Privacy Impact Assessment
for the

United States - Mexico Entry/Exit Data Sharing Initiative

DHS/CBP/PIA-050

December 14, 2017

Contact Point
Michael Hardin
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
(202) 325-1053

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) cooperates with both Canada and Mexico to secure our shared borders while facilitating legitimate trade and travel. Under the U.S.-Mexico Entry/Exit Data Sharing Initiative, CBP and Mexico's National Migration Institute (INM) intend to exchange border crossing information collected from travelers entering Mexico at ports of entry along the U.S.-Mexico border. The exchange of border crossing information under this initiative is intended to assist INM in creating entry records, and assist CBP in creating U.S. exit records based on a record of entry to Mexico, thereby facilitating cross-border travel and supporting both parties' immigration and law enforcement missions. CBP is publishing this Privacy Impact Assessment (PIA) because this initiative involves the exchange of personally identifiable information (PII) between CBP and INM.

Introduction

Existing CBP Exit Processes

While CBP has well-established procedures for conducting immigration and customs inspections on travelers entering the United States, the process of recording the departure of outbound travelers is still in development. A variety of statutes require DHS, and CBP specifically, to develop a system for collecting records of travelers departing the United States. The 1996 Illegal Immigration Reform and Immigrant Responsibility Act[1] called for the creation of an automated system to record arrivals and departures of aliens at all air, sea, and land ports of entry. The 2002 Enhanced Border Security and Visa Entry Reform Act,[2] the Intelligence Reform and Terrorism Prevention Act of 2004,[3] and the Implementing Recommendations of the 9/11 Commission Act of 2007[4] all called for the creation of a nationwide biometric entry-exit system. Biometric screening on entry has been in place since 2004,[5] and CBP continues to conduct tests of various systems and processes to identify a method for comprehensive biometric exit screening, including the creation of exit records for individuals departing the United States.

Under the U.S.-Canada Beyond the Border Action Plan,[6] CBP exchanges border crossing information with the Canada Border Services Agency (CBSA) pursuant to the Beyond the Border entry/exit program.[7] By exchanging entry information, CBP and CBSA track entries into the other country as records of exit from their own. For example, when a traveler leaves Canada and enters

[1] Pub. L. 104-208.
[2] Pub. L. 107-173.
[3] Pub. L. 108-458.
[4] Pub. L. 110-53.
[5] *See* DHS/NPPD/PIA-001 US-VISIT Program, Increment 1 (January 16, 2004), *available at* www.dhs.gov/privacy.
[6] United States-Canada Beyond The Border: A shared Vision for Perimeter Security and Economic Competitiveness, *available at* https://obamawhitehouse.archives.gov/sites/default/files/us-canada_btb_action_plan3.pdf.
[7] *See* DHS/CBP/PIA-004 Beyond the Border Entry/Exit Program, *available at* www.dhs.gov/privacy.

the United States via a land port of entry, the United States creates a record of entry and sends the record to CBSA to annotate as an exit record. By using the entry record of one country to establish an exit record for the other, both countries are able to reduce the expense and burden of establishing exit record processes at the shared border.

Similarly, CBP and INM signed an Implementing Arrangement on August 30, 2017, documenting the intent to implement a process to exchange information and support both countries to generate accurate biographic entry and exit records. CBP and INM also developed a Concept of Operations which outlines how the initial phase of the pilot will operate. The pilot will consist of several phases, with the initial phases implementing data sharing practices between INM and CBP. For the first phase, INM will collect information from Western Hemisphere Travel Initiative (WHTI)[8]-compliant, radio frequency identification (RFID)-enabled travel documents and transfer the information to CBP.

Data Sharing with Mexico

Overview: Joint Pedestrian Land Port of Entry Pilot

Consistent with CBP's efforts with the CBSA to share entry records, CBP plans to cooperate with INM to share border crossing information. Under this effort, CBP and INM seek to (1) enhance INM's capabilities of processing entry information; (2) develop CBP's use of Mexican entry records to create U.S. exit records; and (3) further facilitate sharing of information relevant to both countries' customs and immigration enforcement.

The initial phase of the initiative will take place on the Mexican side of the San Ysidro Port of Entry. Currently, INM separates Mexican Nationals[9] from all other travelers for entry processing. INM officers verify that all travelers are using the appropriate travel documents, but do not currently collect information on Mexican Nationals to generate entry records at the land border. For this initiative, INM will create a second, separate "Mexican Nationals Only" travel lane for Mexican Nationals who have RFID-compliant travel documents. The goal for this phase of the initiative is for (1) INM to collect RFID information from Mexican Nationals, (2) INM to send that information to CBP, (3) CBP to create U.S. exit records from the RFID information, and

[8] WHTI is a program designed by DHS in conjunction with the Department of State to comply with the Intelligence Reform and Terrorism Prevention Act of 2004. In order to comply with the law, DHS was required to collect travel information from an expanded group of people, specifically travelers from Mexico, Canada, and Bermuda, who previously only had to show limited information to enter the country. DHS determined the best way to collect this information was to create RFID-enabled travel documents that could easily be used by citizens of Canada, Mexico, and Bermuda.

[9] The term "Mexican Nationals" refers to all citizens of Mexico and children of citizens who are under 18 (under Mexican law, a person is not a citizen until they turn 18 years old). Being a Mexican National does not preclude someone from being a U.S. Citizen or a U.S. Lawful Permanent Resident (such as dual citizens).

(4) CBP to send the exit records back to INM to use in creating its entry record.[10]

While INM will only direct Mexican Nationals who possess an RFID-compliant travel document to the RFID reader-equipped lane, it is possible that non-Mexican nationals, including U.S. Citizens (USC) and Lawful Permanent Residents (LPR), who possess an in-scope RFID-enabled travel document may inadvertently use the RFID reader-equipped lane. INM will send all information collected via the RFID lanes to CBP, regardless of citizenship. CBP will send complete exit records back to INM, regardless of citizenship. CBP's Arrival and Departure Information System (ADIS)[11] matches an exit record created from information sent from INM, with an entry record for the same individual to verify his or her departure from the United States.

INM and CBP are working on a process that allows INM to share entry data from all travelers, including USCs and LPRs, from whom INM collects a biographic entry record via established inspection procedures. INM will transfer entry information to CBP and CBP will create exit records from the information. CBP will publish updates to this PIA and any other required privacy compliance documentation prior to exchange of data on all other non-Mexican nationals.

Use of RFID Reader

For this initiative, travelers using the new "Mexican Nationals Only" travel lanes will scan their WHTI-compliant, RFID-enabled travel documents issued by U.S. Government agencies. These documents include the Border Crossing Card (BCC) issued by the U.S. Department of State, the Permanent Resident Card (PRC) issued by U.S. Citizenship and Immigration Services (USCIS), U.S. Passport Cards issued by the U.S. Department of State, and Trusted Traveler Cards including CBP Secure Electronic Network for Travelers Rapid Inspection (SENTRI), CBP NEXUS, and CBP Free and Secure Trade (FAST) cards.[12] The RFID chip in WHTI-compliant, RFID-enabled documents is encoded with only two pieces of information: a 96-bit encoding (or RFID number) from the issuer of the document that is unique to that document; and a unique encoding from the chip manufacturer known as the Tag Identifier (TID). The RFID number encoding indicates the type of card (*e.g.*, the Border Crossing Card or SENTRI card). The remainder of the number is unique to that record. No other information is encoded in the chip. The RFID reader will send the RFID number to an INM-controlled workstation located in a secure Local Area Network (LAN) room. These numbers, along with the date and time stamp of the

[10] External sharing with INM for this purpose is consistent with Routine Use P of the Border Crossing Information (BCI) System of Records Notice, DHS/CBP-007 Border Crossing Information (BCI), 81 FR 89957 (December 13, 2016), which permits CBP to disclose records to appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS is aware of a need to use relevant data for purposes of testing new technology.
[11] DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (November 18, 2015).
[12] The CBP SENTRI, NEXUS, and FAST programs are Trusted Traveler Programs that provide expedited travel for pre-approved, low risk travelers through dedicated lanes and kiosks. For more information, please *see* DHS/CBP/PIA-002 Global Enrollment System, *available at* www.dhs.gov/privacy.

transaction, will be stored on the local workstation. These records will be batched weekly and sent to CBP via a secure encrypted device. CBP will upload the encrypted batch file to CBP's secure databases using the RFID number as an index. CBP will conduct queries in TECS[13] using the RFID numbers to locate the corresponding record within CBP's Border Crossing Information (BCI)[14] database and return the following biographic information associated with that RFID number to create a border crossing record:

- First/Given Name
- Last Name/Surname
- Middle Name
- Date of Birth
- Nationality/Citizenship
- Gender

CBP will send a weekly batch of associated exit records back to INM, which will retain this information as a record of entry into Mexico. INM will initially store the records at its National Targeting Center, and will eventually store the records in the appropriate designated IT systems. INM may also use the records for statistical purposes to enhance information on tourism and immigration trends, as permitted by applicable law and policy.[15]

CBP retains border crossing records in the TECS BCI database for USCs and LPRs for 15 years, and for non-immigrant aliens for 75 years, in accordance with the BCI System of Records Notice (SORN).[16] In addition, CBP retains border crossing records for LPRs and non-immigrant aliens in ADIS for up to 75 years, consistent with the ADIS SORN.[17] Mexico will retain the biographic information it receives from CBP for 35 years, consistent with existing requirements for border crossing records.

Future Phases

Once INM and CBP operationalize the collection of RFID information from Mexican Nationals and the exchange of data, they will work to expand the pilot to share information on all travelers. INM will share entry information collected on all travelers, including USCs and LPRs who are not using RFID documents, through their established immigration inspection procedures. INM will batch these records weekly and send to CBP via a secure encrypted device, until such time as CBP and INM mutually determine that such data can be transferred electronically through

[13] *See* DHS/CBP/PIA-021 TECS Platform, *available at* www.dhs.gov/privacy.
[14] DHS/CBP-007 Border Crossing Information (BCI) System of Records, 81 FR 89957 (December 13, 2016).
[15] *See* INM Statistics, *available at* http://www.politicamigratoria.gob.mx/es_mx/SEGOB/Estadistica.
[16] DHS/CBP-007 Border Crossing Information (BCI) System of Records, 81 FR 89957 (December 13, 2016).
[17] DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (November 18, 2015).

a system-to-system connection. The INM entry records sent to CBP will be used to create exit records. The INM entry records may include the following data:

- Full Name (last, first, middle (if available))
- Date of Birth
- Nationality (citizenship)
- Gender (M/F)
- Document Type
- Document Number
- Document Country of Issuance
- Land Port of Entry
- Date of Entry
- Time of Entry

Data Sharing Governance

Sharing of border crossing information between CBP and INM is documented in the following agreements:

- *Implementing Arrangement between the Department of Homeland Security*, U.S. Customs and Border Protection, and the Secretariat of Governance, National Migration Institute, Regarding the Sharing of Border Crossing Data (signed August 30, 2017), executed under the framework of Memorandum of Cooperation between the Department of Homeland Security of the United States and the Secretariat of the Government of the United Mexican States (signed April 17, 2013);
- Interconnection Security Agreement between the Secretariat of Governance for the United Mexican States and the U.S. Department of Homeland Security for the United States of America (dated April 20, 2011);
- Each separate initiative is governed by a Concept of Operations, which outlines the information being exchanged, the manner of collection and mechanism of exchange, and any technical and procedural requirements.

These documents establish the procedures for information transfer and outline the requirements for protecting the information. Specifically:

- Further sharing of the information by the recipient agency is subject to the laws, policies, and approval of the source agency;

- Both agencies apply technical safeguards to protect the information against unauthorized access, disclosure, use, modification, or deletion;
- Any information received in error or inconsistent with the terms of the program documentation is to be destroyed immediately and not used without express prior written consent;
- INM commits to promptly notifying CBP in the event of any unauthorized access, disclosure, use, modification, or deletion of any information;
- Each agency commits to providing mechanisms through which individuals may seek correction of their records; and
- Each agency commits to notifying the other in writing in the event that any information is discovered to be inaccurate.

Fair Information Practice Principles (FIPPs)

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

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. 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 and the Homeland Security Act of 2002 Section 222. Given that Joint Pedestrian Land Port of Entry Pilot is a phased approach, led by the CBP Entry/Exit Transformation Office, rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of the Joint Pedestrian Land Port of Entry Pilot as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

DHS provides general notice of information sharing with Mexico through this PIA. In addition, the BCI SORN[18] provides general notice to travelers of CBP's collection of border crossing records. DHS also provides notice via general information about CBP's data sharing efforts with Mexico on the public-facing CBP website. CBP will issue and post online a press release on the launch date of the pilot which will discuss the information sharing.[19]

Privacy Risk: There is a risk that travelers entering Mexico will not realize that their Mexican entry records will be shared with the United States.

Mitigation: This risk is partially mitigated by press and media engagement regarding data sharing efforts with Mexico, as described above, in addition to future press engagements as the project commences and progresses. CBP provides notice through privacy documentation that CBP shares traveler information with INM, and receives information from INM to create the U.S. exit record. Despite these efforts, some risk to transparency remains, since providing timely notice at the time of crossing it is not feasible.

Privacy Risk: There is a risk to transparency that CBP does not have a Routine Use in the BCI SORN that explicitly mentions this type of sharing with INM.

Mitigation: This risk is partially mitigated. Because this initiative is a test of new technology by INM and CBP, CBP may share information pursuant to Routine Use P of the BCI SORN, which permits sharing to test new technologies. In addition, Routine Use H of the BCI SORN permits sharing with foreign governmental agencies for the enforcement and implementation of a statute, rule, regulation, or order. For additional transparency, CBP will update the BCI SORN to include a Routine Use specific to INM, much like the current Routine Use I, "To the CBSA for law enforcement and immigration purposes, as well as to facilitate cross-border travel when an individual enters the United States from Canada," as the program testing phase continues and is evaluated.

[18] DHS/CBP-007 Border Crossing Information (BCI) System of Records, 81 FR 89957 (December 13, 2016).
[19] *See* https://www.cbp.gov/newsroom.

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.*

INM collects RFID information directly from the traveler's valid U.S. travel document. That information is matched to information, stored in TECS, which the traveler provided to the issuing U.S. agency in order to obtain a travel document. The direct participation of the traveler in providing information to cross the border and providing the information necessary to obtain a travel document provides a higher degree of confidence that the data provided is accurate, timely, and complete. INM will direct Mexican Nationals with valid RFID travel documents to the RFID-enabled travel lanes. Crossing an international border is a voluntary action; to gain entry individuals must comply with the rules and regulations enforced by the relevant border authority. While an individual may decline to provide his or her information, it may result in the individual's inadmissibility and denial of entry.

No new access, redress, or correction measures are being instituted pursuant to Phase I of the U.S.-Mexico Entry/Exit Data Sharing Initiative. Individuals may use the existing access, redress, and corrective measures for border crossing information to correct information described in the BCI systems of records.[20] Records in BCI that came from this pilot will be tagged as coming from INM, but will be wholly owned by CBP.

Individuals seeking notification of and access to records contained in BCI, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

[20] DHS/CBP-007 Border Crossing Information (BCI) System of Records, 81 FR 89957 (December 13, 2016).

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

Persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

DHS TRIP
601 South 12th Street, TSA-901,
Arlington, VA 20598-6901

Privacy Risk: Once an individual has provided his or her information and crossed the common border, there is no option for an individual to opt out of the sharing of his or her information between the United States and Mexico.

Mitigation: This privacy risk cannot be fully mitigated. Although the redress and access procedures above provide for an individual's ability to correct his or her information, the only opportunity to completely opt-out of the sharing of that information under this program is to decline to enter the other country. Crossing the border is considered voluntary and individuals seeking to do so are subject, and presumed to have consented, to the laws and rules enforced by CBP and INM.

Privacy Risk: There is a risk that travelers will not be able to correct erroneous records CBP receives from INM.

Mitigation: This privacy risk is partially mitigated. Travelers may notify CBP through the TRIP or through a Privacy Act amendment request if they believe CBP border crossing records are inaccurate. CBP has an interest in ensuring its records are accurate and up to date, and will work to correct any records it discovers are inaccurate. However, some risk remains, since CBP may not be made aware of an inaccurate record in its holdings.

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.*

All information sharing is informed and guided by the *Implementing Arrangements between U.S. Department of Homeland Security, U.S. Customs and Border Protection and the*

Secretariat of Governance, National Migration Institute Regarding the Sharing of Border Crossing Data, signed August 30, 2017, under the framework of the Memorandum of Cooperation between the Department of Homeland Security of the United States of America and the Secretariat of Government of the United Mexican States, signed April 17, 2013.

CBP collects and maintains border crossing information pursuant to the various authorities, including:

- The Aviation and Transportation Security Act of 2001;[21]
- The Homeland Security Act of 2002;[22]
- The Enhanced Border Security and Visa Entry Reform Act of 2002;[23]
- Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004;[24]
- The Immigration and Nationality Act (INA), as amended, including Title 8, Aliens and Nationality (including 8 U.S.C. §§ 1365(a) and (b), which authorize the creation of a biographic and biometric entry and exit data system); and
- The Tariff Act of 1930, as amended, including Title 19, Customs Duties.

The BCI SORN outlines the purposes for which CBP collects and maintains the information in accordance with the Privacy Act of 1974, and details the routine uses of the information, which clarify with whom CBP may share the information, and for what purposes. CBP updates its SORNs, as well as the relevant PIAs, whenever it intends to use any information it collects for a purpose that is not covered by an existing routine use.

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).*

Information transferred from INM to CBP, for those travelers arriving in Mexico using the RFID lane, includes:

- RFID Number
- Tag Identifier (TID) Number

[21] Pub. L. 107-71, 115 Stat. 597. 19 U.S.C. §§ 1628
[22] Pub. L. 107-296, 116 Stat. 2135.
[23] Pub. L. 107-173, 116 Stat. 543.
[24] Pub. L. 108-458, 118 Stat. 3638.

- Date of Entry
- Time of Entry

Information transferred from CBP to INM, for those travelers using the RFID lane, includes:

- First/Given Name
- Last Name/Surname
- Middle Name
- Date of Birth
- Nationality/Citizenship
- Gender (M/F)
- Document Type
- Document Number
- Document Country of Issuance
- Land Port of Exit (U.S.)
- Date of Entry (Mexico)
- Time of Entry (Mexico)

In the future, INM intends to transfer the following information it currently collects on non-Mexican nationals to CBP:

- Full Name (last, first, middle (if available))
- Date of Birth
- Nationality (citizenship)
- Gender (M/F)
- Document Type
- Document Number
- Document Country of Issuance
- Land Port of Entry
- Date of Entry
- Time of Entry

CBP retains exit records created from information obtained from Mexico in accordance with the BCI SORN. CBP continues to work with the National Archives and Records Administration to formalize the appropriate retention schedules based on the information below.

- USC and LPR information that is related to a particular border crossing is maintained for 15 years from the date when the traveler entered, was admitted to, or departed the United States, at which time it is deleted.
- Non-immigrant alien information related to a particular border crossing is retained for 75 years from the date obtained.

Any BCI records are linked to active law enforcement lookout records, CBP enforcement activities, or investigations will remain accessible for the life of the law enforcement activities to which they are related.

Privacy Risk: There is a risk that either agency will retain the information contained in CBP exit records for a longer period of time than is required by the originating agency's record retention.

Mitigation: This risk is managed through program agreements, by which the agencies have agreed that the information transferred will be governed by the *receiving* agency's retention schedules. However, because INM keeps all crossing records for 35 years they will be keeping crossing records on USCs and LPRs longer than the 15 years CBP keeps it for. Because both agencies have the right to collect the information, the retention schedules will always follow the receiving agency's requirements, regardless of the retention requirements of the sharing agency. CBP is bound by U.S. records laws and INM is bound by Mexican records laws. Each agency must retain records exchanged under this program in accordance with their designated schedules. CBP continues to work with the National Archives and Records Administration to formalize the records schedules listed above and develop a strategy for managing these records lifecycles appropriately. This plan will include a specific approach for expunging records from systems that have reached their disposition date. CBP will conduct an update to this PIA upon completion of the records schedule.

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.*

CBP will use the records shared under the U.S.-Mexico Entry/Exit Data Sharing Initiative to create exit records, as well as for other authorized purposes including but not limited to:

- For reconciliation of entry and exit data that indicate a lawful exit from either country;

- For potential cancellation of overstay warrants for those determined to have exited the United States; and
- To develop more precise and reliable exit data that can be applied to increase the effectiveness of border management and enable targeted policy development and implementation in the future.

CBP may also share information it receives from INM with other DHS Components as appropriate, and may share information outside of DHS consistent with the routine uses outlined in the BCI SORN and as otherwise authorized by law.

INM will initially store the records at its National Targeting Center, and will eventually store the records in the appropriate designated IT systems. INM may also use the records for statistical purposes to enhance information on tourism and immigration trends, as permitted by applicable law and policy.

Privacy Risk: There is a risk that CBP will use the information in a manner inconsistent with the purposes listed above.

Mitigation: The arrangements between CBP and INM set forth terms concerning the use of the information exchanged under this program.[25] CBP only shares information consistent with previously published system of records notices. The BCI SORN provides a comprehensive list of routine uses that are compatible with the purpose of collection and is available to the public on the DHS website and in the Federal Register.

Privacy Risk: There is a risk that CBP will use this information for a purpose beyond the original collection.

Mitigation: This risk of information being used for purposes other than what it was collected is mitigated through CBP's strict adherence to the confines of the arrangement negotiated with INM and applicable U.S. law. INM and CBP are permitted to use each other's land border crossing data for border crossing and immigration purposes, and for such purposes as otherwise authorized under their respective U.S. and Mexican laws. Information will be used primarily in support of CBP's border mission, which is consistent with the data collection's original purpose but is not limited solely to recording entries and exits or identifying overstays. Knowing when a person has entered and left the United States is important information that can inform a variety of Federal Government decisions, such as immigration benefits and law enforcement activities.

[25] CBP and INM intend to use the information obtained pursuant to the Implementing Arrangement for border crossing, immigration, or migratory purposes, and for such purposes as otherwise authorized under their respective U.S. and Mexican laws.

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.*

Because INM collects the shared information directly from the individual at the time of crossing, there is relatively high confidence that the information is accurate and current, assuming the individual is not using a fraudulent travel document. Individuals provide information to CBP in order to obtain a valid travel document. The information collected from travelers by INM is matched against the records previously provided to CBP. For non-USCs, CBP's ADIS system matches an exit record created with information provided by INM with a U.S. entry record for the same individual to verify his or her departure from the United States. CBP regularly tests the ADIS matching algorithm, which is able to accurately match records with an accuracy rate in the high 90th percentile. CBP periodically reviews non-matches to assess whether they may be the result of fraud or criminal behavior, and ADIS users are able to flag records in the rare instances that a matching error occurs. Exit records in CBP systems created from information provided by INM will be tagged as provided by INM. The relevance and limitation of the data is ensured because CBP and INM only share data captured in direct relation to the border crossing event. Both countries also intend to apply corrective action, if appropriate, and if notified that the data is incorrect and have procedures in place to notify the other country in the event that corrective action is necessary.

Privacy Risk: There is a risk that CBP will associate an exit record created from information provided by with the wrong individual.

Mitigation: This risk is mitigated through the use of existing access, redress, and corrective measures for border crossing information to correct information described in the BCI systems of records and under the *Principle of Individual Participation* outlined above. Because records are identified through a unique RFID number, there is a high degree of confidence that records will be associated with correct individuals.

Privacy Risk: There is a risk that travelers will use fraudulent documents to enter Mexico and those incorrect INM entry records will become CBP exit records.

Mitigation: This risk is partially mitigated through INM's extensive training in identifying fraudulent documents and suspicious behavior. INM examines all travel documents presented at crossing to determine their validity. All information received from INM is tagged accordingly, which allows CBP to conduct an audit, if necessary. In addition, CBP's queries into DHS law enforcement databases will reveal the existence of derogatory information, including prior use of fraudulent documents that may be associated with that traveler.

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.*

CBP and INM will exchange data under the U.S.-Mexico Entry/Exit Data Sharing Initiative through a secure encrypted device until such time as CBP and INM mutually determine that such data can be transferred electronically through a system-to-system connection. By using a secure encrypted device, CBP and INM control and restrict the information that may be transmitted between the agencies, thus mitigating the risk of improper disclosures. CBP will destroy the encrypted device in accordance with applicable CBP policies.

The United States and Mexico have signed the *Implementing Arrangement between the Department of Homeland Security, U.S. Customs and Border Protection, and the Secretariat of Governance, National Migration Institute, Regarding the Sharing of Border Crossing Data*, which specifies that each country intends to protect the information exchanged by applying appropriate technical safeguards to such information to protect against unauthorized access, disclosure, use, modification, or deletion. In the event that information is received by INM in error or otherwise due to a request inconsistent with the Implementing Arrangement and the Mexico Entry/Exit Data Sharing Initiative, it is to be destroyed immediately and may not be used further without the express prior written consent of CBP. Further, INM intends to notify CBP within 24 hours in the event that INM becomes aware of any unauthorized access, disclosure, use, modification, or deletion of information in its applicable databases. To safeguard the information received, both countries intend to limit the onward disclosure of this information according to the terms described in Section 5 above. Records received from INM are identified in BCI as having come from Mexico to assist DHS in limiting the onward disclosure of the information to those permissible purposes.

Privacy Risk: There is a risk that the security of the secure encrypted devices used to transmit the information between CBP and INM will be compromised or someone without authority will access the information.

Mitigation: This risk is mitigated through the commitment by both agencies to technical, security, and organizational procedures to protect the information exchanged. In the event of an apparent or confirmed breach, CBP and INM have established clear procedures for written notification and response.

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.*

Records maintained by DHS may only be disclosed to authorized individuals with a work-related need for the information and only for uses that are consistent with the intended purposes of the program. All information received from INM and retrieved from CBP systems under this initiative will be identified as such and will be stored and secured in accordance with DHS system security requirements and standards. Users of these systems must complete annual privacy training and be provisioned in the system to view the records based on their official need to know. User access and activities are audited, with audit logs that capture the date, time, and search terms, and misuse may subject the user to disciplinary consequences in accordance with DHS policy, as well as criminal and civil penalties.

Information maintained by INM may only be accessed by authorized individuals with an operational need-to-know and only for uses consistent with their program line of business. INM will store the biographic entry data received from the United States in accordance with the INM's security standards and is safeguarded through a number of technical, physical, and administrative safeguards.

Privacy Risk: There is a risk that a CBP user will view border crossing records exchanged under this program without the appropriate need to know.

Mitigation: This risk is mitigated through the provision of training on the appropriate use of systems of CBP personnel. Additionally, CBP system users are informed of the need-to-know requirement for access to records, including border crossing records. Audit logs allow CBP system administrators to oversee CBP user queries and identify potential misuse of the CBP system. All CBP users are educated on the consequences of misuse of records, which can include civil and criminal penalties as well as disciplinary actions. INM and CBP will strictly adhere to the *Implementing Arrangement between the Department of Homeland Security, U.S. Customs and Border Protection, and the Secretariat of Governance, National Migration Institute, Regarding the Sharing of Border Crossing Data* signed August 30, 2017. The Implementing Arrangement includes provisions regarding the disclosure of data, use of information, technical safeguards, and retention of information.

Privacy Risk: There is a risk that either party may not be able to audit and review the other's technical, physical, and administrative safeguards to protect the information that the two parties exchange.

Mitigation: CBP has implemented the auditing and accountability measures listed above,

including user access controls, system auditing capabilities and training requirements. Both INM and CBP will strictly adhere to the confidentiality and security of the information outlined in the Implementing Arrangement.

Responsible Officials

Michael M. Hardin
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs & Border Protection

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security