Privacy Impact Assessment

for the

DHS International Biometric Information Sharing (IBIS) Program

DHS Reference No. DHS/ALL/PIA-095

November 2, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (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 enhance cooperation between DHS components and foreign partners in 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 created IBIS to improve the Department's and its foreign partners' ability to more definitively establish 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) considers the privacy risks and applicable mitigation strategies associated with implementing this Departmental program.

Introduction

Notwithstanding the Coronavirus 2019 (COVID-19) pandemic, global migration has increased significantly in the last five years as increasing numbers of migrants leave their home countries for economic opportunities, to flee conflicts and violence, or to join family members abroad. Individuals with malicious intent—such as terrorists or transnational criminals—may present themselves as legitimate asylum seekers, refugees, and migrants, posing a public security risk to the United States and its partners while also harming lawful travelers and vulnerable people in dire need of protection and assistance. The United States, and the global community at large, need to improve capabilities to assess whether an individual encountered in a law enforcement investigation related to immigration or border security, at the border, or during an immigration application process poses a risk to the national security or public safety of its people. Biometric data sharing assists in identifying fraud, transnational criminals, irregular migratory patterns, illicit smuggling pathways, and the enhancement and tracking of terrorism-related information. Fingerprints are a unique identifier that are used to positively identify individuals by federal, state, and local law enforcement agencies, as well as foreign partner agencies. Immigration and law enforcement records that include fingerprints bolster the integrity of our respective immigration systems and border security while facilitating access to protection for legitimate refugees and asylum seekers and access to legitimate migration and travel pathways. Once a fingerprint-based match has been established, the subsequent sharing of other biometric modalities and associated biographic information can provide useful investigative leads or support future manual or

automated identity verification.

IBIS facilitates fingerprint-based bilateral biometric and biographic information sharing between the United States and a foreign partner. IBIS will only be used for activities 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).[1] IBIS enables automatic comparison of the fingerprints collected by DHS or a foreign partner on international travelers, suspected criminals, asylum seekers, irregular migrants, refugees, applicants for visa and/or immigration benefits, and other individuals encountered by government representatives in the border and immigration context 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 to determine whether they pose a threat to the security or welfare of the United States or its people. It similarly allows its 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 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 regular migration.

Once DHS concludes an appropriate information sharing agreement or arrangement that includes privacy protections and safeguards, foreign partners' records can be vetted or compared against information held in the Automated Biometric Identification System (IDENT)[2] or successor system, Homeland Advanced Recognition Technology (HART),[3] both of which are controlled by the DHS Management Directorate (MGMT) Office of Biometric Management (OBIM). IDENT and HART include fingerprint sets of over 280 million individuals and contain records associated with individuals on the known or suspected terrorist watchlist. The goal of IBIS is to improve

[1] Throughout this PIA, references to law enforcement encounters and investigations should be read in this context. Additionally, references to "criminal" or "crime" should be understood to mean individuals reasonably suspected of acts which are considered a felony under U.S. law, i.e., crimes for which the penalty is more than one year of imprisonment, or other acts which would constitute a crime rendering the individual inadmissible or removable under U.S. law. In forthcoming IBIS agreements with foreign partners, DHS will ensure it is not receiving information that is inconsistent with U.S. values.

[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 PIA prior to the release of each Increment.

global and U.S national security, through the identification of fraud, transnational criminals, irregular migration patterns, illicit smuggling pathways, and the enhancement and tracking of terrorism related information.

The specific data elements exchanged with the foreign partners will vary based on the particular agreement but may include data such as: surnames; first names; former names; other names; aliases; alternative spelling of names; sex; date and place of birth; current and former nationalities; passport data; numbers from other identity documents; other biometric modalities such as facial images; and criminal, police, and immigration records.

The information-sharing made possible by IBIS fulfills statutory mandates[4] and U.S. obligations under United Nations (UN) Security Council resolutions,[5] and represents the culmination of years of work across decades and Administrations to effectively and efficiently identify threats to public safety and national security of the United States and its partners.[6]

DHS's authority to exchange information with foreign governments derives from Section 101 of the Homeland Security Act of 2002 (6 U.S.C. § 111), which defines the Department's primary mission in part as "prevent[ing] terrorist attacks within the United States" and "reduc[ing] the vulnerability of the United States to terrorism." DHS has both explicit and inherent mandates to share information with foreign governments, particularly where sharing information aids in accomplishing DHS's mission. For example, DHS is authorized to exchange information or documents with foreign customs and law enforcement agencies under 19 U.S.C. § 1628 (exchange of information), provide information to foreign partners and allies,[7] and exchange passenger information with foreign governments as well as designate certain databases for use in screening by foreign governments.[8]

The Homeland Security Act of 2002[9] established the Office of International Affairs (OIA) within the Department to "promote information and education exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security . . . [to] include . . . [e]xchange of expertise on terrorism prevention, response,

---

[4] *See, e.g.*, 6 U.S.C. § 111, 19 U.S.C. § 1628, 6 U.S.C. § 485, 8 U.S.C. § 1187(c)(2)(F).
[5] UN Security Council Resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2322 (2016) and 2396 (2017), which call upon UN Member States to develop and implement systems to collect biometric data to identify terrorists, prevent the movement of terrorists or terrorist groups by effective national border controls and through measures for preventing fraudulent use of identity papers and travel documents, and to share such information responsibly.
[6] *See e.g.*, National Security Presidential Memorandum 9 (NSPM 9), Subject: Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise (February 6, 2018); National Security Presidential Memorandum 7 (NSPM 7), Subject: Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans (October 4, 2017); Homeland Security Presidential Directive 24 (HSPD 24), Subject: Biometrics for Identification and Screening to Enhance National Security (June 5, 2008).
[7] *See* 6 U.S.C. §§ 321d(b) & 485(f)(2)(B)(vii).
[8] *See* 8 U.S.C. § 1187(c)(2)(F) & (G).
[9] § 879(b) (codified as amended at 6 U.S.C. § 459(b)).

and crisis management." In 2017, Congress established the Office of Strategy, Policy, and Plans (PLCY), which contains the Office of International Affairs. The Office of International Affairs coordinates DHS's international activities, including the IBIS program.

IBIS helps DHS deliver on a long-standing Congressional intent expressed in statute[10] to "develop an intergovernmental network of interoperable electronic data systems" to access data that is needed "to screen visa applicants and applicants for admission to the United States." Appropriate technology now exists to achieve this statutory intent, and IBIS will help to successfully implement it.

Congress emphasized that a mandated entry and exit data system "shall be able to interface with law enforcement databases for use by Federal law enforcement to identify and detain individuals who pose a threat to the national security of the United States."[11] In directing the United States Visitor and Immigrant Status Indicator Technology (US-VISIT)[12] to operate the "biometric entry-exit data system," Congress in 8 U.S.C. § 1365b also directed US-VISIT to "integrate" relevant datasets and to "add information" to IDENT, thereby authorizing US-VISIT to receive and retain relevant information to the entry and exit data system to further the law enforcement and national security missions of the Department. Importantly, 8 U.S.C. § 1365b requires US-VISIT to make relevant information available to stakeholders in "real-time," explicitly mandating that US-VISIT use available technological methods – including automated sharing – to achieve real-time sharing.

Growth of IBIS will also improve DHS's ability to detect terrorist travel, execute the National Counterterrorism Strategy (2018)[13] and the National Strategy for Combatting Terrorist Travel (2019),[14] and similarly enhance the capabilities for foreign partners.

The Visa Waiver Program (VWP) is a rigorous security partnership that promotes secure travel to the United States while also facilitating U.S. passport-holders' travel to VWP partner nations. No other program enables the U.S. Government to conduct such broad and in-depth assessments of foreign security standards and operations. The VWP is administered by DHS in consultation with the U.S. State Department and permits citizens of [currently] 40 designated countries[15] to travel to the United States for business or tourism for stays of up to 90 days without

[10] *See* 8 U.S.C. § 1772.
[11] *See* 8 U.S.C. § 1365a.
[12] OBIM was created in March 2013, replacing the US-VISIT Program. This transition to OBIM assumed many of US-VISIT's roles, responsibilities, and authorities for the processing of biometrics. Public Law 113-6, Homeland Security Appropriations Act, Public Law 115-31, Div. F., Section 301.
[13] National Strategy for Counterterrorism of the United States of America (2018), https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf.
[14] National Strategy to Combat Terrorist Travel of the United States of America (2019), https://www.hsdl.org/?view&did=821737.
[15] With respect to all references to "country" or "countries" in this document, the Taiwan Relations Act of 1979,

a visa.[16] In return, VWP-designated countries must permit U.S. passport-holders to travel for business or tourism to the partner VWP country for a similar length of time without a visa.[17] Since its inception in 1986, the VWP has evolved into a comprehensive security partnership with many of the United States' closest allies. DHS uses a risk-based, multi-layered approach to detect and prevent terrorists, criminals, and other *mala fide* actors from traveling to the United States. This approach incorporates regular, national-level risk assessments concerning the impact on U.S. national security, immigration, and law enforcement interests of each program country's participation in the VWP. It also includes comprehensive vetting of individual VWP travelers prior to their departure for the United States, upon arrival at U.S. ports of entry, and during subsequent encounters within the United States.

Eligibility for a country's designation in the VWP is defined in Section 217 of the INA (including as amended most recently by the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015).[18] Among other requirements, the Passenger Information Exchange provision of the statute specifies that any country seeking to participate in the VWP enter "into an agreement with the United States to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens, and fully implements such agreement."[19]

DHS in consultation with the Department of State, assessed that establishing direct biometric information sharing partnerships under the IBIS Program would meet the intent of the eligibility requirements for designation in the VWP as enumerated in 8 U.S.C. § 1187(c)(2)(F)

Pub. L. No. 96-8, Section 4(b)(1), provides that "[w]henever the laws of the United States refer or relate to foreign countries, nations, states, governments, or similar entities, such terms shall include and such laws shall apply with respect to Taiwan." 22 U.S.C. § 3303(b)(1). Accordingly, all references to "country" or "countries" in the Visa Waiver Program authorizing legislation, Section 217 of the Immigration and Nationality Act, 8 U.S.C. § 1187, are read to include Taiwan. This is consistent with the United States' one-China policy, under which the United States has maintained unofficial relations with Taiwan since 1979.

[16] *See* https://www.dhs.gov/visa-waiver-program-requirements for full list of VWP countries as well as additional information on VWP program requirements.

[17] 8 U.S.C. § 1187 (a)(2).

[18] *See* generally 8 U.S.C. § 1187 (providing that the Secretary of Homeland Security, in consultation with the Secretary of State, may designate into the VWP a country that: (1) Has an annual nonimmigrant visitor visa (i.e., B visa) refusal rate of less than three percent, or a lower average percentage over the previous two fiscal years; (2) Accepts the repatriation of its citizens, former citizens, and nationals ordered removed from the United States within three weeks of the final order of removal; (3) Enters into an agreement to report lost and stolen passport information to the United States via INTERPOL or other means designated by the Secretary; (4) Enters into an agreement with the United States to share terrorism and serious criminal information; (5) Issues electronic, machine-readable passports with biometric identifiers; (6) Undergoes a DHS-led evaluation of the effects of the country's VWP designation on the security, law enforcement, and immigration enforcement interests of the United States; and (7) Undergoes, in conjunction with the DHS-led evaluation, an independent intelligence assessment produced by the DHS Office of Intelligence and Analysis (on behalf of the Director of National Intelligence)).

[19] 8 U.S.C. § 1187 (c)(2)(F). The requirement to implement the agreement was added by the Visa Waiver Improvement and Terrorist Travel Prevention Act of 2015 (Pub. L. No. 114-113), enacted on December 18, 2015.

Section 217 of the Immigration and Nationality Act (INA)[20] (including as amended most recently by the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015). As a result, DHS and State announced the new Enhanced Border Security Partnership (EBSP) biometric information sharing requirement which all VWP countries will need to complete for initial and continued designation in the VWP. DHS therefore intends to prioritize implementing IBIS relationships with VWP countries over the next five years and may also pursue IBIS relationships with non-VWP countries if appropriate.

Three DHS components are primarily responsible for screening travelers and immigration benefit applicants to determine eligibility: U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), and U.S. Immigration and Customs Enforcement (ICE). These three components are expected to be the components that will submit queries most actively under IBIS for the immigration and border security functions described above. While other DHS components with border security and related functions, such as the Transportation Security Administration, U.S. Secret Service, and U.S. Coast Guard, may also submit IBIS-related queries, to the extent DHS components other than CBP, USCIS, and ICE become routine users, this PIA may be updated to reflect the shift in routine users and assess any consequential privacy risks and mitigations. Additionally, each component that participates in IBIS will complete its own Privacy Threshold Assessment (PTA) before the component makes routine use of the program.

Each component, pursuant to its legal authorities, collects and uses fingerprints from individuals seeking entry to the United States, seeking an immigration benefit, or making another immigration related request, as part of the component's screening process or from those subject to immigration, administrative, or criminal law enforcement actions. The DHS Automated Biometric Identification System (IDENT)[21] — to be replaced by the Homeland Advanced Recognition Technology System (HART)[22] — is DHS's biometric system for storing and processing biometric and limited biographic data for national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. OBIM and PLCY, in collaboration with component data owners, facilitate IDENT/HART-based information sharing under the IBIS Program. PLCY, which leads and coordinates international engagement and negotiations on behalf of the Department, negotiates information-sharing agreements and arrangements with foreign countries in cooperation with the Department of State and with technological and analytical support from OBIM and other DHS components as appropriate.

---

[20] 8 U.S.C. § 1103, *et. seq*. The VWP provisions have been codified at 8 U.S.C. § 1187.
[21] *See supra* note 11.
[22] *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 PIA prior to the release of each Increment.

Because information received through the IBIS program will be stored and queried in IDENT/HART, this PIA builds on the functionality of IDENT/HART. The HART Increment 1 PIA covers the core foundational infrastructure and baseline existing functionality in IDENT that ensures continuity of services without disruption to existing IDENT users. Due to the privacy risks associated with the collection, retention, use, and dissemination of biometric data the DHS Privacy Office included recommendations throughout the "Privacy Impact Analysis" section of the HART Increment 1 PIA, which are also relevant to the information sharing discussed in this PIA. Those recommendations address Transparency, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, and Accountability and Auditing.

The Information Sharing Process

The goal of this information sharing process is to support DHS's mission to vet relevant border and immigration-related fingerprints collected by DHS against relevant border and immigration-related fingerprints collected by the other country to help the United States and the foreign partner in border screening and border security encounters, to identify travelers presenting a threat to the security or welfare of the respective countries, and identify perpetrators of identity fraud in the immigration process. Reciprocity is a principle of international relations and therefore will be part of IBIS agreements or arrangements. Although U.S. law typically does not require DHS to reciprocate by sharing U.S. person information, it is likely that any information sharing agreement or arrangement under this partnership will be reciprocal and therefore permit the sharing of information on U.S. persons. DHS welcomes reciprocity and where it has agreements supporting this sharing will provide relevant identity, criminal history, and immigration data to an IBIS partner when a fingerprint-based search matches a DHS record — as permitted by law and policy — to support the IBIS partner's processing of applications received by its government for international travel, admission, entry, or immigration status.

There are multiple technical implementation models available depending on the existing capabilities of the IBIS partner and the terms of the international agreements. This PIA pertains to Enhanced Border Security Partners where DHS can establish direct interoperability with the partner's existing biometric system. This PIA will be updated to account for other technical implementation models.

For countries with an existing domestic biometric capability, the information sharing process at DHS begins when one country (hereafter "querying country") encounters and has a need to screen an individual to administer or enforce national laws applicable to people entering, staying in, or leaving that country's jurisdiction. The querying country collects the fingerprints of the subject and queries the biometric system of the other country (hereafter "receiving country") to determine if the receiving country has previously encountered this individual. Queries are made on an individual case-by-case basis and in compliance with the querying country's national laws, policies, and the international agreement or arrangement between the querying and receiving

countries. The receiving country indicates whether a fingerprint match exists in its biometric system by responding "match" or "no match" to the querying country. When there is no match, or the receiving country's national law prohibits the disclosure of information that would normally constitute a "match," the receiving country will return a "no match" response. In the event of a "no match," the receiving country deletes the prints and exchanges no further information. 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,[23] T visa applicant (nonimmigrant status victim of human trafficking),[24] or someone applying for a U visa (nonimmigrant status victim of a qualifying crime),[25] except in certain circumstances,[26] because the data of such individuals are protected by law.[27] Similarly, DHS will share Asylum, Refugee, Temporary Protected Status,[28] and Legalization/LIFE Act/Special Agricultural Worker[29] information with partner countries only in accordance with established law

[23] Under VAWA, as amended, certain persons who have been battered or subjected to extreme cruelty by a qualifying relative may self-petition, allowing them to remain in the United States, apply for lawful permanent resident (LPR) status as an approved VAWA self-petitioner, and eventually apply for naturalization. VAWA self-petitioners include: the spouse, child or parent of an abusive U.S. citizen; the spouse or child of an abusive LPR; the conditional resident spouse or child of an abusive U.S. citizen or LPR; the spouse or child of an alien eligible for relief under the Cuban Adjustment Act, the Haitian Refugee Immigration Fairness Act, or the Nicaraguan Adjustment and Central American Relief Act; and the spouse or child eligible for suspension of deportation or cancellation of removal due to abuse by a U.S. citizen or LPR. *See* INA Section 101(a)(51) (defining "VAWA self-petitioner").

[24] T nonimmigrant status is available to certain victims of a severe form of trafficking in persons, as defined in section 103 of the Victims of Trafficking and Violence Prevention Act (VTVPA) of 2000, who are physically present in the United States on account of trafficking and who have complied with any reasonable requests for assistance in a law enforcement investigation or prosecution (with limited exceptions). See Immigration and Nationality Act (INA) Section 101(a)(15)(T). T nonimmigrant status allows victims of human trafficking to remain in the United States for up to four years (or longer if a limited exception applies), receive work authorization, and, if certain conditions are met, apply for adjustment of status to that of an LPR.

[25] U nonimmigrant status is available to certain victims of criminal activity designated in INA Section 101(a)(15)(U) (qualifying crimes) who have suffered substantial mental or physical abuse as a result of being a victim of criminal activity, possess relevant information concerning the crime, and have been helpful, are being helpful, or are likely to be helpful to law enforcement or government officials in the investigation or prosecution of the criminal activity. U nonimmigrant status allows victims to remain in the United States for up to four years (or longer if a limited exception applies), receive work authorization, and, if certain conditions are met, apply for adjustment of status to that of an LPR.

[26] 8 U.S.C. § 1367. For example, the Secretary of Homeland Security or the Attorney General may authorize the disclosure of information involving a "special protected class" to certain agencies, including law enforcement officials for law enforcement purposes or to national security officials for a national security purpose. *Id.* § 1367(b)(2), (8).

[27] 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)).

[28] Temporary Protected Status information (8 U.S.C. § 244, 8 C.F.R. § 244.16). Individuals who have applied for Temporary Protected Status (TPS), a temporary benefit afforded to individuals already in the United States from certain designated countries that have experienced ongoing armed conflict (civil war), environmental disasters (earthquakes), epidemics (Ebola), or other extraordinary conditions.

[29] Legalization/LIFE Act/Special Agricultural Worker information [INA § 245A(c)(4), (5)/8 U.S.C. § 1255a(c)(4),

and policy.

When an IBIS partner country sends DHS a fingerprint for query for purposes consistent with the bilateral agreement or arrangement, that request automatically searches against fingerprints in IDENT/HART. If there is biographic information associated with a fingerprint match that is permissible to share under U.S. law and DHS policy, IDENT/HART returns a "match" response, accompanied with the biographic data approved for sharing.[30] OBIM automatically determines which data elements may be shared with IBIS partner countries based on the foreign partner-specific controls built into IDENT/HART business rules as established by DHS policy with the concurrence of the DHS component who owns the record. Any information that OBIM determines is not authorized for disclosure under U.S. law or DHS policy is automatically filtered out of IDENT/HART responses to the foreign partner.[31] Only data contained in IDENT/HART may be returned automatically.

When there is a fingerprint match, the countries may exchange the type of information listed in Appendix A according to their respective laws and policies and as defined in the applicable international agreement or arrangement to assist in law enforcement or immigration benefit adjudication decisions. Once a fingerprint match has been established and appropriate additional information exchanged, the arrangement may require the searched party to delete the fingerprints used by the querying party to conduct the original search. This requirement may appear in the applicable international agreement or arrangement, ensuring foreign partners only retain U.S. information that is relevant and necessary to their operations. This information may be exchanged at the same time as the "match" response (DHS's preferred approach) or in a subsequent communication (when necessary to align with the foreign partner's domestic processes).

DHS components with immigration and border screening and related criminal investigation missions, including USCIS, ICE, and CBP, may also initiate searches of the IBIS partner biometric

(5); INA § 210(b)(5), (6)/ 8 U.S.C. § 1160(b)(5), (6); 8 C.F.R. § 210.2(3)(e)]. Individuals who were unlawfully residing in the United States before 1982, or who performed seasonal agricultural work in the United States before 1986.

[30] Information disclosed upon a match is outlined in Appendix A and may, when available and appropriate, include data such as surnames, first names, former surnames, other surnames, aliases, alternative spelling of names, sex, date and place of birth, country of origin, current and former citizenships, current and former countries of residence, passport data, information from other identity documents, immigration status, law enforcement or national security lookouts and biometric data.

[31] The HART Increment 1 PIA contains the following Privacy Office Recommendation: OBIM should establish a governance board made up of OBIM, DHS authorized users and providers, and DHS oversight offices (i.e., DHS Privacy Office, DHS Office of Civil Rights and Civil Liberties, Office of the General Counsel) to ensure that internal and external collection and dissemination of HART records is aligned with the data owner authorities and policies as set out in the business rules. The governance board should also review whether business rule configurations align with ISAAs with OBIM or agreements or arrangements with DHS that contemplate sharing from the HART system. The HART Increment 1 PIA also has this 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.

system using a similar process for purposes consistent with the applicable international arrangement. Through DHS OBIM, these components submit queries to a foreign partner through the External Identify Service and receive an automated response.[32]

Each DHS component sending queries to foreign partners under IBIS via IDENT/HART completes its privacy compliance documentation and develops its own procedures and operational policies to determine when and how that component will initiate a query to a foreign partner. The policies and procedures also address the technical mechanism or electronic gateways that components will use to exchange query and response data with OBIM. The privacy compliance documentation and procedures and policies are finalized before these components initiate foreign partner queries under IBIS via IDENT/HART. CBP plans to direct IDENT to send queries to a foreign partner through the Automated Targeting System (ATS);[33] ICE uses the Biometric International Query Service (BIQS);[34] and USCIS uses the Customer Profile Management Service (CPMS).[35] Queries from any of these Component's systems will elicit the same response.

The "match" or "no match" response message and associated information listed in Appendix A provided by the foreign partner is retained in IDENT/HART as a foreign partner encounter associated with that identity and subsequently provided to the requesting component that initiated the query for use as part of its investigation or benefit adjudication, according to the OBIM data access and security requirements.[36]

If OBIM is unable to use the External Identify Service to send automated queries to certain countries (for example as part of a pilot exchange prior to establishing an automated process), then OBIM, at the request of the searching DHS component, would extract the fingerprint images from IDENT/HART and send the queries to those countries through encrypted email. Responses from those countries are also received through encrypted email and passed via secure email to the component who requested the query.

OBIM runs a daily match report of filtered and non-filtered matches in IDENT/HART to

---

[32] *See* DHS/OBIM/PIA-004 Homeland Advances Recognition Technology System Increment 1 Appendix B.
[33] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE LAW ENFORCEMENT INFORMATION SHARING SERVICE, DHS/ICE/PIA-051 (2019), *available at* https://www.dhs.gov/privacy-documents-ice.
[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[36] The Data Access and Security Control (DASC) requirements serve as the basis of OBIM's compliance with oversight responsibilities (e.g., privacy, policy, civil rights, civil liberties, and legal). HART uses the same DASC requirements for automated filtering that IDENT uses; therefore, the technological aspect of the filtering rules will continue as they are in both IDENT/HART. The DASC requirements will also remain configurable in IDENT/HART to meet the ever-changing landscape of data dissemination requirements from the Department.

foreign partner queries and manually imports information from the report into the Technical Reconciliation Analysis Classification System (TRACS).[37] This is done to enable internal notification to DHS and non-DHS OBIM clients on match rates and disclosure rates to a foreign partner. In addition to assisting with reporting and tracking, daily match reports enable research on overall query and response volumes with a foreign partner. TRACS[38] is a tool used by OBIM analysts for manual coordination and analysis of all international queries and responses. TRACS is not involved in the transmission of query data between IDENT/HART and a foreign partner or between IDENT/HART and a DHS component.[39]

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. Depending on foreign partner technical requirements, data entering the DHS network through the CBP Gateway can be sent either directly to IDENT/HART, or to CBP ATS to serve as a proxy between IDENT and a foreign partner's automated biometric system.[40] 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.[41]

Where ATS serves as a proxy to the IDENT/HART system it only records transaction details for auditing purposes and information shared by the foreign partner after a match is established. In this case, CBP merges the information provided to DHS by the foreign partner with existing CBP data for manual review to determine whether to engage in further operational

[37] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT APPENDICES FOR THE TECHNICAL RECONCILIATION ANALYSIS CLASSIFICATION SYSTEM (TRACS), DHS/OBIM/PIA-003 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[38] The specific personal identifiable information (PII) in a TRACS record varies depending upon what information the source records contain. PII contained in TRACS may include name, date of birth (DOB), country of birth, document numbers/types, encounter date, reason fingerprinted, foreign partner unique identifier, fingerprint identification number (FIN), immigration information, border crossing information, and free-form text fields for analyst findings. TRACS does not contain any biometric data and is not the original source for any PII.

[39] TRACS is not used in the automated response back to a foreign partner. TRACS is not connected to IDENT and is not involved in the electronic gateway technical process. IDENT generates a daily match report of filtered and non-filtered matches in IDENT. OBIM then imports that data into TRACS for notification to owners of data in IDENT.

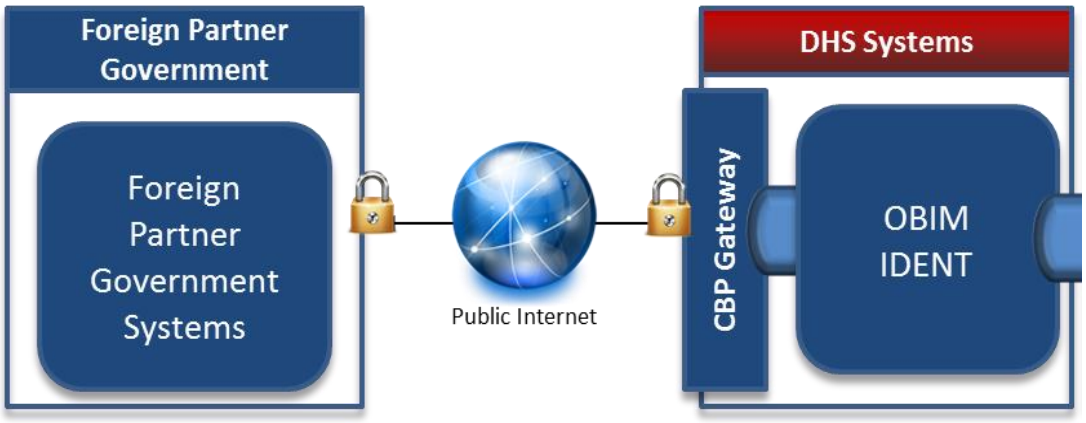
[40] *See supra* note 17.

[41] 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.

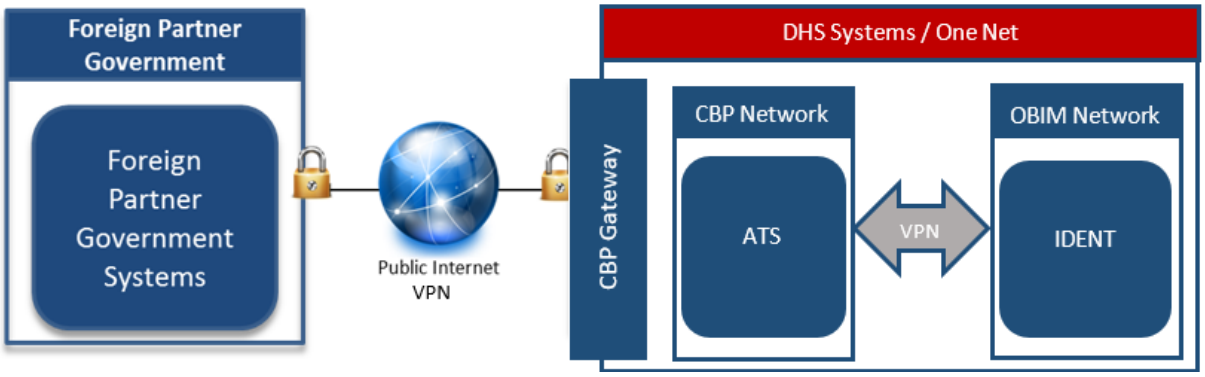
cooperation with the foreign partner regarding the match.[42] The information is clearly marked in ATS as originating from the foreign partner.

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 direct connections to IDENT/HART biometric databases:



The diagram below depicts the current state of bi-directional (two-way) flow of information using ATS as a proxy:



DHS intends to implement the information-sharing described in this PIA in a phased approach,

[42] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

consistent with each IBIS partner's capabilities and resources.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[43] 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 DHS 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.[44]

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.[45] 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[46] and the Homeland Security Act of 2002 Section 222.[47] This PIA examines the privacy impact of DHS' IBIS operations as they relate to the FIPPs. However, because the specific implementing agreements and technical connections have not yet been established with all IBIS countries, it is unclear specifically what identity information each IBIS country will share upon a biometric match, or whether they will choose to query DHS when they process any applications to their governments for travel, admission, entry, or immigration status.

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 PIA and the related component PIAs that discuss border enforcement and vetting of visa and immigration benefit applicants, applicable System of Records Notices (SORN), and public statements attesting to the inclusion of foreign countries in the VWP or other information sharing statements with the United

[43] 5 U.S.C. § 552a.
[44] 6 U.S.C. § 142(a)(2).
[45] *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 PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[46] 44 U.S.C. § 3501 note.
[47] 6 U.S.C. § 142.

States. 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.[48] 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 and its components will disclose fingerprints to conduct a query of IBIS country databases. DHS has provided transparency about the potential disclosure of PII via the relevant SORN(s) and PIA(s) for the program that originally collected the information as well as, when applicable, the DHS website and individual applications/forms.

The following SORNs from the IDENT/HART source system owners — ICE, CBP, and USCIS — cover the DHS data to be eventually shared under IBIS in response to a matching query:

- 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;[49]
- 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;[50]
- 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;[51]
- 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

[48] *See* https://www.dhs.gov/freedom-information-act-foia.
[49] *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.
[50] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[51] *See* DHS/USCIS-018 Immigration Biometric and Background Check (IBBC), 83 Fed. Reg. 36950 (July 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities;[52] 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 SORNs, such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.[53]

In response to a match to a fingerprint-based query, certain additional PII consistent with Appendix A (e.g., biographic information, encounter-related information) may be provided automatically by the receiving country to the querying country. If the queried fingerprint does not match the holdings in the receiving country's automated biometric system, then the fingerprint is not retained by the receiving country. If the fingerprints are provided on a country's own initiative when the country has reason to believe the individual may be planning to commit a terrorist act or commit a felony, the prints and associated biographic data are retained by the receiving country.[54]

Following a fingerprint match, DHS may share data elements consistent with Appendix A, 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.[55]

Under certain agreements, including the Preventing and Combating Serious Crimes (PCSC) agreements, IBIS partner countries may also, in compliance with their respective national laws, share PII — 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.[56] 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;

---

[52] *See* DHS/ALL-041 External Biometrics Records (EBR) System of Records, 83 Fed. Reg. 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[53] *See* DHS/ALL-043 External Biometric Administrative Records (EBAR) System of Records, 85 Fed. Reg. 14955 (March 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[54] *See* e.g., Model PCSC Agreement, Article 11, "Supply of personal and other data in order to prevent serious and terrorism offenses," commonly referred to as the spontaneous sharing provision.
[55] *See supra* note 27.
[56] The HART Increment 1 PIA contains the following Privacy Office Recommendation: OBIM should establish a baseline quality for enrollment of all biometric modalities and provide guidance as to reliability of the modalities according to the age of the subject at the time of collection.

- 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 or shared 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 PIA, as well as the publishing of PIAs and SORNs addressing the collection, notification, and sharing of biographic and biometric information. The IDENT and HART PIAs and the EBR and EBAR SORNs provide general notice that an individual's personal information may reside in IDENT/HART. Notice is also provided through the publication of PIAs and SORNs on the underlying systems of original collection and the information shared from those systems. If required by law or policy,[57] DHS components, as well as external partners that submit information to HART and other DHS systems, provide notice to the individual at the point of collection related to storage and retention of information, including whether it is retained initially in IDENT or in the future HART. However, because this information is collected from source systems and then shared, this risk cannot be fully mitigated.

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

[57] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2017-01, REGARDING THE COLLECTION, USE, RETENTION, AND DISSEMINATION OF PERSONALLY IDENTIFIABLE INFORMATION (2017), *available at* https://www.dhs.gov/privacy-policy-guidance.

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.[58] The Judicial Redress Act (5 U.S.C. §552a note), which supplements the Privacy Act, provides citizens of 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.[59] Many, but not all, VWP countries are also covered countries for the purposes of the Judicial Redress Act. 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 to their records by filing a Freedom of Information Act (FOIA) request with the respective component or DHS FOIA office. Additional information about FOIA is available at https://www.dhs.gov/foia.

Travelers who wish to file for redress can complete an online application through the DHS Traveler Redress Inquiry Program (DHS TRIP)[60] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF) to TRIP. 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 may seek to access, correct, amend, or expunge information held by DHS's foreign partners, or otherwise seek redress from those foreign partners for the processing of information abroad, through partner countries' applicable access and redress laws

[58] 5 U.S.C. § 552a(a)(2).
[59] 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.
[60] *See* DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* www.dhs.gov/privacy.

and programs. DHS seeks assurances from its IBIS partners that they provide appropriate redress mechanisms when negotiating international agreements and arrangements. As IBIS countries provide redress points of contact, DHS intends to publish that information on its website and in Appendix B of this PIA.

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. Outside of the law enforcement context, DHS only receives information from IBIS partners on individuals it has previously encountered or is currently facing. The individuals are likely already aware that DHS has some of their personal data. However, they may be unaware that information is shared with DHS absent knowledge of the issuance of this PIA, applicable System of Records Notices (SORN), and/or public statements attesting to the inclusion of foreign countries in the VWP or other information sharing programs with the United States.

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.

Eligibility for a country's designation in the VWP is defined in Section 217 of the Immigration and Nationality Act (including as amended most recently by the Visa Waiver Program

Improvement and Terrorist Travel Prevention Act of 2015). Among other requirements, the Passenger Information Exchange section of the statute specifies that any country seeking to participate in the VWP enter "into an agreement with the United States to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens, and fully implements such agreement."[61] The purpose of DHS's VWP information sharing policy and the IBIS program is to allow DHS 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 to better screen the individual should DHS 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

[61] *See supra* note 7.

the new agreement alters the current assessment of risks and mitigations discussed in this Privacy Impact Assessment, an annex to this PIA 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. In the event of a match, and after DHS shares associated information with the foreign partner, the foreign partner must reciprocate by sharing its associated information, to include information about the encounter that motivated the 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 PIA, 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 LPR information, will be sent to DHS when there is no purpose for DHS to have that information.

Mitigation: This risk is partially mitigated. DHS would only receive information regarding U.S. citizens or LPRs 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 LPRs 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 information necessary for the IBIS partner country to make similar decisions. DHS requires foreign partners to destroy all fingerprints sent to them by DHS when it sends the fingerprints as part of a query for the purpose of conducting a search against that foreign partner's systems irrespective of whether there is a match. Where a partner's query matches a DHS record, DHS may disclose biographic and biometric information related to the fingerprint in accordance with applicable law and policy.

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)[62] schedule requires DHS to destroy law enforcement records 75 years after the end of the calendar year in which the data was gathered. EBR 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 the last use of individual's data.[63] OBIM is re-evaluating the current retention policy to determine variable retention periods for latent fingerprints and international records and will submit

[62] *See supra* note 45.
[63] *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* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

to NARA to request approval of 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 DHS or a 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 IDENT/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 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 NARA-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 NARA (under 44 U.S.C. § 2904(c)(7)), which may result in administrative, civil, or criminal penalties.[64]

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

[64] The HART Increment 1 PIA 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.

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 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.[65] 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 for Civil Rights and Civil Liberties), as appropriate.

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

[65] The HART Increment 1 PIA 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.

decisions. These purposes are documented 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 partner's authorities or the applicable international agreement or arrangement, DHS partially mitigates this risk through its engagement with each partner country. DHS develops a detailed Concept of Operations plan for implementing the information sharing agreement with all partner countries. These plans further detail when a partner may submit a request. In addition, each request is tagged with a unique category code that aligns to the purposes in the agreement or arrangement and indicates the reason why the query was submitted. 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 O/U/S 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 O/U/S 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 O/U/S is configured to receive or filter out certain types of information based on data owner-set permissions, applicable arrangements or agreements, 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 SORNs and terms of the 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 searches via manual analysis.[66] 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. DHS's ability to deploy its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, investigations, onsite inspections) become complicated when a partner is located overseas. Therefore, DHS and its partner countries will endeavor 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 mechanisms by DHS and its counterpart agency to ensure the information sharing agreements are

[66] The HART Increment 1 PIA 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 for 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 ISAAs 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.

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.

DHS's ability to deploy its traditional oversight mechanisms (e.g., Privacy Compliance Reviews, investigations, onsite inspections) is greatly limited with partners located overseas. It is for this reason that both the United States and its partner countries will work to establish strong working relationships, with regular communications, to ensure the 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 addition, all VWP member countries are, pursuant to law, evaluated to determine whether they should remain in the program no less frequently than every two years. These wide-ranging reviews afford DHS an opportunity to assess how a country is implementing its information sharing agreements, including those related to biometric interoperability. 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 PII with which it is entrusted, then DHS may terminate the 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 DHS Chief Privacy Officer may choose to conduct a Privacy Compliance Review.

Privacy Risk: A risk exists that a partner country will not inform DHS that data that country 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). BSC 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.

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.

DHS's agreements and arrangements with IBIS partners include provisions requiring the use of 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 ensure that the necessary technical and organizational measures are used to protect PII against accidental or unlawful destruction, accidental loss, unauthorized disclosure, alteration, access, or any unauthorized processing of the data. Each country must take reasonable measures so only authorized individuals have access to the PII exchanged.

Further, partner countries will be required to report any privacy incidents, including unauthorized access or disclosure of DHS information. All partner countries will be required to keep logs of data sent and received. 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 PII 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 also 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 PII 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 PII.

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 of the partner country 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 PII with which it is entrusted, then terminating the agreement, in accordance with its terms, may be an option for consideration by DHS.

Conclusion

Given the pace and volume of travel and migration around the world, it is increasingly important that DHS and its partners have effective and scalable tools to determine risk more definitively, whether at the border, in law enforcement encounters involving serious crime, and when determining eligibility of an individual applying for an immigration benefit. IBIS relationships enable rapid international sharing of identity data to support immigration and border decisions and related law enforcement investigations. DHS will continue to work to ensure that all individuals' privacy is protected in accordance with the DHS FIPPs.

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 for 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

Appendix A: Data Elements that DHS Exchanges

Last Updated: November 2, 2022

Alias first name(s)
Alias last name(s)
Aliases
Country of birth
Current immigration status
Date fingerprinted
Date of Arrival
Date of birth
Date of departure
Date of immigration application or non-biometric encounter
Date of outcome of immigration application
Date removed
Error code, if applicable
Expiry date of current leave/stay or visa
Facial image
First name, if not included in 'Last name'
Gender
Last name
Location fingerprinted
Location of Arrival
Location of departure
Match or No match
Message destination
Message origin
Other names
Outcome of immigration application
Passport nationality
Previous immigration status
Priority
Providing country event specific reference number
Providing country subject specific reference number
Reason fingerprinted
Reason for Alert

Reason for outcome of immigration application
Requesting country case type
Requesting country unique reference number
Requesting Participant event specific reference number
Requesting Participant subject specific reference number
Scan of other marked travel document pages
Transaction date
Transaction number
Transaction type
Travel document expiry date
Travel document issuing authority / country
Travel document number
Travel document type
Type of immigration application or non-biometric encounter
Visa Refusal code
Watchlist Indicator

Appendix B:
Country Agency with Agreements or Arrangements with DHS

Last updated: September 25, 2024

Australia	Australia Department of Home Affairs
Bulgaria	Ministry of Interior for the Republic of Bulgaria
Canada	Immigration, Refugees and Citizenship Canada
Cabo Verde	Ministry of Interior
Chile	Ministry of Interior and Public Security
Costa Rica	The Ministry of Public Security, Governance and Police of the Republic of Costa Rica
Croatia	Ministry of Interior for the Republic of Croatia
Cyprus	Ministry of Justice and Public Order of the Republic of Cyprus
El Salvador	Dirección General de Migración y Extranjería (DGME), Ministry of Justice and Public Security
Guatemala	Instituto Guatemalteco de Migracion
Greece[67]	Hellenic National Police
Honduras	Instituto Nacional de Migracion
Italy[68]	Ministry of Interior of the Italian Republic
Israel	Ministry of Public Security
Mexico	Instituto Nacional de Migracion
New Zealand	The Immigration Manager, Privacy Team – Immigration New Zealand
Panama	Ministerio de Seguridad

[67] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE PREVENTING AND COMBATING SERIOUS CRIME (PCSC) AGREEMENTS - GREECE AND ITALY, DHS/ALL/PIA-064 (2018), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[68] *Id.*

Poland	Commander in Chief, Polish Border Guard Commander in Chief, Polish Police
Qatar	Ministry of Interior
Romania	Ministry of Internal Affairs of Romania
United Kingdom	UK Home Office
Uruguay	Ministry of the Interior of the Oriental Republic of Uruguay