needed for the testing and evaluation. Names and several other personal identifiers will be excluded from the data transfer. As stated earlier, the Encounter Identification that will tie the data back to the data in IDENT will be included, however, it will be anonymized. Additionally, as in the case of facial images sent earlier to NIST, OBIM will filter out special protected class data using identity level filtering. Data will be encrypted during the transfer as well. The data will be encrypted on removable drives with on-device FIPS compliant encryption. As part of this testing and evaluation effort, OBIM may need to send additional facial images or fingerprints in the future to NIST; to build upon and augment the analysis. Any additional transfers would be done in the same manner described in this Privacy Impact Assessment.

With these protections in place, sharing this data with NIST for testing and evaluation will ultimately improve DHS operations by improving data quality and integrity. Improvements to data quality and integrity will reduce matching error risks, consistent with OBIM's mission while protecting individuals' privacy. Currently, OBIM does not plan to have NIST conduct iris or other modality testing but will update this Privacy Impact Assessment if OBIM's plans change.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[15] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure

[14] *See* U.S. CITIZENSHIP AND IMMIGRATION SERVICES, POLICY MANUAL VOLUME I, PART A, CHAPTER 7 (current as of September 15, 2020), *available at* https://www.uscis.gov/policy-manual/volume-1-part-a-chapter-7.
[15] 5 U.S.C. § 552a.

that information contained in Privacy Act systems of records is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[16]

In response to this statutory obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[17] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208,[18] and the Homeland Security Act of 2002, Section 222.[19] This Privacy Impact Assessment examines the privacy impact of the OBIM transfer of data from IDENT to NIST as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a System of Records Notice (SORN) and PIA, as appropriate.

OBIM is publishing this Privacy Impact Assessment to provide notice about the sharing of information stored in IDENT with NIST to allow NIST scientists and statisticians to conduct tests and evaluations across a broad set of statistically significant sub-groups of DHS-maintained operational data. The purpose of this sharing is to ultimately improve DHS operations and biometric data matching. In addition, NIST published a high-level summary report of the findings that references the use of DHS-data and made it available on its website.[20]

Both the Face Recognition Vendor Test results and Face Image Quality Standard Working Group will help DHS Components determine the optimal face image capture achievable with the image capture technology that may include different devices used for different operational scenarios. DHS will evaluate which commercial off the shelf (COTS) software and/or government off the shelf (GOTS) software performs best with the face images collected to meet existing DHS Component requirements, and the optimal photo image captures, so that DHS Components may

[16] 6 U.S.C. § 142(a)(2).
[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVCY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[18] 44 U.S.C. § 3501 note.
[19] 6 U.S.C. § 142(a)(4).
[20] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FACE RECOGNITION VENDOR TEST PART 3: DEMOGRAPHIC EFFECTS (2019), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. Additional reports may be published based on NIST's ongoing analysis.

then make adjustments and improvements if needed. NIST uses the data (images and descriptive data to include biographic, non-biometric, and metadata) to conduct comparative analysis based on subjects' phenotype (e.g., age, gender, race). DHS is obligated to use the operational data to ensure that the resulting analysis is applicable to the DHS mission operator context.

NIST personnel are the evaluators and subject matter experts (SME) for the Face Recognition Vendor Test study. As mentioned on NIST's website, face recognition algorithm vendors send their algorithms to NIST to participate in the Face Recognition Vendor Test. At no time will external vendors and/or contractors be involved in the testing and evaluation of DHS data. Only cleared NIST personnel, in the secured Biometric Research Laboratories, will perform test and evaluation tasks. These tasks involve matching samples of DHS face images using the collection of Face Recognition Vendor Test vendor-submitted algorithms. Vendors do not have any access to the data. IDENT transferred facial images, anonymized unique identifiers (Encounter Identification only), year of birth, country of birth, nationality, citizenship, gender, and other metadata to NIST to support evaluation efforts. The facial images and fingerprints are captured by DHS Components (and other stakeholders) during the fulfillment of their missions, and transferred to OBIM for matching, storing, and sharing. OBIM (at this time) does not monitor completeness of data enrolled into IDENT. Anomalies in legacy systems that provided source data to IDENT could result in incomplete data. OBIM plans to send biometric and limited biographic data from certain DHS Components (as described on page 5 above) to NIST while ensuring privacy and security controls are maintained on the data throughout the full lifecycle of its use. OBIM will not send any data collected by foreign partners to NIST.

NIST has published a high-level summary report[21] of the findings that references the use of DHS data, without disclosing any personally identifiable information or details of Component-specific data, and it is available on the NIST website. As NIST further studies facial images and fingerprints, they will publish additional high-level summary reports that also will not disclose any specific personally identifiable information or identify any details of Component-specific data.

This Privacy Impact Assessment, in addition to the HART Privacy Impact Assessment [22] and the Enterprise Biometrics Administrative Records (EBAR) System of Records Notice (SORN),[23] provides general notice that an individual's personal information may reside in IDENT/HART and may be used for testing and evaluation. Notice is also provided through the publication of Privacy Impact Assessments and System of Records Notices on the underlying systems of original collection and the information shared from those systems.[24] If required by law or policy, DHS Components, as well as external partners that submit information to IDENT and

[21] *See* supra note 20.
[22] *See* supra note 3.
[23] *See* DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (March 20, 2020), available at https://www.dhs.gov/system-records-notices-sorns.
[24] *See* Appendix A.

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 if it will be stored in the upcoming HART system.

Privacy Risk: There is a risk that an individual will be unaware their information was sent by DHS to NIST.

Mitigation: This risk is partially mitigated. DHS is publishing this Privacy Impact Assessment to provide transparency of this initiative and associated information sharing activities. However, this Privacy Impact Assessment is being published after the initial transfer of facial image data in 2019.

Nevertheless, at the time biometrics are originally collected by DHS Components, individuals are provided notice of potential information sharing within and beyond DHS. OBIM itself is unable to provide identical and specific notification to individuals in each data set that falls under the Agreement. Transparency into the programs and biometric collections associated with this Agreement, including any associated privacy risks and mitigations, may be found in DHS Component Privacy Impact Assessments and System of Records Notices at www.dhs.gov/privacy. The data in IDENT is collected, processed, and stored consistent with the applicable authorities of the agencies and programs that originally collected the data. Authorities are described in the Privacy Impact Assessments, System of Records Notices, or other materials for each of these programs. DHS System of Records Notices contain a routine use that allows for sharing data with experts performing or working on a service or cooperative agreement, or assignment for DHS, when necessary, to accomplish an agency function. Although each individual may not be aware that their data is shared with NIST, such sharing will have no direct impact on any individual's interactions with DHS (e.g., for benefit applications or credentialling) as NIST will not use the data for operational purposes.

2. Principle of Individual Participation

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

No new data is collected for this project; OBIM is using data previously collected by DHS Components. DHS Components collect the information according to their authorities and missions. IDENT does not seek consent from individuals prior to sending information to NIST, as IDENT is merely a data repository. Because IDENT operates as the DHS back-end biometric identification system and repository, individuals should consult other DHS program Privacy

Impact Assessments for specifics on opportunities to provide or withhold consent.[25] OBIM is sharing data with NIST to improve the integrity and accuracy of biometric matching within IDENT. This sharing is covered under a routine use in DHS System of Records Notices that allows for sharing data with experts performing or working on a service or cooperative agreement, or assignment for DHS, when necessary to accomplish an agency function.

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 online at https://www.dhs.gov/freedom-information-act-foia or to OBIM Freedom of Information Act Office: The Privacy Office, Office of Biometric Identity Management, U.S. Department of Homeland Security, 2707 Martin Luther King Ave., SE, STOP-0655, Washington, D.C. 20528-0655.

If an individual is dissatisfied with the response to their redress inquiry, then they may 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, U.S. Department of Homeland Security, Mailstop 0655, 2707 Martin Luther King Ave, S.E., Washington, D.C. 20528, USA; or by fax: 1-202-343-4011. As with access, amendments may be limited pursuant to applicable Privacy Act exemptions asserted by DHS for IDENT/HART.

Furthermore, travelers who wish to file for redress can complete an online application through the DHS Traveler Redress Inquiry Program (DHS TRIP)[26] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF). Additional information about the types of services the DHS Traveler Redress Inquiry Program can provide is available at https://www.dhs.gov/step-1-should-i-use-dhs-trip.

Individuals can also find information regarding NIST access and correction procedures by following the NIST process at https://www.nist.gov/foia.[27]

Privacy Risk: There is a risk that individuals, particularly non-U.S. persons, may be unable to correct inaccurate or erroneous information about themselves in IDENT/HART.

---

[25] *See* Appendix A.
[26] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM (TRIP), DHS/ALL/PIA-002 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[27] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FREEDOM OF INFORMATION ACT, *available at* https://www.nist.gov/foia.

Mitigation: This risk is partially mitigated. For travelers, the DHS Traveler Redress Inquiry Program provides a redress process that facilitates the submission and processing of requests to correct data held by DHS. Any individual can request access to or correction of his or her personally identifiable information regardless of nationality or country of residence. This process has been described in the DHS Traveler Redress Inquiry Program Privacy Impact Assessment and information is available in multiple places on DHS's public website. Redress requests that come to the Traveler Redress Inquiry Program relating the difficulties encountered by a traveler at the point of entry due to information in IDENT/HART that needs to be modified or updated, are assigned via the Traveler Redress Inquiry Program to OBIM. OBIM then makes appropriate corrections to the IDENT/HART record if warranted and notifies the Traveler Redress Inquiry Program.

Alternatively, any person may submit a request to have OBIM correct a record by contacting OBIM Privacy, U.S. Department of Homeland Security, 2707 Martin Luther King Ave., S.E., Mailstop: 0655, Washington, D.C. 20528-0655.

Privacy Act exemptions associated with the records in IDENT, however, may preclude informing requestors what actions were taken in response to their Privacy Act or Freedom of Information Act inquiry.

3. Principle of Purpose Specification

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

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

- 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 may 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 IDENT/HART to support partner agencies that carry out their authorities pursuant to applicable law and regulation. Specific authorities are referenced in applicable privacy compliance documentation listed in Appendix A: Applicable Privacy Compliance Documentation, updated as appropriate.

Privacy Risk: There is a risk that DHS will provide data to NIST for a purpose other than the purpose for which it was originally collected.

Mitigation: This risk is mitigated. One of OBIM's prime goals as the DHS enterprise biometric system provider is to ensure accuracy in its system and the technology and algorithms that produce results that support the operators' programs. The data in IDENT/HART is collected by DHS Components and other IDENT/HART stakeholders for identification and verification of identities for their various missions. OBIM is working with NIST to ultimately ensure that the data in IDENT/HART is accurate, so that OBIM can continue to provide correct identification and verification of identities. This is consistent with the purpose of the collection of the data. NIST will evaluate the overall quality of IDENT/HART biometric data, how various algorithms perform with IDENT data (using repeatable and generally accepted accuracy measurements), and the strengths/weaknesses that may exist in IDENT/HART's algorithms and suggest updates to relevant industry biometric standards and best practices for DHS adoption. All of these would lead to enhancement of OBIM's technology and system and enhance IDENT/HART's function of providing accurate identification of individuals.

Privacy Risk: There is a risk that NIST will use data for a purpose other than that which is outlined in the Interagency Agreement.

Mitigation: This risk is mitigated. OBIM and NIST have entered into an Interagency Agreement that clearly lists and documents the terms and conditions of the data transfer for the purposes of testing and evaluation. NIST, as a federal agency, has experience in agreements of this nature, and trains employees authorized to access the information governed by the Interagency Agreement to use it only for the purposes specified in the Interagency Agreement. NIST will perform the following services per the Statement of Work: biometric matching algorithm evaluation, 10-print tuning, sampling strategies for the establishment of representative data sets, and give additional technical advice pertaining to the enhancement of OBIM systems matching accuracy.

4. Principle of Data Minimization

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

OBIM worked with each of the data owners to limit sharing personally identifiable information with NIST to only that which is necessary for NIST's analysis for this project. Easily linked data elements like names and Fingerprint Identification Numbers (FIN) will not be included in the data set sent to NIST. In addition, OBIM will continue filtering out all records identified as special protected class,[28] including 8 U.S.C. § 1367[29]), as well as Temporary Protected Status (TPS), Asylum, Refugee, Special Agricultural Worker program (SAW), and the Legal Immigration Family Equity (LIFE).[30]

OBIM and NIST do not anticipate a need to share IDENT/HART data outside of the two agencies. If NIST seeks to share any DHS data or use the data for other than an agreed-upon documented DHS specific purpose, NIST must receive prior written approval from the OBIM Program Manager, who will request permission from the relevant DHS Component and the relevant oversight offices (e.g., privacy, legal).

Both NIST and OBIM agree that NIST may publish and present aggregated results at government meetings and conferences or in journal articles and conference papers. These presentations and documents will not include personally identifiable information.

NIST will retain the DHS data until the end of the period of performance, which is currently scheduled for August 29, 2026, as described in the Interagency Agreement. If the Interagency Agreement is not renewed, NIST will remove all DHS data from the Biometric Research Laboratories no later than 90 days after the expiration of the last active Interagency Agreement. The Interagency Agreement between OBIM and NIST limits the use of the data by NIST for agreed upon DHS stated testing and evaluation purposes. If OBIM requires additional testing and evaluation, it may establish a new Interagency Agreement, with DHS Privacy Office approval. Per the Interagency Agreement, NIST is the only entity outside of DHS approved to

[28] Special protected classes include T, U, and Violence Against Women Act (VAWA) nonimmigrants, Asylee and Refugees, and Temporary Protected Status. These individuals receive special confidentiality through statute, regulation, or DHS policy.
[29] See 8 U.S.C. § 1367. 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.
[30] *See* additional information on Violence Against Women (VAWA), Temporary Protected Status (TPS), Asylum, Refugee, Special Agricultural Workers (SAW), and Legal Immigration Family Equity Life (LIFE) in USCIS compliance documentation in Appendix A.

receive DHS face images and fingerprints for testing and evaluation purposes.

OBIM will share the following data elements collected by CBP, ICE, TSA, and USCIS during the time covered by the period of performance with NIST:

Biometric Data

- Facial images; and
- Fingerprints.

Identity Information (when available)

- EID – The Encounter ID (EID)[31] continues to be the only anonymized data element. While the Encounter ID is associated with a specific encounter in IDENT, since the Encounter ID is anonymized it will not be possible to trace back to the individual from the data shared with NIST. In addition, NIST employees do not have direct access to IDENT to use the data to trace back to an individual's identity even if they were to come upon deanonymized Encounter Identification. All other included Identity Information data elements below will remain in the open because NIST requires these data elements to sub-group and categorize the tests and test results.
- Record batch number – distinct image number for batch (to ensure accountability and integrity);
- Event date – event create date;
- Gender;
- Year of birth;
- Place of birth;
- Place of birth Legacy Code (CD) – legacy code for place of birth; and
- Nationality_CD – code for nationality.

Document Information – (No document numbers will be sent)

- Document type;
- International Civil Aviation Organization (ICAO) Document type; and
- Document country of issuance.

Organization Information (when available)

- Org_ID – Organization ID number;

[31] Encounter Identification Numbers - Unique machine-generated identifiers (e.g., fingerprint identification number (FIN) and Encounter Identification Numbers (EID) link individuals with their encounters, biometrics, records, and other data elements. While the fingerprint and basic biographic information are initially enrolled and assigned a FIN, every subsequent encounter receives a new IDENT-generated Encounter Identification.

- Org_Desc – Organization description;
- Org_Name – Organization name;
- Org_Unit – Organization unit;
- Org_Subunit – Organization subunit;
- Activity_Type – Activity type of specific event; and
- Location – the location where the biometric encounter occurred.

Biometric Facial Image Data (when available)

- Capture device;
- Size type;
- Image format;
- Capture date;
- Height of image;
- Width of image; and
- Image ID.

Other Information:

- Make/Model/Serial/Firmware (MMSF) – used to identify the device information.
- Fingerprint match score – a score value for the fingerprint matching; used to support evaluations.
- Fingerprint Identification Number (FIN)[32] will not be shared with NIST. OBIM will use the Fingerprint Identification Number in support of data validation tasks, internal auditing, and control to ensure an accurate accounting of data transferred is maintained.

Privacy Risk: There is a risk that NIST will retain data for longer than is allowed in the original Interagency Agreement.

Mitigation: This risk is mitigated. NIST will retain the data until the end of the period of performance, which is currently scheduled for August 29, 2026, or possibly earlier if the NIST-DHS study has been completed. If no further Interagency Agreement is in place, then NIST will remove all data from the Biometric Research Laboratories no later than 90 days after the last active Interagency Agreement expires. NIST will inform OBIM upon deleting the data. OBIM will confirm, document, and, if necessary, audit this data deletion. The Interagency Agreement between OBIM and NIST describes the use of the data by NIST. OBIM may complete a new Interagency

[32] Fingerprint Identification Number (FIN) – a number assigned by OBIM to each unique set of fingerprints in the IDENT database.

Agreement, with DHS Privacy Office approval, if OBIM requires additional testing and evaluation by NIST. In addition, the relevant DHS Component Privacy Officers' and other appropriate oversight offices (e.g., legal) will need to approve the Interagency Agreement before OBIM shares additional data with NIST.

Privacy Risk: There is a risk that OBIM will provide more data to NIST than that which is necessary to fulfill the purposes authorized under the agreement.

Mitigation: This risk is mitigated. OBIM only shares with NIST those data elements in IDENT/HART which are required for NIST's testing and development of biometric standards. OBIM obtained approval from the DHS Privacy Office and DHS Component Privacy Offices (i.e., the data providers) prior to the initial transfer of data to NIST to determine which data elements are necessary for the purposes of the Interagency Agreement. Once OBIM determines that NIST evaluation of facial matcher performance and the fingerprints study is no longer required, the Interagency Agreement will be allowed to expire. Following the cessation of work under this agreement, NIST will delete all data from the Biometric Research Laboratories and will not retain any data provided by OBIM for testing.

5. Principle of Use Limitation

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

The capability to correctly match, store, share, and analyze biometric identity information requires the efficient operation, maintenance, and improvement of IDENT/HART. OBIM continues to share face images with NIST to support the development of a face image quality standard, matcher tuning, and increase accuracy performance. OBIM will share fingerprints with NIST to evaluate the overall quality of IDENT/HART data, determine how various algorithms perform with DHS data, and evaluate the strengths and weaknesses of the algorithms for the purposes of updating industry biometric standards and DHS best practices. In the future, OBIM could consider sharing additional modalities with NIST should OBIM require additional NIST support; however, sharing additional modalities will require DHS Components' approval and updated privacy compliance documentation to cover the additional transfers.

Privacy Risk: There is a risk that NIST employees or outside vendors will access more personally identifiable information than is necessary to accomplish their specified purpose.

Mitigation: This risk is mitigated. NIST cannot independently access any data in IDENT. NIST employees do not have access to IDENT and can only use the limited data that OBIM shares with NIST. NIST employees are the evaluators and subject matter experts for these studies. Face recognition vendors will send algorithms to NIST to participate in the Face Recognition Vendor

Test. At no time will external vendors and/or contractors be involved in the testing and evaluation of DHS data. Only cleared NIST personnel, in the secured Biometric Research Laboratories, will perform test and evaluation tasks. NIST will not share the data with any entity outside of NIST. If NIST seeks to use any data for purposes other than described above, NIST must receive prior written approval from the OBIM Program Manager, based on permissions received from the relevant DHS Components and relevant oversight offices (e.g., privacy, legal). NIST has no plans to use IDENT/HART data outside of the current agreement.

6. Principle of Data Quality and Integrity

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

OBIM and NIST are working to support efforts that increase the accuracy of OBIM's biometric matching. In accordance with the Interagency Agreement, research, testing, and development activities will take place to ensure evaluation of the quality of data and matching accuracy[33] for all results. The continual improvement of OBIM's biometric matching will result in lower risk of errors for mission operators, who rely on the accuracy of OBIM's matching services. Decision making based on more accurate matching by mission operators will improved privacy, civil rights, and civil liberties protections for individuals.

Testing algorithm matching accuracy is an important component of any biometric system given the potential impact inaccurate matching could have on individuals in their encounters with DHS. The agreement with NIST represents an effort that OBIM believes will enhance the integrity of the data in IDENT and in the future in HART. This testing would also reduce mismatches due to overlapping fingerprints.

Privacy Risk: There is a risk that the integrity of the personally identifiable information may be compromised during the data transfer to the NIST testing environments.

Mitigation: This risk is mitigated. OBIM mitigates this risk through several key procedures to prevent any compromise of data during the transfer process. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by the DHS Information Security Program.[34] Only approved NIST personnel will handle and monitor the data transfer of face images, just as they did in 2019. OBIM will transfer facial image data to NIST following a controlled and auditable process that incorporates encrypted drives, intermediate process validations, and a dual transfer/sign-off ensuring data security during the transfer process. OBIM will ensure all data is secure during

[33] *See* supra note 5.
[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, 4300A SENSITIVE SYSTEMS HANDBOOK (December 15, 2015 and subsequent updates), *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

transmission, and hard drives containing data are encrypted and hand delivered by OBIM personnel to the NIST facility. OBIM will follow this same process when transferring fingerprint data.

7. Principle of Security

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

OBIM and NIST ensure privacy and security controls are maintained on the data throughout the project. NIST stores the data received from OBIM securely in the NIST Biometric Research Laboratories. The data will never leave the NIST Biometric Research Laboratories and will be accessed only by NIST personnel. During the 2019 data transfer to NIST, OBIM encrypted the data on removable drives with on-device Federal Information Processing Standards (FIPS)compliant encryption. The drives were transported by an OBIM federal employee with an appropriate clearance and received by a NIST federal employee, who signed the property transfer form. OBIM maintained chain of custody throughout the transfer. OBIM will follow this same process for future transfers, including when transferring fingerprint data.

NIST will not share the data with any entity outside of NIST. The data will be retained until the end of the performance period in accordance with the Interagency Agreement.

Privacy Risk: There is a risk that personally identifiable information may be accessed by unauthorized personnel while NIST possesses the hard drives.

Mitigation: This risk is mitigated. OBIM mitigates this risk by ensuring that only NIST personnel with a need to know have access to the Biometric Research Laboratories in which the hard drives are stored. Hard drives containing personally identifiable information are only accessed when data is transferred to the Biometric Research Laboratories. Once data is transferred, the hard drives will go back to the Biometric Research Laboratories where it is then secured in a locked room. The Interagency Agreement and Statement of Work have security requirements that NIST is required to follow.

NIST is a federal agency within the Department of Commerce that has approved policies and procedures for the NIST Biometric Research Laboratories and secures and restricts access and use of the data to those with a need to know. NIST is required to report any data breaches to DHS/OBIM.

8. Principle of Accountability and Auditing

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

NIST staff who have access to the data have been appropriately trained regarding the proper treatment of personally identifiable information and the proper use of information systems to ensure safeguarding of information. NIST makes sure that employees with access to any DHS data have completed privacy training that includes the appropriate handling of personally identifiable information.

All DHS employees are required to complete annual Privacy Awareness Training. Users of DHS/OBIM systems, 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 personally identifiable information for mission- and non-mission-related purposes (e.g., human capital and employment). Training on specific systems is conducted as appropriate. OBIM system users must complete annual refresher training to retain system access.

Privacy Risk: There is a risk that the use of personally identifiable information will not be auditable to demonstrate compliance with these principles and all applicable privacy protection requirements.

Mitigation: This risk is mitigated. The data transferred between OBIM and NIST follows a controlled and auditable process that incorporates privacy and security requirements. Additionally, NIST continually updates and provides reports and briefings to OBIM regarding the testing and the latest results. OBIM will work with NIST to ensure deletion of the data. NIST will inform OBIM of the data deletion at the end of the period of performance of the Interagency Agreement.

Conclusion

OBIM is sharing data with NIST to further its efforts to increase the accuracy of its biometric matching capabilities related to facial images and fingerprints. OBIM and NIST entered into an Interagency Agreement that outlines the roles and responsibilities of each party for these research, testing, evaluation, and development activities. The results of this research, which will include an image quality capture standard and fingerprint analysis, will improve consistency in data definition and accuracy for OBIM's facial recognition services, and the integrity of the fingerprint data for IDENT and in the future HART. OBIM will continue to engage with DHS Component data owners and the DHS Privacy Office to ensure privacy protections remain in place throughout this effort.

Contact Official

John Boyd
Assistant Director of Futures Identity Operations
Office of Biometric Identity Management
Management Directorate
U.S. Department of Homeland Security
john.m.boyd@obim.dhs.gov

Responsible Officials

Craig Kelly
Branch Chief – Privacy and Policy
Office of Biometric Identity Management
Management Directorate
U.S. Department of Homeland Security
(202) 298-5169

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: Applicable Privacy Compliance Documentation

U.S. Customs and Border Protection (CBP)

CBP PIAs: https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

- DHS/CBP/PIA-002 Global Enrollment System (GES);
- DHS/CBP/PIA-006 Automated Targeting System (ATS);
- DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS);
- DHS/CBP/PIA-012 CBP Portal (e3) to EID/IDENT;
- DHS/CBP/PIA-021 TECS System: Platform;
- DHS/CBP/PIA–024 Arrival and Departure Information System;
- DHS/CBP/PIA-026 Biometric Exit Mobile Program;
- 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 Trusted and Registered Traveler Programs, 85 FR 14214 (Mar. 11, 20120);
- 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).

U.S. Immigration and Customs Enforcement (ICE)

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

- DHS/ICE/PIA-015 Enforcement Integrated Database (EID);
- Forthcoming Biometric Identification Transnational Migration Alert Program (BITMAP) PIA.

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

- DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016); and

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;
- DHS/USCIS/PIA-008 Enterprise Service Bus 2 (ESB 2);
- DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems;
- DHS/ALL/PIA-027 USCIS Asylum Division;
- DHS/USCIS/PIA-045 Deferred Action for Childhood Arrivals (DACA);
- DHS/USCIS/PIA-048 USCIS International Biometric Processing Services;
- DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS);
- DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS); 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, 84 FR 54622 (Oct. 10, 2019);
- 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: https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

- DHS/TSA/PIA-012 Transportation Worker Identification Credential (TWIC) Program;
- DHS/TSA/PIA-020 Security Threat Assessment for Airport Badge and Credential Holders;
- 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
- DHS/TSA/PIA-046 TSA OIA Technology Infrastructure Modernization Program.

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

- 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 Biometric Identity Management (OBIM)

OBIM PIAs: https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

- DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1

Department wide Documents:

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

- DHS/ALL-041 External Biometric Records (EBR) System of Records,
- DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records