Privacy Impact Assessment

for the

DHS International Biometric Interoperability Initiative for the Visa Waiver Program

DHS Reference No. DHS/ALL/PIA-089

January 7, 2021

Homeland Security

Abstract

The Visa Waiver Program (VWP), administered by the U.S. Department of Homeland Security (DHS) in consultation with the Department of State (State), permits citizens of designated countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. The eligibility requirements for a country's designation in the VWP are defined in Section 217 of the Immigration and Nationality Act (INA)[1] (including as amended most recently by the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015). A requirement of the program is that any country seeking to participate in the VWP must enter into and implement 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.[2] To implement this program requirement in a manner consistent with law, Presidential Memoranda,[3] and DHS's increasing requirements for mission-based traveler screening, DHS has determined that all countries in the VWP and those aspiring to join must allow DHS and State to compare the fingerprints of travelers and immigration benefit applicants against their appropriate records, including identity, criminal, and terrorist records, for the purposes of border security, immigration, and traveler screening. This enhancement to the VWP screening capabilities will enable DHS to better identify individuals who pose a threat to the security or welfare of the United States. This Privacy Impact Assessment (PIA) considers the privacy risks and applicable mitigation strategies associated with implementing this Departmental policy.

Introduction

The VWP is a rigorous security partnership that promotes secure travel to the United States while also facilitating Americans' 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 State and permits citizens of currently 39 designated countries[4] to travel to the United States for business or tourism for stays

[1] 8 U.S.C. § 1103, *et. seq*. The VWP provisions have been codified at 8 U.S.C. § 1187.
[2] 8 U.S.C. § 1187(c)(2)(F).
[3] *See* https://www.whitehouse.gov/presidential-actions/presidential-memorandum-combating-high-nonimmigrant-overstay-rates/?.
[4] With respect to all references to "country" or "countries" in this document, the Taiwan Relations Act of 1979, 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.

of up to 90 days without a visa.[5] In return, VWP-designated countries must permit U.S. citizens and nationals to travel to their respective countries for a similar length of time without a visa for business or tourism purposes.[6] Since its inception in 1986, the VWP has evolved into a comprehensive security partnership with many of America's closest allies. The VWP uses a risk-based, multi-layered approach to detect and prevent terrorists, serious criminals, and other *mala fide* actors from traveling to the United States. This approach incorporates regular, national-level risk assessments concerning the impact of each program country's participation in the VWP on U.S. national security and law enforcement interests. 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 air travel 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).[7] 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."[8]

Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry Into The United States,"[9] required the U.S. Government to implement a uniform baseline for screening and

---

[5] *See* https://www.dhs.gov/visa-waiver-program-requirements for full list of VWP countries as well as additional information on VWP program requirements.
[6] 8 U.S.C. § 1187 (a)(2).
[7] *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)).
[8] 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.
[9] Executive Order 13780, 82 Fed. Reg. 13209 § 5 (March 6, 2017) (stating: "The Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall implement a program, as part of the process for adjudications, to identify individuals who seek to enter the United States on a fraudulent basis, who support terrorism, violent extremism, acts of violence toward any group or class of people within the United States, or who present a risk of causing harm subsequent to their entry. This program shall include the development of a uniform baseline for screening and vetting standards and procedures, such as in-person interviews; a database of identity documents proffered by applicants to ensure that duplicate documents are not used by multiple

vetting standards and procedures. Previously, VWP countries signed and implemented a Preventing and Combating Serious Crimes (PCSC) agreement, as well as a Homeland Security Presidential Directive-6 arrangement,[10] with the United States.[11] PCSC agreements allow for the exchange of biometric data, such as fingerprints, and biographic data in order to prevent and detect crime while protecting individual privacy.

The United States began entering into PCSC agreements in 2008, primarily with countries that participated or sought to participate in the VWP.[12] PCSC agreements are intended to automate and expedite the sharing of information about persons for whom a government has an official need to inquire for purposes of preventing or combating serious crime, while requiring measures to ensure individual privacy is protected. As recognized by the Government Accountability Office, "PCSC agreements contain numerous provisions pertaining to the handling, sharing, and retention of relevant data, all designed to ensure privacy and data protection."[13] By authorizing both the United States and a VWP country to conduct automated queries of the other's criminal fingerprint databases, PCSC agreements establish a framework for enhanced cooperation.

While useful, the PCSC agreements proved inadequate to improving routine traveler screening now required by law, policy, and the current threat environment. In order to address the current threat environment and to meet the requirements set forth in Executive Order 13780, DHS policy requires all countries in the VWP and those aspiring to join to allow DHS and State to compare the fingerprints of travelers seeking entry or immigration status in the United States against their appropriate criminal, terrorist, *and identity records* (emphasis added) to allow DHS to readily determine whether the individual seeking to enter the United States poses a risk of terrorism, crime, or identity fraud.[14] Identity records may be sourced from foreign biometric-based

applicants; amended application forms that include questions aimed at identifying fraudulent answers and malicious intent; a mechanism to ensure that applicants are who they claim to be; a mechanism to assess whether applicants may commit, aid, or support any kind of violent, criminal, or terrorist acts after entering the United States; and any other appropriate means for ensuring the proper collection of all information necessary for a rigorous evaluation of all grounds of inadmissibility or grounds for the denial of other immigration benefits.").

[10] An HSPD-6 arrangement commits the parties to share watch list information about known or suspected terrorists.

[11] In 2009, a National Security Staff-led Transborder Security Interagency Policy Committee reaffirmed that PCSC and HSPD-6 agreements were appropriate vehicles for satisfying the statutory information-sharing requirements in the 9/11 Act, *available at* https://www.dhs.gov/news/2011/12/06/testimony-assistant-secretary-david-heyman-office-policy-house-committee-judiciary.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT APPENDICES 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.

[13] *Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security*, Government Accountability Office (GAO), note 38, GAO-16-498 (May 2016), *available at* https://www.gao.gov/assets/gao-16-498.pdf.

[14] Under a 2008 Memorandum of Agreement, *Regarding the Sharing of Visa and Passport Records and Immigration and Naturalization and Citizenship Records, S*tate shares visa information with DHS to support State's adjudication and issuance of visas.

systems, including those determined by DHS and the foreign government to be relevant to immigration determinations.[15]

DHS will work expeditiously with State and VWP countries to implement these additional information sharing requirements. In particular, the DHS Office of Strategy, Policy, and Plans (PLCY), which leads and coordinates international engagement and negotiations on behalf of the Department, will negotiate information-sharing agreements necessary to implement the new policy with aspiring and current VWP countries in cooperation with State.

Three DHS Components are 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). Each Component, pursuant to its legal authorities, collects and uses fingerprints from individuals seeking entry to the United States, seeking an immigration benefit or other immigration related requests, as part of their screening process or from those subject to immigration, administrative, or criminal law enforcement actions. The DHS Automated Biometric Identification System (IDENT)[16] – and its replacement system, the Homeland Advanced Recognition Technology System (HART)[17] – is DHS's biometric system for storing and processing biometric and limited biographic data for national, law enforcement, immigration, intelligence, and other DHS mission-related functions. IDENT/HART is managed by the DHS Management Directorate (MGMT), Office of Biometric Identity Management (OBIM). OBIM and PLCY, in collaboration with the Component data owners, facilitate IDENT/HART-based information sharing to support the VWP process.

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 biometrics, 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.

---

[15] *See*, for example, Agreement between the Government of the Republic of Poland and the Government of the United States of America On Cooperation on Border Security and Immigration.
[16] *See supra* note 11.
[17] *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.

The VWP Information Sharing Process

The goal of this process is to vet relevant border and immigration-related fingerprints collected by DHS against VWP country databases. The statutory requirement that VWP countries sign and implement information sharing agreements helps the United States identify travelers presenting a threat to the security or welfare of the United States and enhances vetting of individual travelers. Reciprocity is a principle of international relations and therefore will be part of the VWP. Although U.S. law typically does not require DHS to reciprocate information sharing on U.S. persons, it is likely that any information sharing agreement or arrangement that satisfies the VWP will be reciprocal. DHS welcomes reciprocity and also encourages, but does not require, VWP countries to query DHS when they process any applications to their governments for travel, admission, entry, or immigration status.

The information sharing process at DHS begins when one country (herein "querying country") has a need to screen an individual to administer or enforce national laws applicable to people entering, staying in, and leaving that country's jurisdiction. The querying country collects the fingerprints of the subject and queries the biometric system of the other country (herein "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. 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 a match, the countries may exchange appropriate information to assist in law enforcement or immigration benefit adjudication decisions. 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). 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 no further information is exchanged.

Currently, DHS OBIM maintains the services in IDENT/HART to submit a query to a foreign partner through the use of the External Identify Service.[18]

Each DHS Component sending queries to foreign partners via IDENT/HART will develop its own procedures and operational policies to determine when and how that Component will initiate a query to a foreign partner, and the technical mechanism or electronic gateways that Components will use to exchange request and response data with OBIM. CBP currently directs IDENT to send queries to a foreign partner through the Automated Targeting System (ATS);[19]

[18] *See* DHS/OBIM/PIA-004 Homeland Advances Recognition Technology System Increment 1 (*supra* note 16), Appendix B.
[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT

ICE uses the Biometric International Query Service (BIQS);[20] and USCIS uses the Customer Profile Management Service (CPMS).[21] Queries from any of the three systems will elicit the same response.

In response to a fingerprint-based request from DHS, the foreign partner provides a match/no match response. If a biometric match was made in the foreign partner's system that is permissible to share with the United States as a matter of that country's laws and policies, then a "match" response is provided back to IDENT/HART with limited biographic information.[22] If a biometric match was not made, or the information associated with the identity in the foreign partner's database cannot be shared with the United States because of the foreign partner's policy, privacy limitations, or legal requirements, then a "no match" response is returned to IDENT/HART. The response message provided by the foreign partner is assigned to the record in IDENT/HART and subsequently provided to the requesting Component that initiated the query for use as part of its investigation or benefit adjudication.[23]

At present, IDENT/HART has the technical capability to execute outbound queries through the External Identify Service to a number of VWP and non-VWP countries and OBIM will be extending such IDENT/HART capabilities to all VWP countries to achieve a connection by 2025. IDENT/HART's External Identify Service can send a biometric query (outbound) to the aforementioned partners and receive an automated response (inbound). Once a DHS Component decides to submit a query to a foreign partner, the query process is initiated automatically between IDENT/HART and the foreign partner. When a foreign partner provides data to IDENT/HART in response to a query, IDENT/HART retains that information as an encounter and submits the response back to the requestor through automated means.

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 DHS Components, would extract the fingerprint images from

---

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.

[20] *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.

[21] *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.

[22] *See* Appendix A of this PIA for additional information on the data elements the Department exchanges as part of VWP.

[23] OBIM maintains an internal reference of privacy, policy, civil rights and civil liberties, and legal requirements. OBIM uses that reference to configure the IDENT/HART automated filters and can reconfigure the filters to meet the ever-changing landscape of data dissemination requirements from the Department. For more information on data access and security controls, *see* DHS/OBIM/PIA-004 Homeland Advances Recognition Technology System Increment 1 (*supra* note 16).

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 email to the Component who requested the query.

When a VWP partner country sends DHS and its Components a fingerprint for query, that request is automatically matched 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, then IDENT/HART returns a match response, with the biographic data approved for sharing.[24] OBIM automatically determines which data elements may be shared with VWP partners 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 has not been authorized for disclosure by the data owner is automatically filtered out of IDENT responses to the foreign partner.[25]

If there is no match, or OBIM analysts have determined that the match may not be shared as a matter of law or policy, IDENT/HART returns a "no match" response to the foreign partner.[26] 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 Violence Against Women Act (VAWA),[27] T visa nonimmigrant status (victims of human trafficking),[28] or those applying for U visa

[24] Information disclosed upon a match may, when available and appropriate, include data such as surname, 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.

[25] 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.

[26] *See supra* note 26.

[27] 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").

[28] 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

nonimmigrant status (victims of qualifying crimes),[29] except in certain circumstances,[30] because the data of such individuals is protected by law.[31] Similarly, DHS will share Asylum and Refugee data with partner countries only in accordance with established law and policy.

OBIM runs a daily match report of filtered and non-filtered matches in IDENT/HART to foreign partner queries and manually imports information from the report into the Technical Reconciliation Analysis Classification System (TRACS).[32] 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 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.[33]

VWP partner countries will use an electronic gateway to share biometrics and biographic data with DHS. The electronic gateway for sharing biometric and biographic data stored in IDENT/HART uses a combination of the public Internet and high security encryption protocols, and can use multiple pathways to transmit data. One such pathway is via CBP ATS, which acts as a proxy between IDENT and a foreign partner's automated biometric system.[34] A virtual private network (VPN) connection over the public Internet is established between each foreign partner

---

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.

[29] 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.

[30] 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).

[31] 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)).

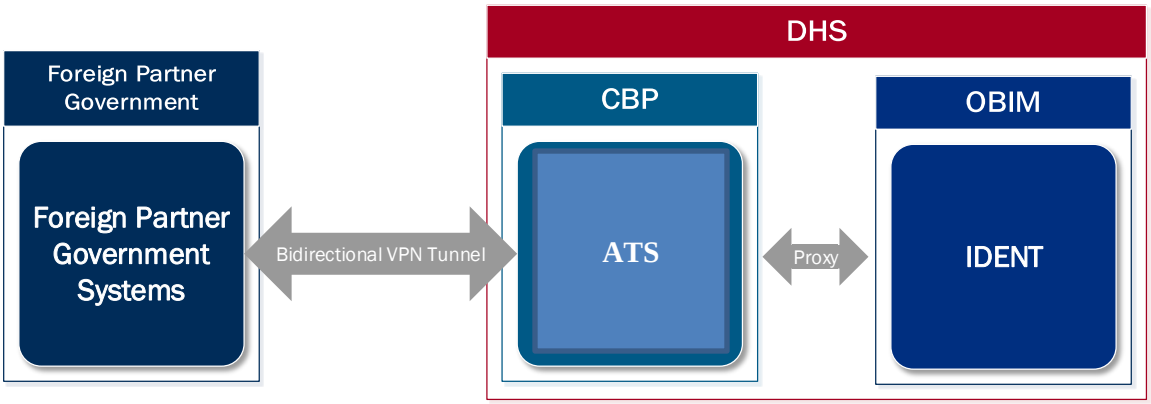
[32] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT APPENDICES FOR THE TECHNICAL RECONCILIATION ANALYSIS CLASSIFICATION SYSTEM (TRACS), DHS/OBIM/PIA-003 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[33] 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.

[34] *See supra* note 17.

and ATS. All message requests and responses from the VWP countries' automated biometric systems to IDENT/HART pass first through this electronic gateway to enter the DHS network. DHS plans to establish future capabilities to send requests and responses from IDENT/HART to the VWP partner countries' automated biometric systems through dedicated technical solutions.[35] ATS is a proxy to the IDENT/HART system. ATS only records transaction details for auditing purposes and information shared by the foreign partner after a match is established. In the latter case, CBP merges the information provided to DHS by the foreign partner with existing CBP data for manual review to which determine whether to engage in further operational cooperation with the foreign partner regarding the match.[36]

The diagram below depicts the current state of bi-directional (two-way) flow of information via ATS:



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

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[37] 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

[35] For example, DHS is developing the Automated Real-Time Identity Exchange System (ARIES), which, once in production, may be used by IDENT/HART as an electronic gateway to pass the identification request from IDENT/HART to the foreign partner for searching. ARIES will apply the proper schema validation, encryption, and security standards to the outbound message for exchange with the foreign partner. This system will be owned and operated by OBIM. A PIA for this system is also in development and will be posted at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim once completed.
[36] *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.
[37] 5 U.S.C. § 552a.

assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[38]

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.[39] 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[40] and the Homeland Security Act of 2002 Section 222.[41] This PIA examines the privacy impact of DHS's Visa Waiver Program operations as they relate to the FIPPs. However, because the specific implementing agreements and technical connections have not yet been established with all VWP countries, it is unclear specifically what identity information VWP countries 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 Systems of Records Notices (SORN), and public statements attesting to the inclusion of foreign countries in the VWP. All conditions for the processing of personal information received from foreign governments under the VWP 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 and when the foreign signatory agrees to publication, will be posted to the DHS FOIA Library at http://www.dhs.gov/foia. 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.

---

[38] 6 U.S.C. § 142(a)(2).
[39] *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.
[40] 44 U.S.C. § 3501 note.
[41] 6 U.S.C. § 142.

DHS and its Components will disclose fingerprints to conduct a query of VWP 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 associated with those collections.

The following SORNs from the IDENT/HART source system owners — ICE, CBP, and USCIS — cover the DHS data to be eventually shared under the VWP policy 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 also those documenting most of ICE's immigration enforcement actions;[42]
- 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;[43]
- 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, covers background checks and their results;[44]
- DHS/ALL-041 External Biometric Records, which covers the maintenance of biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities;[45] 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 such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.[46]

[42] *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.
[43] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[44] *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.
[45] *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.
[46] *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.

In response to a match to a fingerprint-based query, certain additional PII (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, unless the fingerprints are provided on a country's own initiative in furtherance of an authorized DHS mission.[47]

The following biographic information may be shared following a fingerprint match: 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. See Appendix A for a list of possible data elements that DHS may share with VWP partner countries in the event of a match. OBIM analysts coordinate with and provide Components with notification of matches to their data. The Components can decide whether to share information beyond that which is stored in IDENT/HART.[48]

Under certain agreements, including the PCSC agreements, VWP countries may also, in compliance with their respective national laws, share PII – without being requested to do so – to supply information to the other country when there is a reason to believe a person may be a threat.[49] Such instances include when an individual:

- will commit (or may be planning to commit) or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association;
- 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 (or 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 of such data.

Privacy Risk: A privacy risk remains that individuals will not know their information will be used in this manner when applying for a VWP benefit.

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

[47] *See supra* note 45.
[48] *See supra* note 27.
[49] 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.

HART PIAs and the EBR and EBAR SORNs provide general notice that an individuals' 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,[50] 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 knowingly provide their personal information, including fingerprints, to border or immigration officials for the purposes of screening and vetting. In the case of biometric and associated information collected by the United States and its foreign partners for VWP purposes, this information is always collected directly from the individual.

However, a traditional approach to individual participation is not always practical or possible when sharing information with law enforcement agencies, including border enforcement agencies, as may sometimes be the case in the context of VWP information sharing. 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, these individuals may contest or seek redress through any resulting proceedings brought against them.

In addition, the right of individuals to request amendments to their records under the Privacy Act of 1974 is limited to U.S. citizens and Lawful Permanent Residents (LPR).[51] Executive Order 13768[52] reiterates that agencies, to the extent consistent with applicable law, will ensure that only PII relating to U.S. citizens and LPRs are covered by the protections of the Privacy Act. The Judicial Redress Act (5 U.S.C. §552a note), which amended the Privacy Act, provides citizens of covered countries with access and amendment rights under the Privacy Act in certain limited

[50] *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.
[51] 5 U.S.C. § 552a(a)(2).
[52] Executive Order 13768, Enhancing Public Safety in the Interior of the United States (January 25, 2017).

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.[53] Many, but not all, VWP countries are also covered countries for the purposes of the Judicial Redress Act.

The DHS Privacy Policy that implements Executive Order 13768[54] makes clear that 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 helps 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 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 http://www.dhs.gov/foia.

Additionally, travelers who wish to file for redress can complete an online application through the through the DHS Traveler Redress Inquiry Program (DHS TRIP)[55] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF). For more information about the types of services DHS TRIP can provide, please visit https://www.dhs.gov/step-1-should-i-use-dhs-trip.

Individuals who believe information about them was processed under or pursuant to a VWP information sharing agreement may seek to access, correct, amend, or expunge information held by DHS's foreign partners, or otherwise seek redress from these foreign partners for the processing of information abroad, through partner countries' applicable access and redress laws and programs. As VWP countries provide redress points of contact, DHS intends to publish them on its website and in Appendix B of this PIA.

[53] 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.

[54] *See supra* note 50. As the DHS Privacy Policy notes, Executive Order 13768, does not affect other statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. § 1367. These laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and aliens, regardless of a person's immigration status.

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

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.

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."[56] The purpose of DHS's VWP information sharing policy is to allow DHS and State to compare the fingerprints of travelers and immigration benefit applicants against partners' appropriate identity records in addition to criminal and terrorist records. Information gleaned from this sharing is used to assess whether an individual presents a criminal or terrorist risk and aids law enforcement, 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 unauthorized queries may be made about individuals.

Mitigation: This risk is partially mitigated. 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, helps 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 help avoid future reoccurrences.

[56] *See supra* note 7.

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).

The DHS VWP information sharing policy only requires that DHS and State receive and retain information from foreign governments that is necessary to make law enforcement, border enforcement, and immigration-related decisions. Under the principle of reciprocity, DHS will only share information necessary for the VWP partner country to make similar decisions. DHS requires foreign partners to destroy fingerprints sent by DHS when it sends them as part of a query for the purpose of conducting a search against foreign partner systems. Where DHS has requested information pursuant to a partner's query and match to 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)[57] 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 last use of individual's data.[58] OBIM is re-evaluating the current retention policy to determine variable retention periods for latent fingerprints and international records and will submit to NARA for approval for any change in retention periods. Consistent with both retention schedules, DHS and a partner country may agree to establish a retention period of less than 75 years as part of the applicable agreement or arrangement.

Privacy Risk: There is a risk DHS may retain data beyond the period of approved disposition schedules mandated by U.S. law.

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.

[57] *See supra* note 45.
[58] *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.

OBIM provides training and guidance to HART data providers prior to submitting information to HART. In addition, DHS oversight offices and data providers may use HART auditing capabilities to ensure implementation of the data retention schedules.

OBIM has a dedicated team that continually monitors sharing to ensure quality assurance and issues reports on its sharing with VWP 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.[59]

Information sharing agreements used to satisfy VWP requirements authorize DHS to retain and use information for one or more of the following purposes. DHS may retain information to enrich or update DHS's existing record on an individual after a biometric match has been established. This authorization ensures DHS's interactions with the individual are based on complete and accurate information, which is critical to both detecting fraud and facilitating interactions with low risk travelers and migrants. Agreements may also authorize DHS to retain information about individuals the providing country believes present a threat to 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 request DHS serve as a biometric repository for their data because they lack the ability to store or match biometric data at sufficient volumes. In these instances, a country may opt to authorize DHS to retain, either on a categorical or case-by-case basis, that information for future use by the foreign partner and/or DHS in order to meet VWP requirements.

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

[59] 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.

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. 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.[60] The DHS Chief Privacy Officer may also direct that a Privacy Compliance Review be conducted, take other action, or refer the issue to another oversight office (such as the DHS Office of Civil Rights and Civil Liberties), as appropriate.

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 assist DHS Components and VWP partner countries in verifying an individual's identity for immigration purposes and assessing whether an individual presents a criminal or terrorist risk, and aiding DHS Components and foreign partners in making border and immigration related decisions. These purposes are documented in the relevant international agreement or arrangement negotiated with the VWP 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 indicating 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. 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's information-sharing relationships are documented in applicable agreements,

[60] 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.

arrangements, and other implementing documentation, including privacy compliance documentation.

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.

Privacy Risk: A privacy risk remains that data will be shared more broadly than permitted by the relevant SORNs and terms of the VWP 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 VWP searches via manual analysis.[61] 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. 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 need 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 five 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.

[61] 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 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 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.

Mitigation: This risk is partially mitigated. VWP information-sharing agreements restrict disclosure of information to third parties and include accountability and auditing mechanisms to ensure the information sharing agreements are properly implemented. The agreements permit the country responding with information to inquire 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) used within the Department or with domestic third-party vendors is greatly limited with partners located overseas. It is for this reason that both the United States and its partner countries will 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 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 VWP 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 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 consistent with the position's authorities.

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

Mitigation: This risk is partially mitigated. DHS cannot fully mitigate the risk that a foreign government will fail to correct inaccurate information as required under its applicable agreement. To mitigate this risk, USCIS, CBP, and ICE do not make decisions solely on the information provided by foreign governments. Officials from these agencies consider the totality of information, including information collected directly from the individual, prior to making a law enforcement, border enforcement, or immigration decision.

OBIM has built additional accuracy measures into the process 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 VWP 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 used to implement VWP requirements 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. Most 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 a more frequent 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 its VWP partner countries will be intercepted or compromised by a third party.

Mitigation: This risk is partially mitigated. DHS mitigates this risk through the use of 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 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 make corrections, 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 of time.

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 with the partner country about how the data was used and the results generated. These responses may be useful in revealing privacy incidents or unauthorized disclosures by a partner country. However, it is dependent on the partner country's willingness to comply with the request and to be transparent about prior privacy incidents involving DHS-supplied data. In the event DHS concludes that the country is not a responsible steward of the PII with which it is entrusted, then terminating the agreement, in accordance with its terms, may be an option for consideration by the U.S. Government.

Conclusion

On October 22, 2019, the Acting Secretary of Homeland Security signed an adjustment to the information sharing requirements of the VWP through a memorandum. This policy is an important milestone for the maturation of the VWP and will improve DHS's access to relevant information. For many years the Department considered only whether a VWP country had signed certain agreements and taken any action to implement those agreements. The new policy adds to the definition of DHS's expectations of VWP countries, and reduces information sharing gaps.

Due to the privacy risks associated with the collection, retention, use, and dissemination of biometrics, the DHS Privacy Office will continue to advise PLCY, OBIM, and other DHS Components who participate in VWP activities. Specifically, the DHS Privacy Office will contribute to mitigation strategies such as increased training, annual reviews, and the establishment a governance board while aiding the Department's mission of promoting secure travel to the United States but also facilitating Americans' travel to VWP partner nations.

Contact Officials

Michael Scardaville
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security
(202) 282-8321

Erik Rye
Visa Waiver Program Office
U.S. Department of Homeland Security
(202) 282-9907

Responsible Officials

Tyler Q. Houlton
Acting Assistant Secretary for International Affairs
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A

Data Elements that DHS Exchanges

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

Australia	Australia Department of Home Affairs
Bulgaria	Ministry of Interior for the Republic of Bulgaria
Croatia	Ministry of Interior for the Republic of Croatia
Greece[62]	Hellenic National Police
Italy[63]	Ministry of Interior of the Italian Republic
New Zealand	The Immigration Manager, Privacy Team – Immigration New Zealand
Poland	Commander in Chief, Polish Border Guard Commander in Chief, Polish Police
United Kingdom	UK Home Office

[62] *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.
[63] *Id.*