Privacy Impact Assessment
for the

Beyond the Border Entry/Exit Program Phase III

DHS/CBP/PIA-004(h)

August 12, 2016

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP), as a component of the Department of Homeland Security (DHS), is publishing this Privacy Impact Assessment (PIA) update to give notice of changes to the Beyond the Border Entry/Exit Program, an initiative of the U.S.-Canada Beyond the Border Action Plan. The Beyond the Border Entry/Exit Program expands the sharing of border crossing information with the Canada Border Services Agency (CBSA) by exchanging biographic, travel document, and other border crossing information collected from individuals entering the United States from Canada and vice versa at land ports of entry. This PIA update covers the third and final phase of the Entry/Exit Program, which is expanding to include the sharing of data on Canadian and U.S. citizens to allow both governments to use the other's entry data so that the record of a traveler's entry into one country can establish a record of exit from the other country.

Overview

To further its immigration, law enforcement, and national security missions, DHS is participating in the Beyond the Border Entry/Exit Program, a part of the U.S.-Canada Beyond the Border Action Plan (Action Plan).[1] Through this program, the United States and Canada seek to exchange biographic information on the entry of travelers at the common land border, such that a record of an entry into one country could be considered a record of an exit from the other. The framework for entry/exit information sharing between Canada and the United States, as identified in the Action Plan, mandates an integrated entry and exit data sharing mechanism between the two countries. Although CBP has considered a number of different exit mechanisms, such as the use of exit lanes, these solutions pose challenges for ports of entry with limited physical space and resources. Deploying an exit mechanism like the Entry/Exit Program has been deemed to be the most cost-effective and practical method for establishing exit information.

Program Phases

This program is being implemented in three phases. Phase I, implemented in 2012, piloted the exchange of information on third country nationals and permanent legal residents at four land border ports.[2] Building upon the pilot, Phase II institutionalized this exchange of data at all

[1] *United States–Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness Action Plan* (December 2011), *available at*: http://www.whitehouse.gov/sites/default/files/us-canada_btb_action_plan3.pdf.

[2] DHS/CBP/PIA-004(f) Western Hemisphere Travel Initiative (WHTI) Beyond the Border Entry/Exit Program Phase I, September 24, 2012, *available at: https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_whtibtb_sept2012.pdf*.

common land border ports in June 2013.[3] Phase III of this program will expand the exchange of data to include U.S. and Canadian citizens, and will continue the sharing of data on legal permanent residents and third country nationals.

Phase III Implementation

Implementation of Phase III of the Beyond the Border Entry/Exit Program involves CBP and CBSA sharing data on the land border crossings of U.S. and Canadian citizens and will occur in two stages. Phase III will also incorporate the sharing that is already ongoing, pursuant to Phase II. During the first stage of Phase III, to begin in August 2016, Canada will share biographic and entry data about U.S. citizens and U.S. nationals[4] who exit the United States and enter Canada at Canadian land ports of entry. The second stage for implementing Phase III is expected to begin in June 2017, and will expand the sharing of information to include biographic and entry data on Canadian citizens from the United States to Canada. Full implementation of Phase III and sharing of Canadian citizen data will occur once legislation permitting it passes Canada's parliamentary review.

Biographic entry data exchanged in Phase III serves U.S. objectives related to border management and law enforcement and enables both countries to:

- Reconcile entry and exit records that indicate a lawful exit from either country;
- Identify persons overstaying their lawful period of admission and enable the potential closure of immigration warrants;
- Identify persons subject to a removal or departure order and who are recorded as having departed.
- Identify individuals who may have failed to meet residency requirements for permanent resident status or citizenship applications; and
- Develop more concise and reliable exit data that can be applied to increase the effectiveness of border management and other law enforcement, counterterrorism, national security, and public health and safety needs.

Phase III uses the same secure connection as Phase II to transmit information between the United States and Canada. At the time of entry, a document reader scans the traveler's travel document and his or her entry data is collected and stored in a secure border crossing information

[3] DHS/CBP/PIA-004(g) Beyond the Border Entry/Exit Program Phase II, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-btbphase2-june2013.pdf.

[4] *See* 8 U.S.C. § 1408 for the definition of categories of individuals qualifying as U.S. nationals.

system. A subset of the 10 data elements collected (detailed in Section 4) will be securely transmitted in near real time. Border crossing records received from CBSA are stored in TECS (not an acronym), as part of the Border Crossing Information (BCI) system of records[5] as an implied exit from the United States to Canada. Implied exit records transmitted from CBP to CBSA will be stored in the CBSA's Entry/Exit Information System.

Consistent with Phase II, exit records regarding third country nationals and legal permanent residents received from Canada will be transmitted along with other BCI records to the Arrival and Departure Information System (ADIS).[6] ADIS matches the CBSA exit records with entry records about the individual for the immigration and law enforcement purposes mentioned above. When available, ADIS sends an implied exit record to CBP's Nonimmigrant Information System (NIIS)[7] to record the corresponding exit of a nonimmigrant alien's entry in that system.[8]

To ensure that the information is properly limited in scope, exchanged securely, accessed appropriately, and used responsibly, the United States has issued the following documents:

- Letter of Intent between the United States Department of Homeland Security and the Canada Border Services Agency for Phase I of the Entry-Exit System (LOI), September 9, 2012;
- Entry/Exit Information Systems Phase I Joint Canada-United States Report, May 2013,[9] and
- Annex Regarding the Sharing of Biographic Entry Data to the 2003 Statement of Mutual Understanding (SMU) on Information Sharing Between The Canada Border Services Agency (CBSA), The Department of Citizenship and Immigration Canada (CIC) and The U.S. Department of Homeland Security (DHS).[10]

Reason for the PIA Update

CBP is updating this PIA to provide notice to the public that it is implementing Phase III of the Beyond the Border Entry/Exit Program, starting with CBSA providing CBP with U.S.

[5] DHS/CBP-007 Border Crossing Information (BCI) (January 25, 2016), 81 FR 404, *available at:* https://www.regulations.gov/document?D=DHS-2016-0006-0001.
[6] DHS/CBP-021 Arrival and Departure Information System (ADIS) (November 18, 2015, 80 FR 53019, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2015-11-18/html/2015-29445.htm.
[7] DHS/CBP-016 Nonimmigrant and Immigrant Information (March 13, 2015), 80 FR 13398, *available at:* System of Records, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05804.htm.
[8] Note that information from CBSA is not sent directly to NIIS, because the matching functionality is done in ADIS. ADIS correlates the exit records with an entry record. ADIS then sends the complete record of entry and exit to NIIS for nonimmigrant aliens.
[9] https://www.cbp.gov/sites/default/files/documents/canada_usreport_3.pdf.
[10] See Appendix A.

citizen and nationals information in 2016, and expanding in 2017 to CBSA and CBP exchanging data on Canadian citizens, as well as CBP providing CBSA with U.S. Citizen and national information. Consistent with Phase II of the program, biographic and border crossing information will continue to be collected and shared regarding third-country nationals and legal permanent residents crossing the U.S.-Canadian land border.

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 PIAs 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 the Beyond the Border Initiative is a phased program, led by the CBP Entry/Exit Transformation (EXT) 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 Phase III of the Beyond the Border Initiative 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.*

U.S. citizens, third country nationals, and legal permanent residents traveling from the United States into Canada are required to provide information directly to CBP or CBSA, respectively, at the time of crossing. DHS provides general notice to the public of sharing of U.S. citizen information with Canada through this PIA, the PIA for Phases I and II, the Border Crossing Information (BCI) SORN, and the Beyond the Border Action Plan. DHS also provides notice via extensive information about the Beyond the Border program on the public-facing CBP website, press material, news articles, and via Congressional and industry briefings.

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

Mitigation: This risk is mitigated by a full public relations strategy regarding Beyond the Border, as described above. As most people crossing the United States-Canadian land border do so via car or bus, it is ineffective for CBP and CBSA to post specific signage at ports of entry due to limited time to communicate with travelers regarding specific uses of their information. However, in addition to the public relations strategy and materials available on the CBP website, CBP provides notice through privacy documentation that CBP shares traveler information with CBSA, and receives information from CBSA to complete the United States exit record.

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.*

CBP and CBSA share information collected directly from travelers at the time of their entry into the country. The direct participation of the traveler at the time of collection provides a higher degree of confidence that the data provided is accurate, timely, and complete. Individuals may decline to provide their information at the border, but it will result in their inadmissibility and denial of entry. Because crossing the border is considered a voluntary action, individuals must comply with the rules and regulations enforced by the relevant border authority.

The same access, redress, or correction measures that were instituted for prior phases of the Beyond the Border Entry/Exit Program are available for Phase III. Individuals may use the existing access, redress, and corrective measures for border crossing information to correct information described in the BCI systems of records.

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.

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 his or her information being shared between the United States and Canada.

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 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 to the laws and rules enforced by CBP and the CBSA.

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.*

The Entry/Exit Program is part of the Beyond the Border Action Plan, a program implemented as part of the Western Hemisphere Travel Initiative (WHTI).[11] The WHTI is a joint initiative between DHS and the Department of State to implement a requirement of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004,[12] which mandates that all travelers present a valid travel document when entering the United States. All information sharing is informed and guided by the Beyond the Border Action Plan: Statement of Privacy Principles.[13]

DHS has existing authorities to collect and use border crossing records from other countries. CBP maintains information in BCI pursuant to the following statutes:

- The Aviation and Transportation Security Act of 2001;[14]
- The Enhanced Border Security and Visa Entry Reform Act of 2002;[15]
- Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004;[16]
- The Immigration and Nationality Act (INA), as amended, including Title 8, Aliens and Nationality;[17] and
- The Tariff Act of 1930, as amended, including Title 19, Customs Duties.[18]
- CBP maintains records in NIIS pursuant to IRTPA; INA, as amended; the Homeland Security Act of 2002;[19] and Title 8, Aliens and Nationality.[20]
- CBP maintains information in ADIS pursuant to Title 6, Border, Maritime and Transportation Responsibilities,[21] and Title 8, Aliens and Nationality.[22]

---

[11] *United States–Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness Action Plan* (December 2011), *available at:* http://www.whitehouse.gov/sites/default/files/us-canada_btb_action_plan3.pdf.
[12] Pub. L. No. 108-458, 118 Stat. 3638.
[13] The Beyond the Border Action Plan: Statement of Privacy Principles was issued by Canada and the United States on May 30, 2012, *available at*: https://www.dhs.gov/xlibrary/assets/policy/beyond-the-border-action-plan-statement-of-privacy-principles.pdf.
[14] Pub. L. No. 107-71, 115 Stat. 597. 19 U.S.C. §§ 1628
[15] Pub. L. No. 107-173, 116 Stat. 543.
[16] Pub. L. No. 108-458, 118 Stat. 3638.
[17] 8 U.S.C. §§ 1185 and 1354.
[18] 19 U.S.C. §§ 66, 1433, 1454, 1485, 1624 and 2071.
[19] P. L. No. 107-296, 116 Stat. 2135.
[20] 8 U.S.C. §§ 1103, 1184, and 1354.
[21] 6 U.S.C. § 202.
[22] 8 U.S.C. §§ 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, and 1732.

Privacy risk: There is a risk that CBP will use this information for a purpose beyond immigration management; law enforcement; national security; counterterrorism; public health and safety; and to the extent required by U.S. law.

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 CBSA and the parameters of the routine uses listed in CBP's applicable public SORNs. CBP and CBSA have negotiated acceptable uses of each other's land border crossing data. CBSA permits CBP to use CBSA land border crossing data for: immigration management; law enforcement; national security; counterterrorism; public health and safety; and to the extent required by U.S. law.

Information will be used 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.

To ensure transparency, CBP has published SORNs for the systems that house the information exchanged with the CBSA. These SORNs outline the purposes for which CBP collects and maintains the information. The SORNs also list the routine uses of the information and detail which other entities may access the information, and for what purposes. CBP may share this information pursuant to routine uses when it deems the use to be compatible with the original purpose of the information collection. CBP updates these SORNS, as well as the relevant PIAs, whenever it intends to use the information for a new purpose.

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).*

No new categories of information will be collected by CBP or the CBSA from individuals as part of Phase III of the Beyond the Border Entry/Exit Program. The information sharing consists of information already collected as part of the existing border crossing process. CBSA and CBP will share the data elements listed below, which are collected during an individual's primary inspection upon arrival in the United States or Canada at any common land port of entry along the U.S.-Canadian border.

Information transferred from CBSA to CBP's BCI includes:

- Name (First, Middle, Last);
- Date of Birth;
- Nationality (citizenship);
- Gender;
- Document Type;
- Document Number;
- Document Country of Issuance;
- Port of entry location (Port code);
- Date of entry; and
- Time of entry.

CBP will transfer the same set of 10 data elements from BCI to CBSA once full implementation occurs.

CBP is not collecting any new information as part of the Beyond the Border Entry/Exit Program. CBP retains all information obtained from Canada according to the retention period for the destination system. CBP continues to work with the National Archives and Records Administration to formalize the appropriate retention schedules based on the information below.

- U.S. citizen information in BCI 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 from BCI.
- Third country national information collected and maintained in NIIS is used for entry screening, admissibility, and benefits purposes and is retained for 75 years from the date obtained. NIIS records that 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.
- For records retained in ADIS, records will be purged after 75 years or after the statute of limitations has expired for all criminal violations, whichever is longer.

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

schedule.

Mitigation: This risk is mitigated through program agreements, by which the agencies have agreed that the information transferred will be governed by the *receiving* agency's retention schedules. Therefore, the retention schedules will always follow the receiving agency's requirements, regardless of the retention requirements of the sharing agency. As with all international agreements, CBP is bound by U.S. records laws and the CBSA is bound by Canadian 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.*

Records shared under Phase III will be used by CBP to create an exit record in BCI, as well as for the purposes listed below:

- Reconciliation of entry and exit data that indicate a lawful exit from either country;
- Potential cancellation of overstay warrants for those determined to have exited the relevant country; and
- Development of more concise 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.

Information received by CBP from the CBSA may be shared with other DHS Components and be disclosed as required by U.S. law or to federal, state, local, or tribal government authorities for law enforcement, national security, counterterrorism, or public health and safety purposes.

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 the CBSA place restrictions upon the use of the information exchanged under this program. Further use of the information must be consistent

with the original purpose or pursuant to a requirement by U.S. law or for law enforcement, national security, counterterrorism, or public health and safety. Other uses of the information are subject to prior written consent by CBSA. CBP only shares information consistent with previously published system of records notices. The BCI, ADIS, and NIIS SORNs provide comprehensive lists of routine uses that are compatible with their various purposes and are available to the public on the DHS website and in the *Federal Register*.

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 CBP and CBSA collect the shared information directly from the individual at the time of crossing, there is relatively high confidence that the information is accurate and current. For legal permanent residents and third country nationals, CBP's ADIS system matches an implied exit record with an 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 over 99% of records. 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. The relevance and limitation of the data is ensured because CBP and CBSA only share data captured in direct relation to the border crossing event. The data is also timely and current, since CBSA transmits the data to CBP in near-real time. Both countries also intend to apply corrective action 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.[23]

Privacy risk: There is a risk that CBP will associate an implied exit record received from CBSA with the wrong individual.

Mitigation: This risk is mitigated through the implementation of Phase I of the program, which enabled CBP and CBSA to pilot the process of reconciling implied exit records with an entrance record for the same individual. CBP has consistently been able to reconcile approximately 99% of entry and exit records for in-scope travelers. Because records are reconciled using unique identifiers, including travel document number, there is a high degree of confidence in a record match.

[23] See Appendix A, Section 13 (Compliance and Review).

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.*

Technical access is provided to CBSA through an existing secure electronic connection, which will be used to transmit information between CBP and CBSA. By using this existing secure connection, CBP and CBSA control and restrict the information that may be transmitted between the agencies, thus mitigating the risk of improper disclosures.

The United States and Canada have signed an Annex to the SMU,[24] which specifies that each country intends to protect personal information by appropriate technical, security, and organizational procedures and measures to guard against such risks as loss, corruption, misuse, unauthorized access, alteration, disclosure or destruction, or any other risks to the security, confidentiality, or integrity of the information. Further, each country intends to notify the other in writing as soon as practicable, but no later than 24 hours after any accidental or unauthorized access, use, disclosure, modification, or disposal of information received under the Annex to the SMU, and within 24 hours of becoming aware of the breach, to furnish all necessary details of the accidental or unauthorized access, use, disclosure, modification, or disposal of that information.

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.[25] Records received from CBSA are identified in BCI as having come from Canada 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 connection used to transmit the information between CBP and CBSA will be compromised.

Mitigation: This risk is mitigated through the commitment by both agencies to technical, security, and organizational procedures to protect the information exchanged. CBP and CBSA have been exchanging information under the Beyond the Border Entry-Exit program using secure servers, routers, and a private electronic transmission channel established prior to the beginning of the program. In the event of an apparent or confirmed breach, CBP and CBSA have established clear procedures for written notification and response.

[24] See Appendix A.
[25] See Appendix A, Section 8

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 stored in CBP systems, including information received from Canada under this program, is 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 the CBSA may only be accessed by authorized individuals with an operational need-to-know and only for uses consistent with their program line of business. Formal audit controls are in place to ensure that CBSA IT systems record the user ID, timestamp, and actions taken by each user for each query. All information stored in CBSA's Entry/Exit Information System including biographic entry data received from the United States, is stored in accordance with the CBSA's security standards and is safeguarded through a number of technical, physical, and administrative safeguards. Authorized users are required to complete mandatory privacy training as well as ongoing annual training in order to maintain their authorization and role-based user access to secure CBSA databases.[26]

Privacy risk: There is a risk that a CBP or CBSA 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 and CBSA personnel. Additionally, system users are informed of the need-to-know requirement for access to records, including border crossing records. Audit logs allow system administrators to oversee user queries and identify potential misuse of the system. All users are educated on the consequences of misuse of records, which can include civil and criminal penalties as well as disciplinary actions.

Privacy risk: There is a risk that either party may not be able to audit and review the

[26] *See* Annual Report to Parliament on the Privacy Act, Canada Border Services Agency 2013-2014, for an example of CBSA training and auditing requirements, *available at* http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/pa-lprp-20132014-eng.html.

other's technical, physical, and administrative safeguards to protect the information that the two parties exchange.

Mitigation: This risk is mitigated by clauses in the Phase III documentation that enable mutual review of the other parties' safeguards upon request. Further, both CBP and CBSA have implemented the auditing and accountability measures listed above, including user access controls, system auditing capabilities and training requirements.

Responsible Officials

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

Debra L. Danisek
Acting CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature Page

Original signed copy on file with DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security