



Privacy Impact Assessment  
for the

# Biographic Visa and Immigration Information Sharing with Canada

**DHS/CBP/PIA-023**

**February 10, 2014**

**Contact Point**

**Mark Koumans**

**Principal Deputy Assistant Secretary**

**Office of International Affairs**

**U.S. Department of Homeland Security**

**(202) 282-8000**

**Reviewing Official**

**Karen L. Neuman**

**Chief Privacy Officer**

**Department of Homeland Security**

**(202) 343-1717**



## Abstract

Under the United States-Canada Biographic Visa and Immigration Information Sharing (BVIIS) program, the Department of Homeland Security (DHS) makes certain biographic information from its systems of records available to the Department of Citizenship and Immigration Canada (CIC) and the Canada Border Services Agency (CBSA) via query through the Department of State's (DOS) Consular Lookout and Support System (CLASS). CIC and CBSA will use the information to assist in the administration and enforcement of Canada's immigration laws. Similarly, CIC and CBSA will make certain biographic information from the Global Case Management System (GCMS), which is Canada's system used to process applications for citizenship and immigration services, available to DHS via query through CLASS. DHS will use this information to assist in the administration and enforcement of the United States' immigration laws. This Privacy Impact Assessment (PIA) provides notice to the public regarding the information sharing and resulting privacy impacts of the BVIIS program.

## Introduction

The United States (U.S.) and Canada (the Participants) have a long history of sharing information to support the administration and enforcement of their respective immigration laws. The U.S. and Canada currently exchange immigration information on a case-by-case basis pursuant to a *Statement of Mutual Understanding on Information Sharing* (SMU), and its annexes.<sup>1</sup>

In addition, the *United States-Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness Action Plan*<sup>2</sup> (BTB Action Plan) calls for enhanced information sharing to strengthen the ability of Canada and the U.S. to increase security, counter fraud, promote mobility, and improve efficiency within, at, and beyond our shared border. The BTB Action Plan further recognizes the need to supplement existing information sharing activities, such as those under the SMU. The BTB Action Plan further recognizes the need to have timely access to current and accurate information in support of the parties' collaborative efforts to administer and enforce each nation's respective immigration laws. To meet these needs, Canada and the U.S. have agreed to develop and implement a systematic, automated process for conducting immigration information exchanges.

---

<sup>1</sup> *Statement of Mutual Understanding on Information Sharing among the Department of Citizenship and Immigration (CIC) and the U.S. Immigration and Naturalization Service (INS) and the U.S. Department of State (DoS)*, February 27, 2003 (the "Statement of Mutual Understanding") and the *Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims to the Statement of Mutual Understanding on Information Sharing between the Department of Citizenship and Immigration Canada (CIC) and the Bureau of Citizenship and Immigration Services (BCIS), of the U.S. Department of Homeland Security (DHS)*, August 22, 2003, (the "Asylum Annex").

<sup>2</sup> February 4, 2011, available at: <http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf>.



To accomplish this goal, in December 2012, both countries entered into *The Agreement Between the Government of Canada and the Government of the United States of America for the Sharing of Visa and Immigration Information*<sup>3</sup> (the Agreement); which lays out mutual obligations for relevant biographic and biometric-based information sharing. In order to carry out the biographic information sharing called for in the Agreement, the Parties entered into an *Arrangement between the Department of Citizenship and Immigration Canada, the Canada Border Services Agency, and the Department of State and the Department of Homeland Security of the United States concerning Biographic Visa and Immigration Information Sharing*<sup>4</sup> (the Arrangement).<sup>5</sup> The Arrangement establishes guidelines for sharing biographic visa and immigration information through automated processes to assist in the effective administration and enforcement of their respective immigration laws. Together, these two documents establish and govern the Biographic Visa and Immigration Information Sharing (BVIIS) program.

This PIA provides public notice about information sharing under the BVIIS program, and resulting privacy impacts. While the Agreement and subsequent Arrangement govern the BVIIS, the Parties incorporated the BTB Privacy Principles into the Agreement and Arrangement to guide and inform all BTB information sharing activities, including the BVIIS program. The BTB Privacy Principles<sup>6</sup> are aligned with the *DHS Fair Information Practice Principles*<sup>7</sup> (FIPPs). For purposes of this PIA, the BTB Privacy Principles and DHS FIPPs are used interchangeably for ease of reference and analysis.

## **1. Overview of Automated Process**

DHS currently sends certain immigration and law enforcement data sets to the Department of State (DOS) consistent with their shared visa and immigration processing missions. The records are transmitted via CBP's TECS system<sup>8</sup> and maintained in DOS's CLASS system. Under the terms of the Agreement and Arrangement, DHS and DOS make

---

<sup>3</sup> See Appendix A.

<sup>4</sup> December 2013. See Appendix B.

<sup>5</sup> A biometric implementing arrangement will be established for biometric-based information sharing under the Agreement.

<sup>6</sup> *Beyond the Border Action Plan: Statement of Privacy Principles by the United States and Canada*, May 2012. See Appendix C.

<sup>7</sup> DHS Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 29, 2008, available at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>8</sup> The TECS (not an acronym) system serves as an information-sharing platform among CBP and other agencies through which users are able to provide, access, and/or maintain law enforcement, immigration enforcement, inspection, intelligence-gathering, and operational records relevant to CBP and other agencies' antiterrorism and law enforcement missions. PIA: DHS/CBP/PIA-009(a) – TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (August 5, 2011), available at: <http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf>. SORN: [DHS/CBP-011 - U.S. Customs and Border Protection TECS](#), 73 FR 77778 (December 19, 2008).



certain limited derogatory records about third country nationals (non-U.S. or Canadian citizens or U.S. nationals) available to Canada by permitting authorized CIC and CBSA users to query records in CLASS based on the restrictions and conditions described below. Similarly, authorized DHS and DOS users can query CIC's GCMS to receive certain limited derogatory records about third country nationals. The TECS-to-CLASS and CLASS-to-GCMS connections are secure, encrypted system-to-system connections to safeguard the data in transit.

The Participants have agreed that the exchange of information should be limited in scope to exclude citizens of Canada and the U.S. and U.S. nationals. The exchange of information is thus subject to the following limitations:

**a. Queries**

The Participants intend to submit queries to each other's systems on persons believed to be third country nationals. This means the Participants do not intend to submit queries regarding persons identified on the basis of applicant responses on an immigration benefit request, identity documentation provided, or the nature of the application or investigation as:

- A citizen of Canada, or a citizen or national of the U.S.;
- for Canadian queries, a Permanent Resident of Canada; or
- for U.S. queries, a Lawful Permanent Resident (LPR) of the U.S.

As a further protective measure, the Participants do not intend to send queries relating to:

- Refugee Status Claimants at the time of application for protection;<sup>9</sup> or
- Persons, when such queries are inconsistent with the laws of the querying Participant, or detrimental to the national sovereignty, national security, public policy, or other important national interest of their respective countries, consistent with Article 8 of the Agreement.<sup>10</sup> For example, for the United States Participants, this includes applicants for and beneficiaries of applications under U.S. law for T (victims of human trafficking) or U (victims of crime who are cooperating with law enforcement) non-immigrant status or Violence Against Women Act relief.<sup>11</sup>

The Participants will only send queries about third country nationals who have applied for admission, a visa or other immigration benefit, or who are the subject of an investigation.

Through the BVIIS program, users will submit queries consisting of the following data elements, when available:

---

<sup>9</sup> This does not preclude the Participants from sending Queries on Refugee Status Claimants in other immigration contexts.

<sup>10</sup> See Appendix A.

<sup>11</sup> See 8 U.S.C. § 1367.



1. Last name;
2. First name;
3. Alias last name(s);
4. Alias first name(s);
5. Date of birth;
6. Country of birth;
7. Passport nationality (given nationality if passport not available);
8. Gender;
9. Travel document number; and
10. Travel document issuing authority or country.

## **b. Responses**

Participants will respond to a query with data from potentially matching records only if a potential match:

- is believed, on the basis of data available to the Participant, to be a third country national;
- is identified based on mutually determined criteria that ensure a high degree of certainty in the accuracy of potential matches; and
- has one or more of the following:
  - A previous decision or determination in which the person failed to meet the requirements, including admissibility or eligibility requirements, of the immigration law of their respective countries; or
  - Other derogatory data related to the person that is relevant to administering or enforcing the immigration law of their respective countries.

Pursuant to the Agreement, a Participant may decline to provide a response, in whole or in part, if it determines that sharing biographic data through the automated query responses is inconsistent with the laws of its country, or is detrimental to its national sovereignty, national security, public policy, or other important national interest.<sup>12</sup> If the Participant makes such a determination, it may decline to provide any such biographic data, or offer to provide all or part of the biographic data subject to specific terms and conditions.

Pursuant to Article 8 of the Agreement, DHS and DOS will limit the data available to Canada by filtering out records or excluding whole data sets containing these categories of

---

<sup>12</sup> See Article 8 of the Agreement, Appendix A.



records and individuals, including data sets likely to have U.S. citizens or nationals, LPRs, and applicants for or beneficiaries of applications under U.S. law for T or U non-immigrant status or Violence Against Women Act relief.

If a matching record is found that complies with the restrictions and conditions of this program, the receiving system provides the following limited biographic data, when available:<sup>13</sup>

1. Last name;
2. First name;
3. Alias last name(s);
4. Alias first name(s);
5. Date of birth;
6. Alias date(s) of birth;
7. Country of birth;
8. Alias country or countries of birth;
9. Passport nationality (given nationality if passport not available);
10. Gender;
11. Travel document number;
12. Travel document issuing authority or country;
13. Date of outcome of application, encounter, or record;
14. Place of refusal;
15. Date of application, encounter, or record;
16. Type of application, encounter, or record;
17. Date of Entry;
18. Port of Entry;
19. Indicator of the derogatory data;
20. Date removal order enforced; and
21. Current immigration status.

---

<sup>13</sup> These data elements do not contain the full content of the record, which may include comments or narrative information that may be more sensitive and require manual review before being shared.



## **2. DHS Information Exchanged**

In order to limit the data DHS provides to CIC and CBSA to only that which is required under the Agreement and Arrangement, DHS components identified the following data sets that contain derogatory records about third country nationals:

- Derogatory records entered by U.S. Citizenship and Immigration Services (USCIS) into TECS<sup>14</sup> regarding immigration fraud, denials of a benefit request, and/or notices to appear to initiate removal proceedings.
- Immigration and Customs Enforcement's (ICE) ENFORCE Alien Removal Module's<sup>15</sup> (EARM).
  - Alien Absconders (fugitive aliens)
  - Final Orders of Removal
- CBP's Electronic System for Travel Authorization (ESTA)<sup>16</sup> denials.

No other DHS data sets stored in CLASS are accessible to CIC and CBSA users.

Canada has authorized DHS users to query CIC's GCMS records through DOS's CLASS system. These users consist of USCIS and ICE employees who have received training about the use and limitations of the data. USCIS's users include employees in the Office of Fraud Detection and National Security (FDNS), Service Center Operations, and Field Operations Directorate. The results of their queries are stored in the FDNS<sup>17</sup> system of records and/or the Alien File, Index, and National File Tracking System of Records<sup>18</sup> (A-File), as appropriate. ICE users include employees in the Fugitive Operations Support Center, who store the results of their queries in EARM. ICE users are also sending a list of Alien Absconders from ICE's EARM in a one-time bulk query of GCMS to determine whether the individual has been encountered in Canada. This process enables ICE to record the individual's departure from the U.S.

## **3. Follow Up Requests**

Because this exchange does not provide systematic access to the full record, the U.S. and Canada may use the results of the query to make a separate manual request for additional information, including for the full record, subject to the terms of the SMU. These requests and responses are encrypted between the Participants' designated points of contact to safeguard the data in transit. To limit the information sharing to only that which the requesting Participant needs in furtherance of its immigration and law enforcement purposes, the Participants indicate

---

<sup>14</sup> [DHS/CBP-011 - U.S. Customs and Border Protection TECS](#), 73 FR 77778 (December 19, 2008).

<sup>15</sup> [DHS/ICE-011 - Immigration and Enforcement Operational Records System \(ENFORCE\)](#), 75 FR 23274 (May 3, 2010).

<sup>16</sup> [DHS/CBP-009 - Electronic System for Travel Authorization \(ESTA\)](#), 77 FR 44642 (July 30, 2012).

<sup>17</sup> [DHS/USCIS-006 - Fraud Detection and National Security Records \(FDNS\)](#), 77 FR 47411 (August 8, 2012).

<sup>18</sup> [DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records \(A-File\)](#), 76 FR 34233 (June 13, 2011).



what additional information is needed in the follow up request (e.g., photo, reason for refusal).

This process allows each country to manually review the full contents of the record and determine whether the sharing is inconsistent with the laws of its country, or detrimental to its national sovereignty, national security, public policy, or other important national interest.

## Fair Information Practice Principles (FIPPs)

Section 222(2) of the Homeland Security Act of 2002 directs the DHS Chief Privacy Officer to assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

The DHS Privacy Office developed a set of *Fair Information Practice Principles* (FIPPs) to encompass the full breadth and diversity of the Department's programs, operations and systems.<sup>19</sup> The FIPPs reflect the nature and purpose of the information being collected in relation to DHS's mission.

DHS conducts PIAs for both programs and information technology systems, pursuant to the E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899; and the Homeland Security Act of 2002, Pub. L. No. 107-296, § 222, 116 Stat. 2135. However, the BVIIS is an information sharing program rather than an information technology system. Accordingly, this PIA examines the privacy impact of the BVIIS program as it relates to the Fair Information Practice Principles.

### 1. Principle of Transparency

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

**BTB Privacy Principle #9: Transparency and Notice** - The U.S. and Canada are to provide individuals, as required by law, with general and, as appropriate, individual notice, at least as to the purpose of the provision, receipt and use of PII that concerns the individual, the identity of the entity controlling that information, the applicable rules or laws, the types of third parties to whom information may be subsequently disclosed, as well as other information insofar as is necessary to seek effective sanctions and/or remedies. Should notice need to be limited for national security or law enforcement reasons, such as the protection of an ongoing

---

<sup>19</sup> DHS Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008.



investigation or the protection of victims or witnesses, the limitation on notice should be consistent with domestic law

In addition to the publication of the Agreement and the Arrangement, DHS is providing notice through this PIA about its biographic information sharing with Canada. Regarding the information provided to Canada, biographic data provided in response to a query, and full records provided in response to a follow up request, come from existing DHS source systems for which SORNs<sup>20</sup> have already been published. DHS also provides general notice in each of the source system SORNs that information may be shared pursuant to Routine Use G.<sup>21</sup> Additional notice is provided on immigration benefit request forms and/or in instructions indicating that the provided information will be used to determine an individual's eligibility or admissibility.

With regard to the information received from Canada, each DHS system of records contains access and amendment provisions, subject to certain exemptions. Due to the law enforcement nature of these records and consistent with relevant Privacy Act exemptions, an individual may not be specifically notified that DHS has received records from Canada about him or her. Canada does not store the data received from these systems; instead, it queries the system directly to obtain derogatory records.

---

<sup>20</sup> DHS/CBP-011 - U.S. Customs and Border Protection TECS (December 19, 2008).

DHS/ICE-011 - Immigration and Enforcement Operational Records System (ENFORCE) (May 3, 2010).

DHS/CBP-009 - Electronic System for Travel Authorization (ESTA) (July 30, 2012).

<sup>21</sup> 19 Routine Use G, which allows sharing of A-File and FDNS-DS:

To appropriate federal, state, tribal, territorial, local, international, or foreign law enforcement agencies or other appropriate authorities charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

For ESTA:

To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations.

For TECS:

To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

And for ENFORCE:

To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.



Under the terms of the BTB Privacy Principles and relevant law, regulation, and policy, Canada provides similar notice about the sharing of biographic data with the U.S.<sup>22</sup> In addition, all of Canada's immigration application forms, including claims for protected person status, provide notice that PII collected by CIC may be disclosed to a foreign government when that information may be relevant to administering or enforcing the foreign government's immigration laws. These forms also seek consent to allow the Canadian Government to collect PII from a foreign government that may be relevant to administering or enforcing Canadian immigration laws.

## 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.*

**BTB Privacy Principle #8: Individual Access and Rectification** - The U.S. and Canada are to provide individuals with access to and the means to seek rectification and/or expungement of their PII. Should access to PII need to be limited, the specific grounds for any restrictions are to be specified consistent with domestic law. In appropriate cases, an individual may object to the provision, receipt and use of PII related to him or her.

The Privacy Act of 1974 extends access and amendment rights to U.S. citizens and LPRs. As a matter of policy, DHS extends these rights to all persons, regardless of citizenship. When DHS retains Personally Identifiable Information (PII) from the results of a query or follow up request, the information is stored in one of the listed DHS systems of records. Consistent with Article 5 of the Agreement and DHS policy, DHS permits individuals to access and amend that information subject to the processes and exemptions listed in the relevant SORN.

Generally, persons may request to access, correct, or add a notation to indicate a correction request was made to their records from DHS through its website, <http://www.dhs.gov/freedom-information-act-and-privacy-act>, or through mail addressed to:

Chief FOIA Officer  
The Privacy Office  
U.S. Department of Homeland Security  
245 Murray Lane SW, STOP-0655,  
Washington, D.C. 20528-0655.

Persons who wish to access biographic data held by DOS may contact the U.S. Department of State via:

---

<sup>22</sup> Available at: <http://canadagazette.gc.ca/rp-pr/p1/2013/2013-10-05/html/reg2-eng.html>



Director  
Office of Information Programs and Services (A/GIS/IPS)  
515 22nd Street NW, Room 8100, SA-2  
Department of State  
Washington, D.C. 20522-6001

Persons who wish to access biographic data held by the Government of Canada may visit <http://www.cic.gc.ca/english/department/atip/requests-atip.asp> for additional information on how to make an online or written request to access their PII.

***BTB Privacy Principle #10: Redress*** - The U.S. and Canada are to provide, consistent with their respective domestic law, effective remedies before a fair and objective authority where a person's privacy has been infringed or where there has been a violation of data protection rules with respect to that individual. Any such infringement or violation is to be subject to appropriate and effective sanctions and/or remedies. Redress may not be available for frivolous claims or where there has been no material infringement of a person's privacy.

The DHS Traveler Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals who have inquiries or who seek resolution regarding difficulties they experienced during travel screening at transportation hubs—like airports and train stations—or crossing U.S. borders, including watch list issues, screening problems at ports of entry, and situations in which travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our nation's transportation hubs. DHS TRIP is part of an effort by the Departments of State and Homeland Security to welcome legitimate travelers while still securing our country from those who want to do us harm. The DHS TRIP is accessible at <http://www.dhs.gov/dhs-trip>, or via post at:

U.S. Department of Homeland Security  
Traveler Redress Inquiry Program (DHS TRIP)  
601 South 12th Street, TSA-901  
Arlington, VA 20598-6901

The DHS Office of Citizenship and Immigration Services Ombudsman also assists individuals who may wish to resolve issues regarding petitions to U.S. Citizenship and Immigration Services (USCIS). The contact information is as follows:

Office of the Citizenship and Immigration Services Ombudsman  
Department of Homeland Security  
Mail Stop 0180 Washington, D.C. 20528  
Phone: 1-855-882-8100 (toll free) or 202-357-8100 (local)  
Fax: 202-357-0042



By e-mail: [cisombudsman@dhs.gov](mailto:cisombudsman@dhs.gov)

Persons wishing to correct biographic data held by the Government of Canada, or to request to add a notation to indicate a correction request was made, may submit a correction request to:

Access to Information and Privacy Division  
Citizenship and Immigration Canada  
Ottawa, ON K1A 1L1

or to:

Canada Border Services Agency  
Access to Information and Privacy Coordinator  
410 Laurier Avenue West, 10th floor  
Ottawa, ON K1A 0L8

### 3. Principle of Purpose Specification

*Principle:* DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

**BTB Privacy Principle #1: Purpose Specification** - The purposes for which PII is provided, received and used are to be specified in any BTB arrangements or initiatives and such PII is to be subsequently used in furtherance of the fulfillment of those purposes or such other lawful purposes as are not incompatible with those purposes and are specified either in the relevant BTB arrangement or initiative or in a notice to the public and to the other participant in the relevant BTB arrangement or initiative.

DHS administers and enforces U.S. immigration law pursuant to the Immigration and Nationality Act, as amended.<sup>23</sup> Specific mission authorities for each component to provide and receive derogatory biographic data to and from Canada may be found in the SORNs listed in the Overview under DHS Information Exchanged, above.

As noted, the SMU, Agreement, and Arrangement permit DHS to access biographic data from Canada, to enforce U.S. laws, and in return, to provide biographic data to Canada for law enforcement purposes by:

- using the biographic information to enforce or administer the immigration laws of the Participants;

---

<sup>23</sup> See 8 U.S.C. § 1101 *et seq.*



- furthering the prevention, investigation, or punishment of acts that would constitute a crime rendering a third country national inadmissible or removable under the immigration laws of the Participant providing the information; or
- facilitating the Participants' adjudication of an application for a visa, admission, or other immigration benefit, or determination of whether an individual is to be ordered removed by providing information regarding the admissibility of the individual.

***BTB Privacy Principle #4: Non-Discrimination*** - Canada and the U.S. are to apply this Statement of Privacy Principles to all individuals on an equal basis without unlawful discrimination.

Queries are conducted as part of DHS's authorized operations to administer and enforce immigration laws, so long as the individual queried meets the criteria of the Agreement and Arrangement. Biographic data results are provided to Canada automatically, using the methods described above to properly protect sensitive information and classes of individuals.

#### **4. Principle of Data Minimization**

***Principle:*** *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

***BTB Privacy Principle #2: Relevant and Necessary/Proportionate*** - PII is to be provided, received and used to the extent it is relevant, necessary and appropriate to accomplish a clear purpose set out in any BTB arrangements or initiatives.

The U.S. and Canada are implementing several measures to ensure they only collect and share the minimum amount of data necessary to assist in the administration and enforcement of each country's respective immigration laws. CLASS and GCMS are configured to ensure a high degree of confidence that any matching records actually pertain to the queried individual. If the matching record contains information that would be improper to share (because it would be inconsistent with domestic law, detrimental to national sovereignty, national security, public policy, or other important national interest, such as applicants for or beneficiaries of applications under U.S. law for T or U non-immigrant status or Violence Against Women Act relief), the system provides the user a "No Match" result.

Although the Agreement prohibits sharing information about U.S. citizens, nationals, and LPRs, or Canadian citizens and permanent residents, there is a risk that the Participants may unintentionally exchange this information. This unintentional sharing can occur if a third country national changed immigration status and that change in status is not reflected in a source system. To mitigate this risk, DHS and DOS filter query results from Canada to exclude these or other records that appear to be out of the scope of the Agreement. While these records may be



shared on a case-by-case basis under the terms of the SMU, DHS will review the responses it provides to Canadian queries and make adjustments to exclude any further exchanges of information likely to be out of scope of the Agreement. These exchanges will undergo the same quality assurance and privacy safeguard review as the other information exchanges discussed in this PIA.

Matching records that are provided to the Participant consist of only those data elements necessary to indicate the nature of the derogatory information. Participants do not retain query results unless the biographic data pertains to the individual queried. When a result is received that actually pertains to an individual queried, users manually enter the information into their case files in their systems of records and mark the information as having been received from the other country. All other results about an individual are immediately destroyed.

***BTB Privacy Principle #12: Retention*** - The U.S. and Canada are to retain PII only so long as necessary for the specific purpose for which the information was provided or further used, and in accordance with their respective domestic laws.

The CLASS and GCMS systems are configured to destroy irrelevant and unnecessary data. With regard to biographic data contained in a query, each system keeps audit logs containing the queries it sends, but does not retain queries received. The system receiving the query will immediately destroy the biographic data from the query after searching for matching records and providing a response.

When a DHS user manually enters GCMS response information into a DHS system of records, the information is retained according to the retention schedule for the DHS system. The pertinent portions of the current retention schedules for the DHS systems are:

**A-File:** This system of records is the official record system that contains information regarding the transactions of an individual as he/she passes through the U.S. immigration and inspection process. The A-File records are permanent whether hard copy or electronic. A-Files are transferred to the custody of the National Archives 100 years after the individual's date of birth. Newly-eligible files are transferred to the National Archives every five years.<sup>24</sup>

**FDNS:** This system of records assists USCIS in recording, tracking, and managing immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns. FDNS records have a retention period of 15 years from the date of the last interaction between FDNS personnel and the individual after which time the record will be deleted from FDNS. The 15-year retention schedule provides FDNS with access to information that is critical to the investigation of suspected or confirmed fraud, criminal activity, egregious public safety, and/or national

---

<sup>24</sup> NARA Schedule N1-566-08-011.



security concerns. Upon closure of a case, any information that is needed to make an adjudicative decision (such as a statement of findings report), whether there was or was not an indication of fraud, criminal activity, egregious public safety, and/or national security concerns, is transferred to the A-File and maintained under the A-File retention period of 100 years after the individual's date of birth.<sup>25</sup>

**ENFORCE:** This system of records contains the Enforcement Integrated Database (EID), which captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations. ICE retains records of arrests, detentions, and removals in the EID for 100 years.<sup>26</sup>

DOS will retain information in accordance with the Foreign Records Disposition Schedules, Chapter 9.

The CIC will retain information obtained from DHS in accordance with the departmental “Temporary & Permanent Migration Retention and Disposition Schedule.” The CBSA intends to retain information in accordance with the Institution Specific Disposition Authority.

## 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.*

**BTB Privacy Principle #11: Restrictions on Onward Transfers to Third Countries** - Where PII is provided, in accordance with relevant domestic law, by a competent authority of the U.S. or Canada (the originating country) to a competent authority of the other nation (the receiving country), the competent authority of the receiving country is to authorize or carry out an onward transfer of this information to a third country only if consistent with the domestic law of the receiving country, and in accordance with existing applicable international agreements and arrangements.

In the absence of such international agreements and arrangements, the receiving country may transfer the PII to a third country when consistent with the domestic law of the receiving country, in which case the originating country is to be notified:

- i. prior to the transfer; or
- ii. as soon as reasonably possible after the transfer in the case of exigent circumstances.

<sup>25</sup> NARA Schedule N1-566-08-18

<sup>26</sup> See DHS/ICE/PIA-015, Enforcement Integrated Database (EID) PIA and the associated PIA updates, at <http://www.dhs.gov/privacy-documents-ice>.



As noted, the Participants are exchanging biographic data to assist in the effective administration and enforcement of the immigration laws of the U.S. and Canada. DHS users must protect records received from Canada, including restricting access to those with an official “need to know,” and use it solely for the purpose for which it was collected in support of DHS’s immigration administration and enforcement missions.

Consistent with Article 4 of the Agreement, the Participants may make disclosures as part of an immigration proceeding or under other appropriate circumstances, including as part of a criminal prosecution or in response to a written request from a body with jurisdiction to compel the production of the information. Aside from disclosures in immigration proceedings, the disclosing Participant must notify the other Participant in advance about the disclosure, absent exceptional circumstances. The Participants mark biographic data exchanged as having been received from the other Participant. This marking assists each Participant in restricting the dissemination of the information and ensure the providing Participant is consulted before the information is distributed.

## 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.*

BTB Privacy Principle #3: **Integrity/Data Quality** - Canada and the U.S. are to make reasonable and appropriate efforts to maintain PII accurately and completely, including any caveats or conditions attached to the information. Any further related information, including updates or clarifying information, is to be included to ensure continuing accuracy and completeness.

When a result is received that actually pertains to the individual queried, Participant users manually enter the information into their case files in their systems of records and mark the information as having been received from the other country. This raises a risk that information may be inaccurately transcribed. However, all DHS users are trained to accurately transcribe information as part of their normal business processes. Further, all DHS users are trained to mark the source of the records as having been received from Canada, so that information can be checked against the source system in the event of a discrepancy.

As part of the functionality of CLASS and GCMS, users “subscribe” to matching results in order to be notified if a record is later determined to be inaccurate. If a Participant has reason to believe that it provided inaccurate biographic data, the providing Participant promptly notifies the requesting Participant through the subscription service. Any previously exchanged inaccurate biographic data must be corrected or destroyed. An acknowledgment message will be sent in response to a correction notification confirming the correction request was received.

When DHS corrects a record in one of its data sets, the correction is automatically transmitted to CLASS. CLASS then updates its records and sends a notification to the CIC or



CBSA user that subscribed to the previously inaccurate record, informing him or her of the update. When DHS receives corrected information, it makes a notation in its systems of records and corrects the record as part of its normal business practices.

For purposes of the review process described in Article 10 of the Agreement, the Participants intend to review on an annual basis the volume of transactions and the outcomes and the timeliness of the responses to queries based on mutually decided performance and management measurements, which may include, but are not limited to:

- The number of exchanges from which biographic data was provided to visa, immigration, and border-control decision makers before they made a decision;
- the number and severity of any security or privacy breaches of the information sharing system, databases, or PII exchanged under the Arrangement as well as a summary of remedial actions taken; and
- each Participant's timeliness in responding to queries.

The Participants intend to carry out regular quality assurance activities, including a review of applicable privacy safeguards, using a mutually decided methodology to ensure that the activities carried out under the Arrangement are consistent with the principles outlined by the Arrangement. These quality assurance activities may include, but are not limited to determining:

- whether biographic data has been retained when it should have been destroyed;
- whether biographic data exchanged under the Arrangement has been marked as having been received from the other Participant; and
- whether biographic data has been disclosed in a manner inconsistent with Article 4 of the Agreement.

## 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.*

**BTB Privacy Principle #5: Information Security** - PII is to be protected 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. Only authorized individuals with an identified purpose are to have access to PII.

### a. Canada

In order to protect the information transmitted between the Participants, all system-to-system connections are encrypted. Within the systems, CLASS and GCMS employ passwords



and other safeguards to restrict access to the information. All users must have completed background checks. User roles are assigned based on the employee's official need to know the information. A user may not see data beyond his or her user role.

Canada employs some foreign nationals (Locally Engaged Staff), to assist with its immigration and visa processing in its overseas offices. These employees have completed background investigations and are authorized to use information necessary to assist them with performing visa and immigration benefit processing. To further protect the information provided by the U.S., Canada restricts Locally Engaged Staff from accessing certain types of biographic data determined by DHS and DOS to be sensitive.

## **b. United States**

Once DHS incorporates the information into one of its systems of records, the information is protected to the same extent as all other information in the system. The protections include physical access controls, required background checks, and supervisor approval before being granted a user role, privacy and security training, and compliance with DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1).

## **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.*

***BTB Privacy Principle #6: Accountability*** - Canada and the U.S. affirm their accountability for compliance with their respective domestic law and rules on the protection of personal information.

***BTB Privacy Principle #7: Effective Oversight*** - A system of effective data protection supervision is to exist in the form of a public supervisory authority or authorities with effective powers of intervention and enforcement. These powers may be carried out by a specialized public information protection authority or by more than one supervisory public authority to meet the particular circumstances of different legal systems.

All authorized Canadian and U.S. users receive training about proper information handling procedures. These procedures include restrictions on individuals who are eligible to be queried, retention of information from a result, use limitations, information marking, and protecting the information. These users, in addition to having completed background checks and obtaining a supervisor's approval establishing an official need to know, have their queries and results audited using CLASS and GCMS audit logs. The Participants must review the



performance of the BVIIS program, including any privacy or security breaches as described in Section 6 above, and report the results to each other.

Further, in an effort to assist the U.S. with its audit requirements, Canada intends to provide, upon request from the U.S., a point-in-time snapshot containing the biographic data Canada sent in a query or biographic data sent in response to a U.S.-initiated query. The U.S. may request a point-in-time snapshot by providing Canada with the associated transactional information retained by the U.S. These occasional case-by-case requests are intended to support U.S. audit and accountability requirements.

In addition, as part of their review obligations, the Participants conduct quality assurance activities on a regular basis, including analysis and reporting on the volume of exchanges of biographic data breach or improper use or disclosure of biographic data. One year after the Arrangement goes into effect, and at regular intervals thereafter, the Participants assess their respective implementation of the privacy safeguards. The methodology for these assessments includes data analysis and a review of relevant documents. The Participants share with one another the results of these assessments.

## Conclusion

Through the BVIIS program, Canada and the U.S. have agreed to develop and implement a systematic, automated process for conducting immigration information exchanges. This will result in increased security, counter fraud, promote mobility, and improve efficiency within, at, and beyond our shared border.

## Responsible Officials

Mark Koumans  
Principal Deputy Assistant Secretary  
Office of International Affairs

## Approval Signature Page

Original signed and on file with the DHS Privacy Office.

---

Karen L. Neuman  
Chief Privacy Officer  
Department of Homeland Security



## **Appendix A-C**

**AGREEMENT**

**BETWEEN**

**THE GOVERNMENT OF CANADA**

**AND**

**THE GOVERNMENT OF THE UNITED STATES OF AMERICA**

**FOR THE SHARING OF VISA**

**AND IMMIGRATION INFORMATION**

**THE GOVERNMENT OF CANADA AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA** (hereinafter referred to as the “Parties”);

**NOTING** the importance of a new approach to migration that takes into account the global patterns of both regular and irregular migration and the increasingly sophisticated methods of identity fraud and abuse of their respective immigration laws;

**RECOGNIZING** that border security and border management are significantly enhanced by cooperation and collaboration;

**EMPHASIZING** that it is critically important to have timely access to current and accurate information to inform inadmissibility assessments or other immigration-related determinations that are vital to their common security;

**CONSIDERING** that the administration and enforcement of their respective immigration laws are important to protect the health and safety of their populations, to maintain the security of their societies, and to promote international justice and security by denying access to their territories to persons who are criminals or security risks;

**CONVINCED** that greater cooperation through the exchange of information can make their actions in achieving these objectives more effective;

**NOTING** the need to supplement existing information sharing arrangements between them, including the *Statement of Mutual Understanding on Information Sharing among the Department of Citizenship and Immigration (CIC) and the U.S. Immigration and Naturalization Service (INS) and the U.S. Department of State (DOS)*, 27 February 2003 (the “Statement of Mutual Understanding”) and the *Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims to the Statement of Mutual Understanding on Information Sharing between the Department of Citizenship and Immigration Canada (CIC) and the Bureau of Citizenship and Immigration Services (BCIS), of the U.S. Department of Homeland Security (DHS)*, 22 August 2003 (the “Asylum Annex”);

**RECOGNIZING** the need to establish a mechanism to exchange Information in a manner that respects privacy, civil liberties, and human rights; and,

**COMMITTED** to advancing their shared vision, as expressed in *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, a joint declaration issued by the Prime Minister of Canada and the President of the United States on 4 February 2011 and in *Beyond the Border Action Plan: Statement of Privacy Principles by the United States and Canada*, issued by Canada and the United States on 30 May 2012;

**HAVE AGREED** as follows:

## **ARTICLE 1**

### **Definitions**

For purposes of this Agreement,

- (a) “**National of a Third Country**” means a person who is not a citizen of Canada or a permanent resident of Canada or a citizen or national of the United States of America (the “United States”) or a lawful permanent resident of the United States, and includes a person not having a country of nationality.

- (b) “**Query**” means an electronic search process, requiring minimal human intervention, initiated by a Party under the authority of, and for the purposes delineated in, this Agreement, resulting in the exchange of data limited to the data described in the relevant non-legally binding implementing arrangement.
- (c) “**Information**” means biographic or biometric data on Nationals of a Third Country seeking authorization to travel, work, or live in Canada or the United States, and other immigration-related data about Nationals of a Third Country, including data from admissibility decisions rendered in accordance with the respective immigration laws of the Parties. For Queries on Refugee Status Claimants, Information is limited to data related to a visa application and excludes data otherwise provided under the Asylum Annex.
- (d) “**Refugee Status Claimant**” means any person who, in the territory or at a port of entry of one of the Parties, makes a claim for protection against persecution consistent with the *Convention relating to the Status of Refugees*, done on 28 July 1951 (the “1951 Refugee Convention”) or the *Protocol relating to the Status of Refugees*, done on 31 January 1967 (the “1967 Protocol”), or who has made a claim for protection against torture in accordance with the *Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment*, done on 10 December 1984 (the “Convention against Torture”), or has made a claim for protection on similar grounds in accordance with the Parties’ respective domestic law.

## ARTICLE 2

### Scope and Purpose

1. This Agreement specifies the terms, relationships, responsibilities and conditions for the sharing of Information between the Parties that occurs by means of a Query and in accordance with the Parties' respective domestic law.

2. The purpose of this Agreement is to assist in the administration and enforcement of the Parties' respective immigration laws by:

- using Information in order to enforce or administer the immigration laws of the Parties;
- furthering the prevention, investigation, or punishment of acts that would constitute a crime rendering a National of a Third Country inadmissible or removable under the immigration laws of the Party providing the Information; or
- facilitating the Parties' adjudication of an application for a visa, admission, or other immigration benefit, or determination of whether an individual is to be ordered removed by providing Information regarding the admissibility of the individual.

3. The Parties shall handle all Information exchanged under this Agreement in accordance with the terms of this Agreement, and their respective international legal obligations and domestic law.

4. This Agreement is solely intended to facilitate the sharing of Information between the Parties. The provisions of this Agreement shall not give rise to a right on the part of a private party, including to obtain, suppress, exclude or impede the sharing of any Information that is the subject of this Agreement.

### **ARTICLE 3**

#### **Exchange of Information and Implementation**

1. The Parties shall develop, by mutual consent, non-legally binding implementing arrangements under this Agreement that are consistent with their respective international legal obligations and domestic law.
2. The non-legally binding implementing arrangements shall set forth the data to be exchanged within each category of Information, the operational procedures to be followed, and the security mechanisms and other safeguards to be maintained.
3. The Parties shall provide each other with Query access to the data described in the non-legally binding implementing arrangements.

## **ARTICLE 4**

### **Use and Disclosure of Information**

1. The Parties shall hold Information exchanged under this Agreement in strict confidence and, shall use it only for purposes identified in Article 2, paragraph 2. The Parties agree to protect exchanged Information, and limit its use and subsequent disclosure, in accordance with this Agreement.
2. The Parties shall not interpret this article to preclude the use or disclosure of Information if their respective domestic law requires that use or disclosure in an immigration proceeding.
3. The Parties shall not interpret this article to preclude the use or disclosure of Information if their respective domestic law requires that use or disclosure in a criminal prosecution, or if obligated by the relevant Party's domestic law, in response to a written request from a body with jurisdiction to compel the production of Information. In these circumstances, the Party requiring such use or disclosure shall notify the other Party in advance and provide details of that use or disclosure. In the exceptional case where advance notice is not practicable, the Party using or disclosing the Information shall notify the other Party as soon as possible.

4. A Party may disclose Information exchanged under this Agreement with the express consent, in writing, of the Party providing the Information, subject to any caveats, restrictions or conditions imposed by the Party providing the Information, to:

(a) a domestic court or in a domestic judicial proceeding, for the purposes identified in Article 2, paragraph 2; or

(b) a government of a third country, for the purposes of verifying identity or establishing the provenance of identity documents, in connection with re-documentation or return of an individual to that country. However, the Parties shall make best efforts to ensure that the exchange, use or disclosure of Information:

(i) could not cause the Information to become known to any government, authority or person of a third country from which the subject of the Information is seeking or has been granted protection under the 1951 Refugee Convention, the 1967 Protocol, the Convention against Torture, or under either Party's domestic laws implementing the relevant Conventions or Protocol;

(ii) does not occur in circumstances where, by virtue of that government, authority or person becoming aware of such Information, the subject of the Information may become eligible for the protections set out in paragraph 4(b)(i) above;

(iii) does not occur if, as a result of such exchange, use or disclosure, the subject of the Information or their family members could be placed at risk of refoulement, or another type of harm contemplated under the 1951 Convention, the 1967 Protocol, or the Convention against Torture.

5. In order to prevent the unauthorized disclosure, copying, use, or modification of Information exchanged under this Agreement, each Party shall restrict access to that Information to its government agencies and individuals authorized to be responsible for pursuing the purposes set out in Article 2, paragraph 2. Each Party shall use recognized security mechanisms such as passwords, encryption, or other reasonable safeguards to prevent unauthorized access.

6. Each Party shall promptly notify, by telephone or in writing (including electronic mail), the other Party, within 48 hours after becoming aware of any accidental or unauthorized access, use, disclosure, modification or disposal of Information exchanged under this Agreement and shall furnish necessary details of the accidental or unauthorized access, use, disclosure, modification or disposal of that Information.

7. Each Party shall promptly notify, by telephone or in writing (including electronic mail), the other Party, within 24 hours where practicable, if there is a situation that disrupts the intended transfer of Information between the Parties.

## **ARTICLE 5**

### **Access, Correction and Notation**

To the extent specified in their respective domestic law, the Parties shall provide persons who are the subject of Information exchanged under this Agreement with opportunities to request access to the Information, to correct erroneous Information or to request to add a notation to indicate a correction request was made.

## **ARTICLE 6**

### **Accuracy of Information**

1. Each Party shall provide the other Party with access to the most current and accurate Information available in its databases.

2. In the event that a Party has reason to believe that the other Party is using or relying on inaccurate Information exchanged under this Agreement, it shall promptly notify the other Party, in writing and provide correcting Information, if it is available.

3. When a Party receives correcting Information, the Party shall destroy or correct any inaccurate Information and any Information derived from it. The Party shall notify the other Party, in writing, that it has made the corrections.

## **ARTICLE 7**

### **Retention and Disposition**

1. Each Party shall retain Information exchanged under this Agreement in accordance with the terms of this Agreement and its domestic law. Each Party shall maintain a system of database and document control that provides for the orderly disposition of Information exchanged under this Agreement.

2. A Party shall destroy, as soon as practicable, any data exchanged pursuant to a Query that it determines is not relevant to that Query or was erroneously provided.

## **ARTICLE 8**

### **Security and National Interest Exemptions**

If a Party determines that sharing Information under this Agreement would be inconsistent with its domestic law, or detrimental to its national sovereignty, national security, public policy, or other important national interest, the Party may decline to provide all or part of the Information,

or offer to provide all or part of the Information subject to such terms and conditions as it may specify.

## **ARTICLE 9**

### **Requests for Additional Data**

If, based on access to Information provided under Article 3, a Party has reason to request additional data not covered by this Agreement and its non-legally binding implementing arrangements, such request should be governed by applicable laws, regulations, arrangements, or agreements.

## **ARTICLE 10**

### **Review and Consultation**

1. The Parties shall designate points of contact, and require them to consult regularly to promote the effective implementation and administration of this Agreement.
2. The Parties shall, through their points of contact, jointly review this Agreement. The first review shall take place not earlier than one year from the date of the entry into force of this Agreement, and as the Parties mutually decide thereafter.
3. A Party shall advise the other Party of changes to its laws, regulations, policies, technology, or systems that may affect the implementation or administration of this Agreement.

## **ARTICLE 11**

### **Settlement of Disputes**

1. The Parties shall at all times endeavour to agree on the interpretation and application of this Agreement, and shall make every attempt to arrive at a mutually satisfactory resolution of any matter that might affect its implementation or administration.

2. If the Parties cannot, through discussions, arrive at a mutually satisfactory resolution of a dispute regarding the interpretation or application of this Agreement, they shall resolve the dispute through diplomatic channels.

## **ARTICLE 12**

### **Amendment and Termination**

1. The Parties may amend this Agreement by mutual consent, in writing.

2. A Party may terminate this Agreement at any time by giving notice in writing to the other Party. The termination is effective six months after receipt of the notice. Articles 4, 5, 6 and 7 shall continue to apply to Information exchanged under this Agreement, even after the Agreement is terminated.

## **ARTICLE 13**

### **Entry into Force**

This Agreement shall enter into force on the date of the last note in an exchange of diplomatic notes in which the Parties notify each other of the completion of their respective internal procedures necessary for the entry into force of this Agreement.

**IN WITNESS WHEREOF**, the undersigned, being duly authorized by their respective governments, have signed this Agreement.

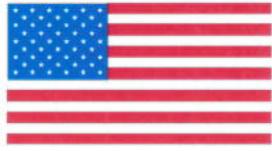
**DONE** at \_\_\_\_\_, this \_\_\_\_\_ day of \_\_\_\_\_ 2012, in  
duplicate in the English and French languages, each text being equally authentic.

---

**FOR THE GOVERNMENT  
OF CANADA**

---

**FOR THE GOVERNMENT  
OF THE UNITED STATES  
OF AMERICA**



**IMPLEMENTING ARRANGEMENT BETWEEN  
THE DEPARTMENT OF STATE AND THE DEPARTMENT OF HOMELAND SECURITY  
OF THE UNITED STATES OF AMERICA,  
AND  
THE DEPARTMENT OF CITIZENSHIP AND IMMIGRATION OF CANADA  
AND THE CANADA BORDER SERVICES AGENCY  
CONCERNING BIOGRAPHIC VISA AND IMMIGRATION INFORMATION SHARING**

**THE DEPARTMENT OF STATE (DOS) AND THE DEPARTMENT OF HOMELAND SECURITY (DHS) OF THE UNITED STATES OF AMERICA, AND THE DEPARTMENT OF CITIZENSHIP AND IMMIGRATION OF CANADA (CIC) AND THE CANADA BORDER SERVICES AGENCY (CBSA), hereinafter referred to as the “Participants”,**

*CONSIDERING the Agreement between the Government of the United States of America and the Government of Canada for the Sharing of Visa and Immigration Information, (“the Agreement”) done at Ottawa, on December 13, 2012;*

**CONSIDERING** that the Government of the United States of America and the Government of Canada are Parties to the Agreement, which provides in Article 3 for the development of implementing arrangements; and

**CONSIDERING** that the DoS and DHS are the departments responsible for the administration and enforcement of immigration laws for the United States and that CIC and CBSA are the department and agency responsible for the administration and enforcement of immigration laws for Canada;

**HAVE COME** to the following understanding:

**DEFINITIONS**

1. The Participants understand that:
  - (i) The definitions in the Agreement are incorporated by reference within this Implementing Arrangement.
  - (ii) “Biographic Data” refers to personal information, as detailed in paragraphs 6 and 9 herein.

**PURPOSE**

2. Consistent with Article 2 of the Agreement, the Participants intend to exchange Biographic Data, consistent with the laws of their respective countries, to assist in the effective administration and enforcement of the immigration laws of their respective countries.

### SCOPE AND PROCESS FOR THE EXCHANGE OF INFORMATION

3. The Participants intend to send to each other Queries on persons believed to be Nationals of a Third Country who have applied for admission, a visa or other immigration benefit, or who are the subjects of an investigation, to determine their admissibility, eligibility for a visa or other immigration benefit, or eligibility to remain in either of the territory of their respective countries.
4. The Participants do not intend to send Queries relating to:
  - (i) Persons identified on the basis of such data as application responses, identity documentation provided, or the nature of the application or investigation as:
    - (A) A citizen of Canada, or a citizen or national of the United States;
    - (B) For Canadian Queries, a Permanent Resident of Canada; or
    - (C) For U.S. Queries, a Lawful Permanent Resident of the United States.
  - (ii) Their respective Refugee Status Claimants at the time of application for protection; or
  - (iii) Categories of persons where such Queries are inconsistent with the laws of their respective countries, or detrimental to the national sovereignty, national security, public policy, or other important national interest of their respective countries, consistent with Article 8 of the Agreement. For the United States Participants, this includes applicants for and beneficiaries of applications under U.S. law for T or U non-immigrant status or *Violence Against Women Act* relief.
5. The Participants intend to mutually establish the estimated annual volume of Queries for the management of this Implementing Arrangement.
6. The Participants intend to include in each Query, where available, the following Biographic Data:
  - (i) Last name;
  - (ii) First name;
  - (iii) Alias last name(s);
  - (iv) Alias first name(s);
  - (v) Date of birth;
  - (vi) Country of birth;
  - (vii) Passport nationality (given nationality if passport not available);
  - (viii) Gender;

- (ix) Travel document number; and
  - (x) Travel document issuing authority or country.
7. Subject to paragraph 8, the Participants intend to respond to a Query only if a potential match:
- (i) Is believed, on the basis of data available to the Participant, to be a National of a Third Country; and
  - (ii) Is identified based on mutually determined criteria that ensure a high degree of certainty in the accuracy of potential matches; and
  - (iii) Has one or more of the following:
    - (A) A previous decision or determination where the person failed to meet the requirements, including admissibility or eligibility requirements, of the immigration law of their respective countries; or
    - (B) Other derogatory data related to the person that is relevant to administering or enforcing the immigration law of their respective countries.
8. If a Participant determines that sharing Biographic Data is inconsistent with the laws of its country, or detrimental to its national sovereignty, national security, public policy, or other important national interest, the Participant may decline to provide any such Biographic Data, or offer to provide all or part of the Biographic Data subject to terms and conditions as it may specify. For the United States Participants, this includes applicants for or beneficiaries of applications under U.S. law for T or U non-immigrant status or *Violence Against Women Act* relief.
9. When the requirements of paragraph 7 have been met, and subject to paragraph 8, the Participants intend to send, in response to a Query, the following Biographic Data, where available:
- (i) Last name;
  - (ii) First name;
  - (iii) Alias last name(s);
  - (iv) Alias first name(s);
  - (v) Date of birth;
  - (vi) Alias date(s) of birth;
  - (vii) Country of birth;
  - (viii) Alias country(ies) of birth;
  - (ix) Passport nationality (given nationality if passport not available);

- (x) Gender;
- (xi) Travel document number;
- (xii) Travel document issuing authority or country;
- (xiii) Date of outcome of application, encounter or record;
- (xiv) Place of refusal;
- (xv) Date of application, encounter or record;
- (xvi) Type of application, encounter or record;
- (xvii) Date of Entry;
- (xviii) Port of Entry;
- (xix) Indicator of the derogatory data;
- (xx) Date removal order enforced; and
- (xxi) Current immigration status.

- 10.** The Participants only intend to disclose Biographic Data received under this Implementing Arrangement to other entities of their respective governments consistent with the Agreement and in accordance with the laws of their respective countries.

#### **POINTS OF CONTACT**

- 11.** The Participants designate the following as their Points of Contact for the implementation and administration of this Implementing Arrangement:
- (i) For CIC: Director General, Operational Management and Coordination, Operations Sector;
  - (ii) For CBSA: Director General, People Projects Directorate, Information, Science & Technology Branch;
  - (iii) For DoS: Managing Director, Visa Services, Bureau of Consular Affairs; and
  - (iv) For DHS: Deputy Assistant Secretary, Office of International Affairs.

#### **PRIVACY SAFEGUARDS**

- 12.** The Participants intend to collect, use and disclose any Biographic Data exchanged pursuant to this Implementing Arrangement in a manner consistent with the Agreement, the laws of their respective countries, and the *Beyond the Border Action Plan: Statement of Privacy Principles by the United States and Canada*, issued by Canada and the United States on May 30, 2012.

13. The Participants intend, to the extent specified in the laws or policies of their respective countries, to provide persons subject of Biographic Data exchanged under this Implementing Arrangement with opportunities to request access to their Biographic Data, to correct their erroneous Biographic Data, or to request to add a notation to indicate a correction was made to their Biographic Data. The Participants intend to notify each other of their respective mechanisms for providing such opportunities.
14. The Participants intend to protect the exchange of Biographic Data by mutually decided upon technical and physical safeguards.
15. The Participants intend to protect Biographic Data with appropriate administrative, technical, and physical safeguards and only disclose it to authorized individuals who have the appropriate security clearance, when required, and a need to know and only for uses that are consistent with the stated purposes of the Agreement and for which the Biographic Data was originally collected, or as otherwise required by the laws of their respective countries.
16. The Participants intend to mark Biographic Data exchanged as having been received from the other Participant.
17. The Participants understand that Biographic Data obtained as part of a Query and in response to a Query are retained only so long as necessary for the specific purpose for which the Biographic Data was provided, in accordance with the Participants' respective applicable retention and disposition schedules, and in accordance with the laws of their respective countries.
18. The Participants intend to immediately destroy all Biographic Data obtained as part of a Query determined not to relate to the person who is the subject of the Query in accordance with Article 7 of the Agreement. This includes:
  - (i) The providing Participant destroying the Biographic Data obtained from the requesting Participant through the Query; and
  - (ii) The requesting Participant destroying any Biographic Data received in response to a Query that is determined by the requesting Participant as not relating to the subject of the Query.

#### **REVIEW AND PERFORMANCE MONITORING**

19. For purposes of the review process described in Article 10 of the Agreement, the Participants intend to review on an annual basis the volume of transactions and the outcomes and the timeliness of the responses to Queries based on mutually decided performance and management measurements, which may include, but are not limited to:
  - (i) The number of exchanges from which Biographic Data was provided to visa, immigration and border-control decision makers before they made a decision;

- (ii) The number and severity of any security or privacy breaches of the information sharing system, databases, or personal information exchanged under this Implementing Arrangement as well as a summary of remedial actions taken; and
  - (iii) Each Participant's timeliness in responding to Queries.
- 20. The Participants intend to carry out regular quality assurance activities, including a review of applicable privacy safeguards, using a mutually decided methodology to ensure that the activities carried out under this Implementing Arrangement are consistent with the principles outlined by this Implementing Arrangement. These quality assurance activities may include, but are not limited to determining:
  - (i) Whether Biographic Data has been retained when it should have been destroyed;
  - (ii) Whether Biographic Data exchanged under this Implementing Arrangement has been marked as having been received from the other Participant; and
  - (iii) Whether Biographic Data has been disclosed in a manner inconsistent with Article 4 of the Agreement.

#### **MATERIAL CHANGES**

- 21. The Participants intend to inform each other of any changes to the technical systems, laws, policies or international obligations of their respective countries that may materially affect the operation or implementation of this Implementing Arrangement.

#### **COSTS**

- 22. The Participants understand that performance of this Implementing Arrangement is subject to their respective availability of funds. Each Participant intends to pay for its own costs and use its own equipment and personnel in performing its activities under this Implementing Arrangement. No provision in this Implementing Arrangement is intended to be interpreted to require the obligation or payment of funds in violation of the laws of the Participants' respective countries.

#### **CONSULTATIONS**

- 23. The Participants intend to resolve any difference in the interpretation, application or implementation of this Implementing Arrangement by mutual consultation.

**FINAL PROVISIONS**

- 24. Participation under this Implementing Arrangement is intended to commence on the date when it has been signed by all Participants.
- 25. The Participants may modify this Implementing Arrangement by mutual consent in writing.
- 26. The Participants of one country may cease participation in this Implementing Arrangement by giving written notice to the Participants of the other country. Consistent with Article 12 of the Agreement, cessation of participation becomes effective six months after receipt of such notice. In such event, the provisions of paragraphs 12 to 18 continue to apply to Biographic Data exchanged pursuant to this Implementing Arrangement.

SIGNED, in quadruplicate, in the English and French languages.

**FOR THE DEPARTMENT OF STATE  
OF THE UNITED STATES OF AMERICA**

**FOR THE DEPARTMENT OF CITIZENSHIP  
AND IMMIGRATION OF CANADA**

Michele T Bond

Anita Biggs

At: Washington DC

At: Ottawa, ont

Date: 12-05-2013

Date: 2013-12-02

**FOR THE DEPARTMENT  
OF HOMELAND SECURITY  
OF THE UNITED STATES OF AMERICA**

**FOR THE CANADA BORDER  
SERVICES AGENCY**

Alan Bessin

[Signature]

At: Washington DC

At: Ottawa, ont

Date: 12-12-2013

Date: 2013-11-29



## BEYOND THE BORDER ACTION PLAN **Statement of Privacy Principles by the United States and Canada**

May 30, 2012

*Recognizing* that greater information sharing between Canada and the United States is vital to protecting the security of our citizens and that our countries have a long history of sharing personal information responsibly and respecting our separate Constitutional and legal frameworks that protect privacy,

*Recognizing* that Canada and the United States are committed to protecting privacy in all Beyond the Border (BTB) arrangements and initiatives undertaken by our two countries and specifically to stating the privacy protection principles that are to inform and guide all BTB information sharing arrangements and initiatives,

*Noting* that the implementation of these Principles may be tailored to the specific context of particular BTB arrangements and initiatives, but always in a manner consistent with the Principles,

*Recognizing* that any exceptions from principles that may be required in the context of particular BTB arrangements for law enforcement and national security purposes will be as few as possible, made known to both the United States and Canada and the public, and consistent with domestic law, and

*Recognizing* that personal information is to be provided, received and used only in accordance with domestic and international law applicable to the United States and Canada.

The United States and Canada set forth the following Statement of Privacy Principles concerning the provision, receipt and use of personal information exchanged by the United States and Canada pursuant to any BTB information sharing arrangements and initiatives:

### **1. Purpose Specification**

The purposes for which personal information is provided, received and used are to be specified in any BTB arrangements or initiatives and such personal information is to be subsequently used in furtherance of the fulfillment of those purposes or such other lawful purposes as are not incompatible with those purposes and are specified either in the relevant BTB arrangement or initiative or in a notice to the public and to the other participant in the relevant BTB arrangement or initiative.

**2. Relevant and Necessary/Proportionate**

Personal information is to be provided, received and used to the extent it is relevant, necessary and appropriate to accomplish a clear purpose set out in any BTB arrangements or initiatives.

**3. Integrity/Data Quality**

Canada and the United States are to make reasonable and appropriate efforts to maintain personal information accurately and completely, including any caveats or conditions attached to the information. Any further related information, including updates or clarifying information, is to be included to ensure continuing accuracy and completeness.

**4. Non-Discrimination**

Canada and the United States are to apply this Statement of Privacy Principles to all individuals on an equal basis without unlawful discrimination.

**5. Information Security**

Personal information is to be protected 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. Only authorized individuals with an identified purpose are to have access to personal information.

**6. Accountability**

Canada and the United States affirm their accountability for compliance with their respective domestic law and rules on the protection of personal information.

**7. Effective Oversight**

A system of effective data protection supervision is to exist in the form of a public supervisory authority or authorities with effective powers of intervention and enforcement. These powers may be carried out by a specialized public information protection authority or by more than one supervisory public authority to meet the particular circumstances of different legal systems.

**8. Individual Access and Rectification**

The United States and Canada are to provide individuals with access to and the means to seek rectification and/or expungement of their personal information. Should access to personal information need to be limited, the specific grounds for any restrictions are to be specified consistent with domestic law. In appropriate cases, an individual may object to the provision, receipt and use of personal information related to him or her.

**9. Transparency and Notice**

The United States and Canada are to provide individuals, as required by law, with general and, as appropriate, individual notice, at least as to the purpose of the provision, receipt and use of personal information that concerns the individual, the identity of the entity controlling that information, the applicable rules or laws, the types of third parties to whom information

may be subsequently disclosed, as well as other information insofar as is necessary to seek effective sanctions and/or remedies.

Should notice need to be limited for national security or law enforcement reasons, such as the protection of an ongoing investigation or the protection of victims or witnesses, the limitation on notice should be consistent with domestic law.

#### **10. Redress**

The United States and Canada are to provide, consistent with their respective domestic law, effective remedies before a fair and objective authority where a person's privacy has been infringed or where there has been a violation of data protection rules with respect to that individual. Any such infringement or violation is to be subject to appropriate and effective sanctions and/or remedies. Redress may not be available for frivolous claims or where there has been no material infringement of a person's privacy.

#### **11. Restrictions on Onward Transfers to Third Countries**

Where personal information is provided, in accordance with relevant domestic law, by a competent authority of the United States or Canada (the originating country) to a competent authority of the other nation (the receiving country), the competent authority of the receiving country is to authorize or carry out an onward transfer of this information to a third country only if consistent with the domestic law of the receiving country, and in accordance with existing applicable international agreements and arrangements.

In the absence of such international agreements and arrangements, the receiving country may transfer the personal information to a third country when consistent with the domestic law of the receiving country, in which case the originating country is to be notified:

- i. prior to the transfer; or
- ii. as soon as reasonably possible after the transfer in the case of exigent circumstances.

#### **12. Retention**

The United States and Canada are to retain personal information only so long as necessary for the specific purpose for which the information was provided or further used, and in accordance with their respective domestic laws.

Nothing in this Statement of Privacy Principles is intended to give rise to rights or obligations under domestic or international law. This Statement of Privacy Principles is not intended to constitute a treaty or other binding agreement under international law.

Canada and the United States intend to consult each other as necessary, including through the Executive Steering Committee, on the application of this Statement of Privacy Principles to particular Beyond the Border arrangements and initiatives, and to discuss more general developments in the protection of privacy rights.