Privacy Impact Assessment Update

for the

DHS International Biometric Information Sharing (IBIS) Program – Enhanced Border Security Partnership (EBSP)

DHS Reference No. DHS/ALL/PIA-095(b)

April 26, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS or the Department), Office of Strategy, Policy, and Plans (PLCY), in coordination with DHS components, created the International Biometric Information Sharing (IBIS) Program 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 enhance 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 in border screening and immigration-related contexts. This Privacy Impact Assessment (PIA) Update considers the privacy risks and applicable mitigation strategies associated with implementing this Departmental program in cases where DHS conducts a search using a national identification number, rather than a biometric identifier, which expands the scope of the IBIS program.[1]

Overview

The IBIS Program principally 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 and Nationality Act (INA). 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 foreign partners to compare fingerprints against DHS records for the same purposes.

In February 2022, DHS introduced a requirement that each Visa Waiver Program (VWP) partner establish an Enhanced Border Security Partnership (EBSP) through the IBIS Program with DHS. Under the EBSP, VWP partners would allow DHS to routinely screen against the biometric

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

records of the VWP partner the biometrics of: a) travelers to the United States who may have a nexus to the VWP partner, including its citizens and nationals; b) applicants for immigration benefits or humanitarian protection in the United States; and c) individuals encountered by DHS in a border screening and immigration context in the United States.

All prospective VWP travelers are required to obtain travel authorization via the U.S. Customs and Border Protection's (CBP) Electronic System for Travel Authorization (ESTA)[2] prior to traveling to the United States. ESTA applications are vetted to ensure that travel authorizations are not issued to individuals who pose a threat to national security. While ESTA does not enable the collection of fingerprint data to be used for the framework envisioned under the new EBSP requirement and IBIS Program, some partners have sophisticated and biometrically anchored unique national identifiers which DHS assesses serve the same function as a biometric marker in enabling accurate identification of individuals and identity resolution. Under bilateral arrangements with foreign partners negotiated to satisfy the EBSP requirement, DHS may be authorized to conduct a search against the partner's relevant national databases using a national identification number when an individual provides that number to CBP as part of their ESTA application. DHS and CBP will develop a technical solution which enables CBP to pull the national identification number from the individual's application and initiate an automated search to the partner using that number. In the event of a match, consistent with the terms of the applicable bilateral information sharing arrangement, the partner will provide biographic information to DHS on the associated identity (e.g., name, date of birth, travel documents, nationality) as well as any known criminal convictions and arrests for serious crimes,[3] and an indication of the individual's immigration status in that country.

The biographic identity information provided to CBP in the event of a match based on a national identification number will be stored in CBP's Automated Targeting System (ATS),[4] consistent with other information yielded during the vetting process, and handled in the same manner as existing biometric data exchange for EBSP through the Secure Real Time Platform (SRTP).[5] That is, the information received from the foreign partner will be marked as originating

---

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[3] References to "criminal" or "crime" or "serious 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.

[4] *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(e) (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[5] The Secure Real Time Platform is an international information sharing architecture that is scalable to any country.

from that partner, enabling CBP to appropriately safeguard the information and ensure onward use and sharing of the data is consistent with the relevant bilateral agreement and applicable DHS policies. This enhancement does not require any other changes to existing processes or systems, and there are no changes to the collection, use, retention, or sharing of personally identifiable information (PII) in the IBIS program.

The Information Sharing Process

The information sharing process for queries using a national identification number begins when CBP receives an ESTA application. CBP will retrieve the national identification number the subject provides when submitting an ESTA application and submit it to the country that issued the identification number to determine if that country has a matching identity record. Queries are made on an individual case-by-case basis and in compliance with the national law, policies, and the international agreement or arrangement between the United States and the foreign partner. The foreign partner indicates whether a national identification number match exists in its relevant system by responding "match" or "no match" to the United States. When there is no match, or the country's national law prohibits the disclosure of information that would normally constitute a "match," the country will return a "no match" response. In the event of a "no match," the foreign partner exchanges no further information. When there is a match based on the national identification number, the foreign partner may exchange the type of information listed in the agreements included in Appendix A according to their respective laws and policies and as defined in the applicable international agreement or arrangement to assist in border screening or immigration benefit adjudication decisions.

DHS establishes interoperability with partner country databases using technologically advanced encryption protocols, the public internet, DHS OneNet, and the DHS Gateway to share 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 to CBP's Automated Targeting System.

The Automated Targeting System 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 to assist with

---

The Secure Real Time Platform pathway provides decision makers with data to assist in the adjudication of immigration benefits, enforcement actions, credentialing, and country access permissions. The Secure Real Time Platform supports business use cases for refugee claimants, entry clearance (visas), foreign criminals, redocumentation, and fugitives. The Secure Real Time Platform enables international partners to transmit and receive queries via encrypted internet messages through the DHS Gateway.

determining whether to approve or deny the ESTA application. The information received from the foreign partner is clearly marked in the Automated Targeting System as originating from that foreign partner. The matching results will be stored with other ESTA vetting results and clearly marked as a foreign partner source.

Reason for the PIA Update

DHS is updating this Privacy Impact Assessment to address privacy risks associated with the screening of ESTA applicants, where DHS has been authorized to conduct queries against foreign partners' relevant national databases using a national identification number, rather than a fingerprint, when an individual provides that number to CBP as part of their ESTA application.

Privacy Impact Analysis

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[6] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). 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.[7]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[8] The FIPPs account for the nature 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[9] and the Homeland Security Act of 2002 Section 222.[10] This Privacy Impact Assessment Update examines the privacy impact of DHS's IBIS/EBSP operations as they relate to the FIPPs. However, because the specific implementing arrangements 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

[6] 5 U.S.C. § 552a.
[7] 6 U.S.C. § 142(a)(2).
[8] *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.
[9] 44 U.S.C. § 3501 note.
[10] 6 U.S.C. § 142.

national identification number match. Those details will be specified in the corresponding information sharing agreement, and this Privacy Impact Assessment will be updated if needed.

1. Principle of Transparency

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

DHS has provided public transparency through the issuance of this Privacy Impact Assessment Update and a separate, concurrent update to the ESTA Privacy Impact Assessment series[11] that discuss the collection and use of personally identifiable information in determining the eligibility to travel of persons seeking to enter the United States under the VWP. Additionally, the DHS/CBP-006 Automated Targeting System[12] and DHS/CBP-009 ESTA[13] System of Records Notices (SORN) provide transparency about the information collected, maintained, used, and disseminated as part of this program. Finally, DHS provides notice through public statements regarding the inclusion of foreign countries in the VWP or other information sharing statements with the United States. All conditions for the processing of personal information received from foreign governments under the IBIS Program 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 (FOIA) request or may be available on the Department of State website.[14] All binding agreements, and qualifying non-binding instruments, 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 information pursuant to their national law and procedures.

Upon receipt of an ESTA application, DHS and its components will disclose national identification numbers to foreign government partners to conduct a query of their databases. DHS has provided transparency about the potential disclosure of personally identifiable information via the relevant System of Records Notice(s) and Privacy Impact Assessments(s) for the ESTA program and on the ESTA application and website.

---

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION (ESTA), DHS-CBP-PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[12] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[13] *See* DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 87 Fed. Reg. 41338 (July 12, 2022), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* https://www.dhs.gov/freedom-information-act-foia.

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 seeking admission to the United States under the VWP are required to obtain travel authorization by applying for an ESTA before traveling to the United States. Individuals directly provide their personal information to CBP when submitting their ESTA application. When accessing the ESTA website, users are presented with a Security Notification, Disclaimer, and Privacy Act Statement. These notices outline the purpose of the collection and use of the information, including conducting law enforcement checks against U.S. and foreign databases. Users are required to review and acknowledge these notices before proceeding with the ESTA application. By acknowledging these notices, the user consents to the uses of information outlined in the notices. 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 foreign partner country.

In addition, U.S. citizens and Lawful Permanent Residents (LPR) have the right to request amendments to their records under the Privacy Act.[15] 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.[16] Many, but not all, VWP countries are also covered countries under 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, uphold our values, 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 FOIA request with the respective component (e.g., CBP) or DHS FOIA office. Additional information about FOIA is available at https://www.dhs.gov/foia.

[15] 5 U.S.C. § 552a(a)(2).
[16] 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.

Travelers who wish to file for redress can complete an online application through the DHS Traveler Redress Inquiry Program (DHS TRIP)[17] 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 Step 1: Should I Use DHS TRIP? | Homeland Security. Additional redress procedures can be found in the DHS/CBP-006 Automated Targeting System and DHS/CBP-009 ESTA System of Records Notices.

Individuals who believe information about them was processed under or pursuant to an IBIS information sharing arrangement 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 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 the original Privacy Impact Assessment.

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

Mitigation: This risk is partially mitigated. When using a national identification number to conduct an IBIS search, DHS will only receive information from IBIS partners on individuals who knowingly submit an ESTA application and provide their national identification number to DHS. The individuals are likely already aware that DHS has some of their personal data, due to their ESTA submission and/or existing travel to 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.

Eligibility for a country's designation in the VWP is defined in Section 217 of the Immigration and Nationality Act (INA) (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 Sates 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 implement[] such agreement."[18] The purpose of DHS's VWP information sharing policy and the IBIS Program is to

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM (TRIP), DHS/ALL/PIA-002 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[18] 8 U.S.C. 1187(c)(2)(F).

allow DHS to compare information of travelers and immigration benefit applicants, as well as those encountered during border inspections or in the course of criminal investigations related to immigration or border issues, 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. The use of a national identification number as the basis for a search against foreign partner systems further enables DHS to conduct appropriate screening of prospective VWP travelers prior to arrival at the U.S. border, as fingerprints are not collected as part of the ESTA application process. These purposes and corresponding safeguards 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 mitigated. A search will only be conducted if an individual submits an ESTA application to CBP and they are from an IBIS partner country with an arrangement that allows for national identification number searches. The IBIS partner may not submit a search to DHS using a national identification number; such a number does not exist in DHS databases. All IBIS Program agreements or arrangements include provisions requiring regular auditing and review of the actual sharing.

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 to receive and retain information from foreign governments that is necessary to inform border enforcement and immigration-related decisions as well as to prevent, detect, and investigate related crime. When a DHS query matches a partner's record, the partner may disclose biographic and biometric information related to the national identification number in accordance with applicable law and policy and the bilateral agreement or arrangement.

The National Archives and Records Administration (NARA) approved the records retention schedule of 75 years for DHS's biometric and biographic records used for national security, law enforcement, immigration, and other functions consistent with DHS authorities.[19] DHS and a partner country may agree to establish a retention period of less than 75 years as part

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

of the applicable agreement or arrangement. Furthermore, CBP retains ESTA records for 15 years in accordance with DAA-0568-2019-0006.[20] This retention schedule allows CBP to address any follow-up inquiries or requests related to the application, including inquiries related to law enforcement, public safety, national security, FOIA/Privacy Act matters, or correcting errors in the application.

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. The CBP Automated Targeting System retains data according to the Systems of Records Notice requirements of the systems from which the data was obtained. The Automated Targeting System collects information directly, ingests information from various systems, and accesses other systems without ingesting the data. Additionally, CBP conducts periodic risk assessments of the Automated Targeting System to ensure compliance. The Automated Targeting System maintains the assessment results from rules together with a record of which rules were used to develop the risk assessment. This assessment and history of relevant rules associated with developing assessment results are maintained for up to fifteen years to support ongoing targeting requirements. Notwithstanding this limitation, information maintained in the Automated Targeting System that is linked to an active law enforcement matter will be retained for the duration of that law enforcement matter.

Nonetheless, the standard for data retention is the data's relevance and utility. Accordingly, CBP will regularly review the retention period for records in Automated Targeting System to ensure their continued relevance and usefulness. If these reviews demonstrate that certain data is no longer relevant and useful, CBP will revise the retention period and delete the information.

IBIS information sharing agreements authorize DHS and the partnering foreign countries 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 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.

[20] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0568/daa-0568-2019-0006_sf115.pdf.

Retention supports the Data Quality and Integrity 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.

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.

In the event of a national identification number match, DHS receives information to: a) assist DHS components in verifying an individual's identity for immigration purposes and assessing whether an individual presents a criminal or terrorist risk; b) aid DHS components and foreign partners in border screening encounters; and c) aid in making border and immigration related decisions. These purposes are documented in the relevant international agreement or arrangement negotiated with the IBIS partner country.

IBIS Program agreements and arrangements include provisions requiring routine auditing and mechanisms for assessing compliance. To ensure compliance, the DHS Chief Privacy Officer may 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 of the collection and scope for which the information can be used, limit onward sharing, and require partners to ensure the data is secured and safeguarded.

Privacy Risk: There is a privacy risk that data will be shared more broadly than permitted by the relevant System of Records Notices and terms of the IBIS information sharing agreements.

Mitigation: This risk is partially mitigated. DHS IBIS Program agreements and arrangements require partner countries to maintain and log all data transmitted and received. If during an audit 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 additional training, or even terminating cooperation. DHS and its partner countries 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 incorporates mutually agreed upon compliance evaluations into the text of IBIS Program agreements and arrangements signed with partner countries, and generally conducts the evaluations no more frequently than annually and no less frequently than every three years. CBP carefully reviews and evaluates the data to be shared

before disclosing it to an external partner. Disclosure of information obtained from an ESTA application must be compatible with the purposes for which the data was collected, and authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3), specifically the routine uses set forth in the ESTA and Automated Targeting System System of Records Notices or as otherwise permitted by the Privacy Act. Additionally, for ongoing, systematic sharing, CBP completes an information sharing and access agreement with external partners to establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy safeguards for the data.

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 or arrangement. The procedures for implementing IBIS Program agreements and arrangements require foreign partners to ensure that any inaccurate personal information is brought to the partner's attention in a timely manner, 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 conduct a Privacy Compliance Review.

Privacy Risk: There is a risk 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. DHS provides 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. Additionally, if DHS discovers a foreign partner's non-compliance with the applicable agreement, DHS may seek revision of the terms of the agreement or end the relationship with the foreign partner.

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 IBIS Program agreements ensure that the necessary technical and organizational measures are used to protect personally identifiable information against accidental or unlawful destruction, accidental loss, unauthorized disclosure, alteration, access, or any unauthorized processing of the data. Each country must take reasonable measures so only authorized individuals have access to the personally identifiable information exchanged.

Further, partner countries are required to report any privacy incidents, including unauthorized access or disclosure of DHS information. All partner countries are 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 personally identifiable information with which DHS entrusts it, then DHS may consider suspending or terminating the agreement. Detection of non-compliance may arise 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 IBIS Program agreements and arrangements require a "regular" and/or "periodic" review of the implementation of the agreement or arrangement. 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.

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 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 IBIS Program agreements and arrangements, 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 IBIS Program agreements and arrangements 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 and policy 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 if the data is supplied to other entities. The countries must protect the log with appropriate measures against inappropriate use and maintain it for a pre-determined period.

IBIS Program agreements and arrangements also require the countries to regularly engage in consultations to—in part—review the number of queries made and percentage of matches, and share—to the extent practical—additional statistics and case studies demonstrating how the exchange of information under the agreement has assisted with law enforcement, immigration adjudication, and border enforcement.

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

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

Mitigation: This risk is partially mitigated. As discussed, partner 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, the amount of risk 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. If DHS concludes that a country is not a responsible steward of the personally identifiable information with which it is entrusted, then DHS may consider terminating the agreement, in accordance with its terms.

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, or 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 work to ensure that all individuals' privacy is protected in accordance with U.S. privacy requirements, DHS policies, and the terms of any applicable international agreements or arrangements.

Contact Official

Caitlin Finn
Director, International Information Sharing
Office of International Affairs, Office of Strategy Policy, and Plans
U.S. Department of Homeland Security

Responsible Official

Bob Paschall
Assistant Secretary (Acting)
Office of 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.

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: Agreements Allowing for Searches Using a National Identification Number

Last Updated: March 26, 2024

- Implementing Arrangement between the Department of Homeland Security of the United States of America and the Ministry of Interior and Public Security of Chile under the Agreement between the Government of the United States of America and the Government of Chile on Enhancing Cooperation in Preventing and Combating Serious Crime (July 31, 2023)
    - When there is a match based on the national identification number, the country of nationality may exchange the type of information listed in the agreements according to their respective laws and policies and as defined in the applicable international agreement or arrangement to assist in border screening or immigration benefit adjudication decisions.