# Privacy Impact Assessment

**for the**

# DHS International Biometric Information Sharing Program (IBIS) - Biometric Data Sharing Partnerships (BDSP)

**DHS Reference No. DHS/ALL/PIA-095(a)**

**November 18, 2022**

Homeland Security

## Abstract

The U.S. Department of Homeland Security's (DHS or the Department), Office of Strategy, Policy, and Plans (PLCY) in cooperation with DHS Components, created the International Biometric Information Sharing Program (IBIS) to support DHS Components and foreign partners in assessing the eligibility or public security risk of individuals seeking an immigration benefit in the context of a border encounter or law enforcement investigation related to immigration or border security issues. DHS created IBIS to improve the Department's and its foreign partners' ability to establish more definitively the identity and assess eligibility of an individual presenting for an immigration benefit or when encountered by DHS law enforcement in border and immigration related contexts. The ability of biometric information sharing to support law enforcement investigations and immigration benefit decisions has been validated in DHS's current international partnerships, which have assisted foreign partners in detecting identity fraud, foreign criminals who have not disclosed their prior criminal activity and known or suspected terrorists (KST). This Privacy Impact Assessment (PIA) Update considers the privacy risks and applicable mitigation strategies associated with implementing this Departmental program in cases where partners permit DHS to retain all biometric enrollments regardless of a match to an existing DHS record, as this additional collection differs from the scope covered by the original IBIS Privacy Impact Assessment.[1]

## Introduction

As discussed in the original IBIS Privacy Impact Assessment, IBIS facilitates fingerprint-based bilateral biometric and biographic information sharing between the United States and a foreign partner. IBIS enables automatic comparison of the fingerprints collected by DHS or a foreign partner on border crossers, suspected criminals, asylum seekers, irregular migrants, refugees, and other individuals encountered by government representatives against U.S. and partner country terrorism, national security, identity, immigration, and criminal records. This helps the United States to identify individuals that present a threat to the security or welfare of the United States, identify perpetrators of identity fraud in the immigration process, and enhance the vetting of individual travelers. It similarly allows its foreign partners to compare fingerprints against DHS records for the same purposes. This biometric and biographic data exchange with foreign partners contributes to United States security interests by reducing the likelihood of onward travel to the United States by national security threat actors, criminals, and undocumented individuals and promotes the integrity of global travel and migratory systems. DHS concludes appropriate information sharing agreements or arrangements that includes privacy protections and safeguards

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

and makes clear the participants will not share information with third countries without explicit consent of the providing country.

In some cases, IBIS partners may seek technical and financial support from DHS to develop biometric identity management systems. With these foreign partners, DHS provides the backbone to support biometric matching and screening capabilities by providing both automated and manual identity information sharing processes, including subject matter expertise, to implement a collaborative solution that meets the foreign partner's biometric requirements. To establish the proper technologies of biometric exchange, DHS may be able to provide technical and security sector assistance support to IBIS partners that lack adequate biometrics programs using U.S. Department of State foreign assistance resources. Through this IBIS implementation model, referred to as the Biometric Data Sharing Partnership (BDSP), DHS can aid foreign governments in obtaining sufficient domestic biometric capacity, including collection, storage, identity management capabilities, and data protection and system security requirements, to be able to partner with DHS and improve their own domestic border security capabilities. This is built in a manner that is fully integrated with DHS's Management Directorate (MGMT) Office of Biometric Management (OBIM) Automated Biometric Identification System (IDENT)[2] and successor system, Homeland Advanced Recognition Technology (HART).[3]

The BDSP implementation model allows the IBIS partner to submit electronic fingerprint-based queries, the nature of the encounter, transactional metadata, and, where agreed by the foreign partner, any other associated biographic or biometric information (such as iris images and face images) that may be determined to be appropriate, to IDENT/HART. DHS will notify the IBIS partner if DHS records match to the fingerprint-based query and will only share relevant personal information in the same manner as discussed in the original IBIS Privacy Impact Assessment.[4]

When DHS builds IBIS/BDSP countries a biometric system using foreign assistance funds, that partner's biometric system uses IDENT/HART as its data repository for biometric matching purposes. If the negotiated international agreement or arrangement allows, the IBIS information

---

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *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 THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim. OBIM is implementing HART in four incremental phases, publishing updates to this Privacy Impact Assessment prior to the release of each Increment.

[4] For example, "IDENT/HART would return a "no match" response when there is a biometric match to an individual in a "special protected class," such as a Violence Against Women Act (VAWA) petitioner, T visa applicant (nonimmigrant status victim of human trafficking), or someone applying for a U visa (nonimmigrant status victim of a qualifying crime), except in certain circumstances, because the data of such individuals are protected by law."

exchange process is then streamlined as DHS builds the partner's biometric system to be directly interoperable with IDENT/HART. For IBIS partners using this implementation model, all biometric and associated biographic information obtained by the partner for relevant purposes as defined in the bilateral agreement or arrangement will be enrolled in IDENT/HART. DHS will not query a partner fingerprint database but will instead query the enrolled partner holdings retained in IDENT/HART. This Privacy Impact Assessment Update addresses the specific privacy risks and business processes associated with this model.

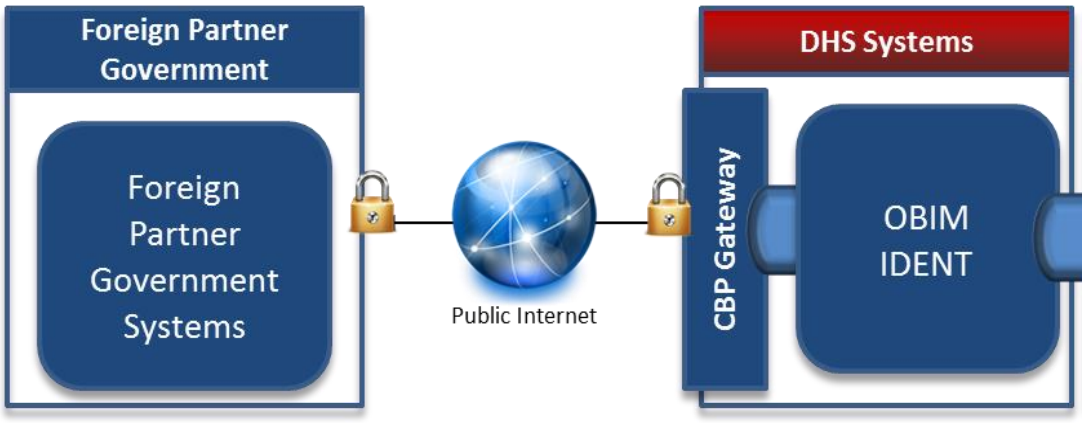
When a fingerprint and associated identity information is enrolled in IDENT/HART, the "match" or "no match" response, as well as appropriate information in the case of a match, is provided back to the IBIS/BDSP partner country in the same manner as other IBIS partners. If the international agreement or arrangement permits, any biometric and corresponding information collected by the partner using the biometric system provided by DHS is automatically enrolled in IDENT/HART and marked as originating from that partner. DHS Components and appropriate IDENT/HART users will have access to that information in accordance with established access policies and for purposes consistent with the international agreement or arrangements. Therefore, DHS Components and appropriate IDENT/HART users do not need to initiate new searches to partner biometric system to support their operations, which minimizes the number of transactions involving personal data.

DHS establishes interoperability between IDENT/HART and partner country databases using technologically advanced encryption protocols, the public internet, DHS OneNet, and the CBP Gateway to share biometrics and biographic data. A Virtual Private Network (VPN) or other secure encrypted connection is established over the open internet between the partner's network and the CBP Gateway. The CBP Gateway is a secure conduit that validates external connections to DHS OneNet and systems, making sure the connection and messages received are authorized. DHS has established future capabilities to send requests and responses from IDENT/HART to the IBIS partner countries' automated biometric systems through a dedicated gateway.[5]

Individual submissions from a foreign partner are packaged in the latest Transport Layer Security (TLS) and submitted to a secure Internet Protocol (IP) address within the United States. Once received by the CBP Gateway, the package is unencrypted, validated for the proper formatting, virus scanned, and sent across DHS OneNet to DHS IDENT for processing.

The diagram below depicts the current bi-directional (two-way) flow of information for DHS-provided fully interoperable biometric databases:

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED REAL-TIME IDENTITY EXCHANGE SYSTEM (ARIES), DHS/OBIM/PIA-006 (2022), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.




DHS intends to implement the information-sharing described in this Privacy Impact Assessment in a phased approach, consistent with each IBIS partner's capabilities and resources.

## Reason for PIA Update

DHS is updating this Privacy Impact Assessment to address privacy risks associated with the BDSP implementation model of the IBIS Program, where that partner permits DHS to retain non-matching biometric, biographic, and transactional data within DHS's system in order to address more effectively shared security concerns, operationalize a biometric system provided by DHS using foreign assistance, enable large volumes of transactions, and/or to minimize the number of times personal data is exchanged between systems.

## Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[6] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[7]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[8] The FIPPs account for the nature

[6] 5 U.S.C. § 552a.
[7] 6 U.S.C. § 142(a)(2).
[8] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework For Privacy Policy at the Department of Homeland Security (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.

and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure the Homeland.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[9] and the Homeland Security Act of 2002, Section 222.[10] Given that the IBIS Program is a Departmental program rather than a particular information technology system, this Privacy Impact Assessment Update is conducted to specifically to examine the privacy impact of IBIS/BDSP partnerships as it relates to the Fair Information Practice Principles.

## 1. Principle of Transparency

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

DHS has provided public transparency through the issuance of this Privacy Impact Assessment and the related Component Privacy Impact Assessments that discuss border enforcement and vetting of visa and immigration benefit applicants, applicable System of Records Notices (SORN) and public statements attesting to such cooperation with foreign countries. All conditions for the processing of personal information received from foreign governments under the IBIS Program or sent to the foreign governments for reciprocity are, or will be, documented in international agreements or arrangements with each participating government, which, when unclassified, may be made available in whole or in part through a Freedom of Information Act request.[11] All binding agreements will be reported to the United States Congress by the Department of State pursuant to U.S. law. Partnering foreign governments may also provide additional notice to individuals from whom they have collected the information pursuant to their national law and procedures.

DHS has provided transparency about the potential disclosure of personally identifiable information via the relevant System of Records Notice(s) and Privacy Impact Assessment(s) for the program that originally collected the information as well as, when applicable, the DHS website and individual applications/forms.

The following System of Records Notices from the IDENT/HART source system owners—U.S. Immigration and Customs Enforcement (ICE), U.S. Customs Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS)—cover the DHS data to be eventually shared under IBIS in response to a matching query:

[9] 44 U.S.C. § 3501 note.
[10] 6 U.S.C. § 142.
[11] *See* https://www.dhs.gov/freedom-information-act-foia.

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, which covers records documenting ICE's criminal arrests, and most of ICE's immigration enforcement actions;[12]
- DHS/CBP-006 Automated Targeting System, which supports CBP in identifying individuals and cargo that need additional review traveling to and from the United States;[13]
- DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, which covers the collection, use, and storage of biometric and biographic data for background checks and its results; it also covers background checks and their results;[14]
- DHS/ALL-041 External Biometric Records, which covers the maintenance of biometric and associated biographic information from non-DHS entities, both foreign and domestic, 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;[15] and
- DHS/ALL-043 External Biometric Administrative Records, which covers technical and administrative information necessary to carry out functions that are not explicitly outlined in component source-system System of Records Notices, such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.[16]

When submitting a fingerprint to DHS for search and enrollment within IDENT/HART, the IBIS partner may provide additional personally identifiable information (e.g., biographic information, encounter-related information) automatically, consistent with Appendix A of the IBIS Privacy Impact Assessment. If the queried fingerprint does not match the holdings in IDENT/HART, and if the international agreement or arrangement permits, the fingerprint and associated information may be retained by DHS for purposes of sharing the IBIS partner's own prior encounter information back with them, and to minimize the need for DHS to initiate searches

[12] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 Fed. Reg. 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[13] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC), 83 FR 36950 (July 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[15] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[16] DHS/ALL-043 External Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (March 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

to the foreign partner during its subsequent encounters. This approach accounts for the reality that BDSP partners typically do not have the technical bandwidth and capabilities to respond to the volumes of searches DHS would need to conduct of their databases. It also minimizes the number of times DHS exchanges personally identifiable information with foreign partners.

As with all IBIS partners, DHS may share data elements consistent with Appendix A of the IBIS PIA, including first and last names, former names, other names, aliases, alternative spelling of names, gender, date and place of birth, photographs, current and former nationalities, passport data, numbers from other identity documents, and applicable encounter data. DHS limits initial disclosures to information available in or through IDENT/HART. OBIM analysts coordinate with and provide CBP, USCIS, and ICE with notification of matches to their data. CBP, USCIS, and ICE can decide whether to share information beyond that which is stored in IDENT/HART.[17]

Under certain agreements, including Preventing and Combating Serious Crimes (PCSC) agreements, IBIS partner countries may also, in compliance with their respective national laws, share personally identifiable information—without receiving a specific query—to supply information to the other country when there is a reason to believe a person may be a threat. Such instances include when there is reason to believe an individual:

- Will commit, may be planning to commit, or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association;
- Is planning to, is undergoing, or has undergone training to commit terrorist or terrorism related offenses, or offenses related to a terrorist group or association; or
- Will commit, may be planning to, or has committed a serious criminal offense or participates in an organized criminal group or association.

The country providing this information may impose conditions on the use and further sharing of such data.

**Privacy Risk:** A privacy risk remains that individuals will not know their information will be used in this manner when applying for an immigration or travel-related benefit or when encountering a DHS law enforcement officer.

**Mitigation:** This risk is partially mitigated. This risk is mitigated to the extent possible through the publication of this Privacy Impact Assessment, as well as the publication of Privacy Impact Assessments and System of Records Notices addressing the collection, notification, and sharing of biographic and biometric information. The IDENT and HART Privacy Impact Assessments and the External Biometric Records and External Biometric Administrative Records System of Records Notices provide general notice that an individual's personal information may

[17] 8 U.S.C. § 1367, "Penalties for disclosure of information" (originally enacted as Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA)).

reside in IDENT/HART. 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. If required by law or policy,[18] DHS components, as well as external partners that submit information to IDENT/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 in the future HART.

However, this risk cannot be fully mitigated because this information is collected from source systems and then shared, and the BDSP implementation model permits DHS to retain non-matching biometric, biographic, and transactional data.

## 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.*

Individuals provide their personal information to border or immigration officials, including fingerprints, for the purposes of screening and vetting to gain an immigration benefit or transit a border. In the case of biometric and associated information collected by the United States and its foreign partners for immigration and border purposes, this information is always collected directly from the individual.

However, a traditional approach to individual participation is not always practical or possible when sharing information with law enforcement agencies, including border enforcement agencies. It would be counterproductive to provide subjects with access to certain investigative information about themselves during a pending law enforcement or security investigation, as this would alert them to, or otherwise compromise, the investigation. Although individuals may not always participate in the collection of information about themselves shared pursuant to an investigation or other law enforcement action or access such records during a pending law enforcement investigation, individuals may contest or seek redress during any resulting prosecution or proceedings brought against them by the United States or through appropriate redress measures made available by the IBIS partner.

In addition, U.S. citizens and Lawful Permanent Residents (LPR) have the right to request amendments to their records under the Privacy Act.[19] The Judicial Redress Act of 2015 (Judicial Redress Act) (5 U.S.C. § 552a note), which supplements the Privacy Act, provides citizens of

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY REGARDING COLLECTION, USE, RETENTION, AND DISSEMINATION OF PERSONALLY IDENTIFIABLE INFORMATION (2022), *available at* https://www.dhs.gov/privacy-policy-guidance.
[19] 5 U.S.C. § 552a(a)(2).

covered countries with access and amendment rights under the Privacy Act in certain limited situations, as well as the right to sue for civil damages for willful and intentional disclosures of covered records made in violation of the Privacy Act.[20] DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information is necessary for DHS to efficiently meet its operational goals, prevent waste, and improve outcomes.

Individuals not covered by the Privacy Act or the Judicial Redress Act may individually request access their records by filing a Freedom of Information Act (FOIA) with the respective component or DHS FOIA office. Additional information about FOIA is available at http://www.dhs.gov/foia.

Travelers who wish to file for redress can complete an online application through the through the DHS Traveler Redress Inquiry Program (DHS TRIP)[21] 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.

Individuals who believe information about them was processed under or pursuant to an IBIS information sharing agreement or arrangement may seek to access, correct, amend, or expunge information held by DHS's foreign partners, or otherwise seek redress from these foreign partners for the processing of information abroad, through partner countries applicable access and redress laws and programs. DHS seeks assurances from its IBIS partners that they provide such appropriate redress mechanisms through its international agreements and arrangements. As IBIS countries provide points of contact for redress, DHS intends to publish them on its website and a full list of countries will be regularly updated in Appendix B of the original IBIS Privacy Impact Assessment.

**Privacy Risk:** There is a risk that foreign partners will collect biometric and biographic information and provide it to DHS without individuals' knowledge.

**Mitigation:** This risk is partially mitigated. Through publication of this Privacy Impact Assessment Update, DHS is providing public notice that its IBIS/BDSP partners may share information with DHS on individuals those IBIS/BDSP partners encounter in the travel, border, immigration, and law enforcement context. When biometrics are collected in the travel, border,

[20] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website https://www.justice.gov/opcl/judicial-redress-act-2015.

[21] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM, DHS/ALL/PIA-002 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

and immigration context, it usually involves the direct participation of the individual. For example, fingerprints submitted to border officials at ports of entry involve direct individual participation. In a law enforcement context, there is a greater likelihood of the individual not being informed about the collection. For example, collection of latent fingerprints from a crime scene may be done without notice, but such instances are usually subject to additional legal safeguards. DHS encourages its IBIS/BDSP partners to provide transparency to individuals they encounter regarding how their data will be handled and shared.

**Privacy Risk:** There is a risk that individuals will not know to seek redress from the United States to make corrections to their information under the BDSP implementation model if the individual has not had any interaction with the Department.

**Mitigation:** This risk is partially mitigated. Each IBIS partner country may have different procedures and mechanisms for providing public notice regarding how they use and share data it collects. However, through this Privacy Impact Assessment Update, DHS provides notice to the public that some IBIS partners, under the BDSP implementation model, may share data with DHS on individuals DHS has not previously encountered and information on how to seek redress from DHS. If individuals seek redress in the IBIS partner country to successfully correct inaccurate data, that partner should notify DHS of those inaccuracies so DHS can update its records, per the terms of underlying information sharing agreement or arrangement. Should the individual subsequently be encountered by DHS, they would have an additional opportunity at that point to correct their data should they believe DHS is relying on inaccurate information. DHS does not use data collected from an IBIS/BDSP partner in its decision-making process until it encounters the individual, commonly at a port of entry or on during an immigration benefit request, at which point individuals are aware the DHS is using their data.

## 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.*

Numerous federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of noncitizens, compares the biometric data of aliens to verify their identity, and authenticates travel documents presented by such aliens through the comparison of biometrics. These include: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106–215, 114 Stat. 337; Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104–828, 110 Stat. 3009–546; Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106–396, 114 Stat. 1637, 1641; Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107–56, 115 Stat. 272, 353; Section 302

of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Public Law 107–173, 116 Stat. 543, 552; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108–458, 118 Stat. 3638, 3817; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110–53, 121 Stat. 266, 338; and Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114–125, 130 Stat. 122, 199 (6 U.S.C. 211(c)(10)). Federal law requires that this integrated system be accessible in real time to consular officers, immigration officers, and criminal investigators across the interagency. 8 U.S.C. § 1365b.

The purpose of the IBIS Program is to allow DHS and its partners to compare the fingerprints of travelers and immigration benefit applicants, as well as those encountered by law enforcement during border inspections or in the course of criminal investigations, against partners' appropriate identity records in addition to criminal and terrorist records. Information gleaned from this sharing is used to prevent, detect, and investigate crime, including assessing whether an individual presents a criminal or terrorist risk and aids border and immigration-related decisions. These purposes are discussed in the relevant information sharing agreement or arrangement negotiated with the foreign government.

**Privacy Risk:** There is a privacy risk that personal information originally collected by DHS for a particular purpose for an authorized DHS mission will be shared with foreign partners who use that information for unauthorized purposes, which may be incompatible with the original purpose of the DHS collection.

**Mitigation:** This risk is partially mitigated. Information obtained consensually by DHS for a specific purpose may be disclosed through IBIS if a foreign partner submits a fingerprint for a purpose consistent with the bilateral agreement or arrangement, and if DHS has a match for that fingerprint which is shareable under U.S. law and policy. U.S. law and policy allows the partner to use that information for purposes consistent with the bilateral information sharing agreement or arrangement. The information exchange will also add new information about an individual to DHS databases that will help DHS and the foreign partner to better screen the individual should DHS or the partner encounter them in the future.

Information sharing under IBIS occurs only in the context of border security, immigration, law enforcement with a nexus to the U.S. border, countering transnational crimes and organizations, terrorism, and detecting crimes. DHS negotiates information-sharing agreements or arrangements with participating foreign partners that outline limitations on how shared information can be used.

The initial biometric search from the foreign partner includes an indicator of the purpose for which they are submitting a search, enabling DHS to validate the search is for a purpose consistent with that agreement or arrangement and facilitating oversight reviews. Before

concluding a new information sharing agreement, the DHS office or component responsible for the agreement will submit a Privacy Threshold Analysis to the Privacy Office. In the event that the new agreement alters the current assessment of risks and mitigations discussed in this Privacy Impact Assessment, an annex to this Privacy Impact Assessment will be published to address the new or differing concerns.

Moreover, Concept of Operations developed by DHS for each partner country ensure foreign IBIS queries align with the purposes enumerated in the applicable information-sharing agreement. Finally, IBIS information-sharing agreements also restrict disclosure of information to third parties and include routine accountability and auditing mechanisms by DHS and its foreign partner to ensure the information sharing agreements are properly implemented. However, because DHS's traditional oversight mechanisms are more limited in foreign countries and because DHS information may be used by the partner for unauthorized purposes and when DHS has no derogatory information, the DHS Privacy Office will (1) continue to engage with the IBIS Program to ensure the execution of additional privacy protections that may be feasible in the future and (2) initiate a Privacy Compliance Review within a mutually determined time period but no later than three years or upon a substantive change to the program, whichever occurs sooner.

**Privacy Risk:** There is a privacy risk that unauthorized queries may be made about individuals.

**Mitigation:** This risk is partially mitigated. All agreements or arrangements include provisions requiring regular auditing and review of the actual sharing. Additionally, OBIM monitors transmissions for quality assurance to ensure that foreign partners submit queries for authorized purposes. All queries must be accompanied by a code stating the purpose of the query, and such purposes must fall within the scope of the arrangement or agreement OBIM developed business rules will reject any submission from a foreign partner that does not maintain an authorized activity type, which denotes the designated purpose of the biometric query. This exchange of information, and the audit trail created by the exchange, help to ensure that the query was submitted for an authorized purpose by providing DHS more information to detect potential unauthorized activity or problematic trends. If DHS were to discover that a foreign partner submitted an unauthorized query on an individual, DHS would take appropriate remedial action to ensure the receiving country purges any information shared about the individual associated with that query. DHS will also reconsider whether it should continue the information-sharing relationship with the foreign partner. These remedial actions, however, may not always fully remedy or mitigate the actions already taken by the receiving country. The DHS Chief Privacy Officer may also direct a Privacy Compliance Review or other action to determine whether the parties or participants followed all terms and conditions of the relevant agreement or arrangement and related policies and protocols, and whether all privacy compliance documents, including this Privacy Impact Assessment, continue to accurately reflect the privacy risks and applicable

mitigation strategies associated with implementing this Departmental program, with a view to helping avoid future reoccurrences.

**Privacy Risk:** There is a privacy risk that personal information, including U.S. citizen or Lawful Permanent Resident information, will be sent to DHS where there is no purpose for DHS to have that information.

**Mitigation:** DHS would only receive information regarding U.S. citizens or Lawful Permanent Residents if they were encountered by a foreign partner in an immigration, border, or law enforcement context where the individual was suspected of committing a crime. This aligns with the information sharing agreements DHS completes with each partner. As such, information on U.S. citizens or Lawful Permanent Residents could be used to support future DHS encounters with those individuals.

## 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).*

IBIS partnerships enable DHS and the Department of State to receive and retain information from foreign governments that is necessary to make border enforcement and immigration-related decisions, as well as to prevent, detect and investigate related crime. Under the principle of reciprocity, DHS will only share biometric and biographic information necessary for the IBIS partner country to make similar decisions in the event a foreign partner enrollment matches a record in IDENT/HART in accordance with applicable law and policy. Some IBIS/BDSP countries may request DHS serve as a biometric repository for their data because they lack the ability to store or match biometric data at sufficient volumes. In these instances, a country may opt to authorize DHS to retain biometric and biographic information for future use by the foreign partner and/or DHS components. In addition to minimizing DHS data disclosures to the partner, DHS Components do not need to send a fingerprint search to discover whether the partner has previously encountered the individual in question because that information is already held in IDENT/HART.

The National Archives and Records Administration (NARA) approved the records retention schedule for DHS's biometric and biographic records used for national security, law enforcement, immigration, and other functions consistent with DHS authorities. The External Biometric Records (EBR)[22] schedule requires DHS to destroy law enforcement records 75 years

[22] *See* National Archives And Records Administration, U.S. Department of Homeland Security Request For Records Disposition Authority, Biometric With Limited Biographical Data (2013), *available at*

after the end of the calendar year in which the data was gathered. This schedule also covers 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.[23] OBIM is re-evaluating the current retention policy to determine variable retention periods for latent fingerprints and international records and will submit to the National Archives and Records Administration for approval for any change in retention periods. Consistent with both retention schedules, DHS and a partner country may agree to establish a retention period of less than 75 years as part of the applicable agreement or arrangement.

**Privacy Risk:** There is a risk the foreign partner may enroll individuals for purposes other than those specified in the applicable international agreement or arrangement, making the use inconsistent with the analysis contained in this Privacy Impact Assessment.

**Mitigation:** This risk is partially mitigated. While DHS has no control over who a foreign partner chooses to enroll in IDENT/HART, the circumstances under which a foreign partner may enroll an individual are specified in the international agreement or arrangement, are discussed in the training provided to officials of the foreign partner, and may be examined by DHS as the result of audits conducted by DHS. Furthermore, enrollment occurs based on individual encounters rather than in bulk and enrollment is limited to encounters that take place after BDSP becomes fully operational for the foreign partner. Moreover, DHS installs the equipment and configures the software at mutually-agreed locations in the partner country, and verifies the activities conducted at those sites support the uses and purposes outlined in this Privacy Impact Assessment.

**Privacy Risk:** There is a risk DHS or the foreign partner may retain data beyond the period of approved disposition schedules mandated by U.S. law or the applicable agreement or arrangement with that foreign partner.

**Mitigation:** This risk is partially mitigated. Data providers are responsible for deleting their information from IDENT/HART in accordance with the applicable data retention schedule. OBIM provides training and guidance to IDENT/HART data providers prior to submitting information to IDENT/HART. In addition, DHS oversight offices and data providers may use HART auditing capabilities to ensure implementation of the data retention schedules.

OBIM has a dedicated team that continually monitors sharing to ensure quality assurance and issues reports on its sharing with IBIS partner countries. These monthly, quarterly, and annual reports help identify and remedy any data that may be retained longer than necessary. The partner

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

[23] *See id*.

countries agree to engage in regular consultations with DHS, which may also help to identify areas of non-compliance. If data is found to have been retained by DHS longer than necessary, DHS will take appropriate remedial actions, including notifying the data owner.

Under the Federal Records Act and accompanying regulations, OBIM remains responsible (as do all federal agencies) for ensuring the proper retention and disposal of biometric and associated information stored in its systems. Data owners who use OBIM's services can schedule the deletion of biometric records in accordance with their National Archives and Records Administration-approved retention schedule. Failure to comply with these legal and policy requirements can lead to investigations by oversight bodies such as the DHS Office of the Inspector General or National Archives and Records Administration (under 44 U.S.C. § 2904(c)(7), which may result in administrative, civil, or criminal penalties.[24]

IBIS information sharing agreements authorize DHS and its partners to retain and use information for one or more of the following purposes: assessing the eligibility or public security risk of individuals seeking an immigration benefit or encountered in the context of a border encounter or law enforcement investigation related to immigration or border security issues. DHS may retain information to enrich or update DHS's existing record on an individual after a biometric match has been established. This authorization ensures DHS's interactions with the individual are based on complete and accurate information, which is critical to both detecting fraud and facilitating interactions with low-risk travelers and migrants. Agreements may also authorize DHS to retain information about individuals the providing country believes present a threat to border or national security, regardless of whether DHS has previously encountered them. Both circumstances support the data quality principle that personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date. In addition, some countries may opt to authorize DHS to retain, either on a categorical or case-by-case basis, that information for future use by the foreign partner and/or DHS.

**Privacy Risk:** There is a risk that information about individuals in special protected classes will be inadvertently shared with the querying country.

**Mitigation:** This risk is partially mitigated. While the automatic and manual filtering processes are methodically performed, data concerning an individual in a special protected class may be inadvertently shared with a partner country. For instance, an individual's special protected

[24] The HART Increment 1 Privacy Impact Assessment contains the following Privacy Office Recommendation: When onboarding a new O/U/S [Organization/Unit/Subunit] 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. 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.

class status may not have been known at the time of the sharing. In order to ensure such sharing is performed appropriately, OBIM maintains a log of all data transmitted and received, which OBIM reviews on a regular basis. OBIM has a dedicated team that continuously monitors and reports on sharing with partner countries. Reports are generated, reviewed, and distributed to CBP, ICE, USCIS, and PLCY on a monthly, quarterly, and annual basis. If information is found to have been inappropriately shared, OBIM will report those incidents to the DHS Privacy Office, consistent with DHS policy, and DHS will take remedial action, such as contacting the sharing partner and requesting that the information be deleted and requiring staff receive additional training.[25] The DHS Chief Privacy Officer may also direct that a Privacy Compliance Review be conducted, take other action, or refer the issue to another oversight office (such as the DHS Office of Civil Rights and Civil Liberties), as appropriate.

**Privacy Risk:** There is a risk DHS collects data on individuals who may never seek to travel to the United States.

**Mitigation:** This risk is partially mitigated. Data retention ensures that any subsequent DHS interactions with an individual are based on complete and accurate information. DHS has no way of knowing whether it will ultimately encounter an individual about whom it has collected data; however, the applicable international agreement or arrangement limits enrollment by the BDSP country to specific activities. If the individual never seeks to travel to the United States, DHS will not have a reason to use the data in its decision-making process. However, data retention enables DHS to provide foreign partners with information they previously collected should the partner encounter the individual again, thereby ensuring the partner has access to accurate and complete information to inform their subsequent encounters.

## 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.*

DHS receives and discloses information to: 1) assist DHS components and IBIS partner countries in verifying an individual's identity for immigration purposes and assessing whether an individual presents a criminal or terrorist risk; 2) aid DHS components and foreign partners in border-related law enforcement encounters; and 3) aid in making border and immigration related decisions. These purposes are in the relevant international agreement or arrangement negotiated with the IBIS partner country.

While there is a risk that a foreign partner may submit a request to DHS outside of the

[25] The HART Increment 1 Privacy Impact Assessment includes the following 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.

partner's authorities or the applicable international agreement or arrangement, DHS partially mitigates this risk through its engagement with each partner country and, for BDSP countries, through its detailed involvement in establishing the partner's systems and business processes and through extensive training. DHS develops a detailed Concept of Operations plan for implementing the information sharing agreement with all partner countries. These plans and the associated training provided to the partner further detail when a partner may submit a request. In addition, each request is tagged with a unique category code indicating why the query was submitted which align to the purposes in the agreement or arrangement. Through OBIM, DHS tracks the volume of requests received by category code on a weekly basis and can identify anomalies in search trends and engage with the partner government to determine the cause of such anomalies. Furthermore, IBIS agreements and arrangements include provisions requiring routine auditing and mechanisms for assessing compliance. In order to ensure compliance, the DHS Chief Privacy Officer may choose to conduct a Privacy Compliance Review of the sharing activities that occur under these agreements.

DHS limitations on use of personal information in information-sharing relationships are documented in applicable agreements, arrangements, and other implementing documentation. For example, these agreements and arrangements define the purpose and scope for which the information can be used, limit onward sharing, and require partners to ensure the data is secured and safeguarded.

USCIS, ICE, and CBP ensure all disclosures of data in response to queries from foreign partners are compatible with the purposes for which the data was originally collected through established policy. Organizational filtering, also called Organization/Unit/Subunit (O/U/S) filtering, uses configuration settings within IDENT/HART to remove information about encounters that are not permissible to share from responses to the authorized user's query. Each IDENT/HART authorized user has an Organization/Unit/Subunit account for their specific agency or organization, and their account receives information in accordance with defined filtering rules as determined by statutes and DHS policies, and in information sharing arrangements and agreements, and as described in component compliance documentation. Since IDENT/HART is only a repository and OBIM does not own the data, authorized users who upload and store biometric information in IDENT/HART are considered "data providers," as well as the "data owners." IDENT/HART can either filter or share IDENT/HART data from an Organization/Unit/Subunit in accordance with permissions set by the data owner or at the request of the user requesting the data. Filtering can also be done at the request of the data provider. Each Organization/Unit/Subunit is configured to receive or filter out certain types of information based on data owner-set permissions, applicable arrangements or agreements, DHS policies, 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.

**Privacy Risk:** A privacy risk remains that data will be shared more broadly than permitted by the relevant System of Records Notices and terms of the relevant IBIS information sharing agreement.

**Mitigation:** This risk is partially mitigated. OBIM limits inappropriate disclosure from IDENT/HART by setting OBIM's automated filtering rules in IDENT/HART and applying them to all IBIS partner searches via manual analysis.[26] OBIM continually monitors quality assurance and generates monthly, quarterly, and annual reports for each information sharing partner country that are also made available to relevant components. In addition, DHS international information sharing agreements and arrangements will make partner countries responsible for maintaining and logging all data transmitted and received. If data is found to have been inappropriately shared, DHS will take appropriate remedial action, including contacting the sharing partner and requesting that the information be deleted, requiring staff receive additional training, or even terminating cooperation. Under the BDSP implementation model, DHS has direct insight and knowledge of the data the partner is sharing and receiving through the integrated systems and can conduct independent auditing and oversight when deploying its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, investigations, onsite inspections). Further, DHS and its partner countries continue to establish strong working relationships, and maintain regular communications based on agreed-upon Concepts of Operations, to ensure information sharing agreements are faithfully adhered to by all countries. DHS will incorporate compliance evaluations into the text of information-sharing agreements and arrangements signed with partner countries that will provide DHS with the opportunity to compare OBIM's information-sharing reports with partners' logs. Such evaluations will be mutually determined with each foreign partner, and generally be no more frequent than annually and no less frequent than every three years.

**Privacy Risk:** There is a risk that a partner country may share DHS-provided data with a third party without first obtaining DHS's consent.

**Mitigation:** This risk is partially mitigated. IBIS information-sharing agreements restrict disclosure of information to third parties and include routine accountability and auditing

[26] The HART Increment 1 Privacy Impact Assessment contains the following Privacy Office Recommendations: 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. 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 owner authorities and policies as set out in the business rules. The governance board should also review whether business rule configurations align with information sharing and access agreements with OBIM or agreements or arrangements with DHS that contemplate sharing from the HART system. The DHS Privacy Office recommends OBIM implement technology that allows authorized users to read caveats that indicate a record contains special protected class information. 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.

mechanisms by DHS and its counterpart agency to ensure the information sharing agreements are properly implemented. The agreements permit the country responding with information to inquire about how its data is used and the results obtained. However, because the sharing would have already occurred, any such remedial actions would be forward-looking and would not remedy or mitigate the unauthorized sharing that has already occurred.

Under the BDSP implementation model, DHS has direct insight and knowledge of the data the partner is sharing and receiving through the integrated systems and can conduct independent auditing and oversight when deploying its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, investigations, onsite inspections). DHS and its partner countries establish strong working relationships and maintain regular communications, routine training and troubleshooting support, and operational advisors to ensure information sharing agreements are faithfully adhered to by all countries. Furthermore, DHS incorporates compliance evaluations into the text of information-sharing agreements and arrangements signed with partner countries. In the case of agreements, the parties are legally bound to follow the applicable privacy and data security provisions. When DHS uses a non-binding arrangement to govern the information sharing, those arrangements memorialize the participants' political commitment to adhere to these same requirements. In either case, if DHS concludes that a country is not a responsible steward of the personally identifiable information with which it is entrusted, then DHS may terminate the information sharing agreement or arrangement.

**Privacy Risk:** There is a risk specific to the BDSP implementation model that information provided by a foreign partner will be queried and used by DHS components and other IDENT/HART users for purposes incompatible with the original purpose of the enrollment.

**Mitigation:** This risk is mitigated. In the BDSP implementation model, biometric and any corresponding biographic information collected by a foreign partner is automatically enrolled in IDENT/HART whether there is a "match" or "no match" to any existing fingerprint records contained in IDENT/HART. Despite retaining foreign partner "no match" information, DHS and any other IDENT/HART users may only query this information for purposes related to border security, immigration decision-making, law enforcement activities with a nexus to the U.S. border, countering transnational crimes and organizations, detecting terrorism, and preventing and detecting crimes considered felonies under U.S. law or which render an individual inadmissible under the Immigration Nationality Act (INA), consistent both with applicable System of Records Notices and the bilateral information sharing agreement or arrangement.

## 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.*

Information exchanged between DHS and IBIS partners is expected to reflect the most up-

to-date and accurate information about an individual held by the parties to the agreement. The procedures for implementing information sharing agreements will require foreign partners to ensure that any inaccurate personal information is brought to the partner's attention in a timely manner, preferably within 48 hours of determining that inaccurate information was transferred. Anytime DHS is informed that it has received inaccurate information it will correct, annotate, block, or delete the incorrect information as appropriate and take measures to avoid relying upon any of the erroneous information. To ensure both DHS and the partner country are complying with the data integrity provisions of the agreement, the agreements require routine review and auditing of the data sharing and adherence to the agreement. Additionally, the DHS Chief Privacy Officer may choose to conduct a Privacy Compliance Review.

Data retention under the BDSP model ensures DHS's subsequent interactions with the individual are based on complete and accurate information. Information sharing agreements and arrangements may also authorize DHS to retain information about individuals the providing country has identified as representing a threat to public security, regardless of whether DHS has previously encountered them. Both circumstances support the data quality principle that personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept current.

**Privacy Risk:** A risk exists that a partner country will not inform DHS that data it provided was inaccurate.

**Mitigation:** This risk is partially mitigated. DHS cannot fully mitigate the risk that a foreign government will fail to correct inaccurate information as required under the applicable agreement. USCIS, CBP, and ICE provide individuals with opportunities for administrative and judicial redress regarding the accuracy of their data, such as through DHS TRIP. Officials from these agencies are instructed to consider the totality of information, including information collected directly from the individual, prior to making a final law enforcement, border enforcement, or immigration decision.

OBIM has built additional accuracy measures for matching IDENT/HART records against partial, incomplete, or differently oriented fingerprints. Because of these and other possible anomalies, accurate identification is less reliable than for complete fingerprint records. To ensure accurate matches for such prints, IDENT/HART returns a limited number of possible matches to trained and experienced fingerprint examiners in its Biometric Support Center (BSC). Biometric Support Center fingerprint examiners make a final determination on whether the submitted print matches any of the fingerprints currently retained in IDENT/HART. If BSC examiners confirm that there is a match in IDENT/HART, the submitting agency can request additional information on the individual.

**Privacy Risk:** There is a risk that partner countries lack expertise on collecting and maintaining quality biometric data.

**Mitigation:** This risk is mitigated. DHS employs security sector assistance to purchase quality biometric collection and storage equipment for use by the BDSP partner country, and to properly train foreign partner officials on using and maintaining the equipment and systems. DHS extensively trains operational end users and technical experts in the partner government when deploying the system and periodically thereafter to ensure they are making appropriate and high-quality biometric collections.

## 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*.

Under the BDSP implementation model, as DHS procures and establishes the partner's biometric system and configures it to be integrated with IDENT/HART, DHS deploys equipment and software with data and cyber security measures equivalent to those employed domestically to its source systems. DHS uses modern technical solutions to protect all shared information, covering a wide variety of techniques and technologies ranging from access controls to cyber security measures. The biometric information sharing agreements and DHS implementation activities ensure that the necessary technical and organizational measures are used to protect personally identifiable information against accidental or unlawful destruction, accidental loss, unauthorized disclosure, alteration, access, or any unauthorized processing of the data. Each country must take reasonable measures so only authorized individuals have access to the personally identifiable information exchanged.

Further, partner countries will be required to report any privacy incidents, including unauthorized access or disclosure of DHS information. Due to system integration in the BDSP model, IDENT/HART maintains logs of data sent and received, minimizing the reliance on partner record keeping and cooperation. The country providing information is entitled to ask the country receiving information about what was done with the data and any results generated. These logs may be useful in revealing privacy incidents or unauthorized disclosures by a partner country. If after an examination of a partner country's implementation of the agreement, including the safeguards within it, DHS concludes that a partner country is not a responsible steward of the personally identifiable information with which DHS entrusts it, then DHS may consider suspending or terminating the agreement. Detection of non-compliance can come either in response to an event that illuminates a deficiency in a foreign government's practices or as part of a review of the agreement. All agreements require a "regular" and/or "periodic" review of the implementation of the agreement. While the exact schedule is left for DHS and each foreign

government to determine, they generally occur no less frequently than every five years after the agreement is fully implemented, unless a specific event requires an earlier review. The review generally considers whether data that should have been destroyed has been retained, whether data has been shared inconsistent with the agreement, and whether there was any inappropriate access to data, among other matters.

The countries must establish procedures for automated querying of fingerprints using appropriate technology to ensure data protection, security, confidentiality, and integrity; employ encryption and authorization procedures that are recognized by each country's respective expert authorities; and ensure that only permissible queries are conducted.

**Privacy Risk:** There is a risk that the transmission of data between DHS and IBIS partner countries will be intercepted or compromised by a third party.

**Mitigation:** This risk is partially mitigated. DHS mitigates this risk by using an approved and accredited electronic gateway, which uses high security encryption protocols to provide biometric query and response capabilities. The transmissions are conducted over the public Internet using a VPN connection to provide a secure "tunnel" between DHS and foreign partners. Despite the robust protocols of an electronic gateway, DHS cannot fully mitigate any security risks associated with its own or partners' technology and processes.

DHS places limitations on third-party sharing by limiting the amount of data shared based on specific circumstances described in information sharing access agreements, and by conducting periodic reviews, as appropriate, of the use of the data with end users.

## 8. Principle of Accountability and Auditing

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

DHS's international information sharing agreements require each country to maintain a log of the transmission and receipt of data communicated to the other country. This log serves to: a) ensure effective monitoring of data protection in accordance with the national law of the respective country; b) enable the countries to effectively correct, block, or delete certain data; c) inform the querying country of the result obtained from the supplied data; and d) ensure data security.

At a minimum, the log must include: a) information on the data supplied; b) the date on which the data was supplied; and c) the recipient of the data in case the data is supplied to other entities. The countries must protect the log with suitable measures against inappropriate use and maintain it for a pre-determined period.

The agreements also require the countries to regularly engage in consultations to, in part, review the number of queries made and percentage of matches, and share, to the extent practical,

additional statistics and case studies demonstrating how the exchange of information under the agreement has assisted with law enforcement, immigration adjudication, and border enforcement.

The agreements further require the countries to consult one another on any privacy incidents (including unauthorized access or disclosure) involving personally identifiable information shared under the agreement, and remedial actions taken in response to any such incidents.

**Privacy Risk:** There remains a risk that a partner country may not report a privacy incident to DHS, including unauthorized access or disclosure of personally identifiable information.

**Mitigation:** This risk is partially mitigated. As discussed, countries are required to keep a log of data sent and received. Either country is entitled to inquire with the partner country about how the data was used and the results generated. These responses may be useful in revealing privacy incidents or unauthorized disclosures by a partner country. However, it is dependent on the partner country's willingness to comply with the request and to be transparent about prior privacy incidents involving DHS-supplied data. In the event DHS concludes that the country is not a responsible steward of the personally identifiable information with which it is entrusted, then terminating the agreement, in accordance with its terms, may be an option for consideration by DHS.

## Contact Officials

Bob Paschall
Principal Deputy Assistant Secretary, Office of International Affairs
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

## Responsible Officials

Serena Hoy
Assistant Secretary, Office of International Affairs
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

## 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