Appendix: A

Organization:

U.S. Department of State, Bureau of Consular Affairs (DoS/CA)

Purpose and Use:

The sharing between DoS/CA and US-VISIT supports the visa application and issuance process for aliens seeking to enter the United States.

DoS/CA consular officers working at DoS posts collect fingerprints from visa applicants and input them into the DoS Consular Consolidated Database (CCD) system. CCD is the DoS/CA gateway to IDENT.

DoS shares with US-VISIT biometrics, certain biographic data elements, and visa issuance or refusal data from visa applicants. US-VISIT then runs searches in the IDENT database and returns search results. DoS returns information regarding visa issuance or serious refusal of visas after a visa has been issued or denied.

Individuals Impacted:

The sharing between DoS/CA and US-VISIT impacts any individual who applies for a U.S. visa with DoS.

Data Elements:

DoS/CA searches and enrolls data it collects directly from visa applicants. The information returned from IDENT assists in determining identity and visa eligibility. IDENT also sends wrap-back notifications as described in the PIA overview. If visas are denied for a derogatory reason, DoS/CA transmits the relevant derogatory information for storage in IDENT. If visas are revoked for serious reasons, DoS/CA transmits the notice of revocation for storage in IDENT. These denial and revocation encounters are also added to the IDENT watchlist.

DoS/CA submits the following data elements:

Biometric data: finger scans and digital facial photographs

Encounter data: Place and date of issuance

Biographic data: name, date of birth, gender, physical details, and visa issuance or visa refusal data.

DoS/CA receives the following data elements from IDENT:

Biometric data: digital facial photograph

Biographic data: (1) full name (i.e., first, middle, last, nicknames, and aliases), date of birth, gender, signature; personal identifiers including Alien Registration Number, Social Security

number (when provided), state identification number, civil record number, Federal Bureau of Investigation Fingerprint Number, Fingerprint Identification Number, National Unique Identification Number; and personal physical details, such as height, weight, eye color, and hair color; (2) identifiers for citizenship and nationality, including person-centric details, such as country of birth, country of citizenship, and nationality; (3) derogatory information,[1] if applicable, including wants and warrants, KSTs, sexual offender registration, and immigration violations; (4) IDENT watchlist status information; (5) miscellaneous officer comment information; (6) document information and identifiers (e.g., passport and visa data; document type; document number, and country of issuance); and (7) current and historic whereabouts.

Encounter data: transaction identifier data, such as sending organization; timestamp; workstation; reason fingerprinted, such as entry, visa application, credentialing application, or apprehension; and any available encounter information, including an IDENT-generated encounter identification number (EID).

Applicable IDENT SORN Routine Uses:

The sharing between DoS/CA and US-VISIT is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice:

The DoS Consular Consolidated Database (CCD) PIA is available on the DoS website at http://www.state.gov/documents/organization/93772.pdf . The DoS Visa Records SORN, available at http://www.state.gov/documents/organization/102815.pdf, covers the data in CCD.

Retention by Partner:

DoS/CA retains all data received from IDENT.

Compliance Reporting:

Section 8 of the IDENT PIA covers US-VISIT compliance reporting. The MOU between DHS and DoS did not establish any additional compliance-reporting requirements.

Onward Transfer:

The DoS-DHS MOU limits access to DoS personnel who have a need to know to carry out their official duties and establishes that data may not be disseminated outside DoS without the expressed consent of DHS.

[1] A set of data related to negative or criminal information associated with an encounter.

Training:

US-VISIT is currently developing an on-boarding package for distribution to all IDENT users. The package covers privacy compliance, as well as the relevant terms of any relevant MOU.

Correction and Redress:

Legitimate travelers can submit concerns to and seek relief from DoS/CA regarding screening-related difficulties they may have experienced during travel to or from the United States by filing a complaint online at www.dhs.gov/trip and tracking their status using the control number assigned to the query. Redress is additionally available under the DoS Visa Records SORN, available at http://www.state.gov/documents/organization/102815.pdf.

Appendix: B

Organizations:

The Five Country Conference (FCC) is a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States (collectively called the FCC partners).

Purpose and Use:

The purpose of this information sharing is to support immigration processes, including asylum, visa, and refugee determinations, as well as admissibility, among the FCC partners. Foreign partners perform a search only; no data is enrolled in IDENT.

FCC countries use information shared through the FCC project for immigration and border management, national security, and law enforcement purposes in that country only.

FCC partners exchange their biometric data to search against the existing biometric holdings of other FCC partners to determine whether information pertinent to immigration and border management exists.

Individuals Impacted:

Individuals impacted include those encountered in the following immigration situations in an FCC partner country:

- Where there is an indication of derogatory activity (e.g., child smuggling) or other associations of concern such that the individual could be found inadmissible to one or more of the FCC partner countries.
- Where the identity of the individual is unknown (e.g., an individual who has destroyed his or her identifying documents or withheld information about his or her identity to prevent removal).
- Where there is reason to believe that another FCC partner has encountered the individual.
- Where there is an asylum claim that involves identifying individual(s) encountered inside the FCC partner country, or locating individuals whose whereabouts are unknown or who may have violated immigration or criminal laws.
- Where an individual requires re-documentation for removal or another immigration-related process.

Data Elements:

Shared information may include personal information relating to nationals of a FCC country that is deemed relevant and necessary for immigration or nationality determination purposes, as defined in the MOU. Shared information may include:

Biometric data: digital facial photographs and fingerprints.

Biographic data: full name, date of birth, place of birth, citizenship, document identifier (e.g., document type, document number, and country of issuance), current and historic whereabouts, gender, date fingerprinted, reason fingerprinted, location fingerprinted, and aliases.

In the event of an information match, two FCC partners (the requesting and providing countries) may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

Sharing among FCC partners is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice:

The following FCC partner countries have provided notice by posting PIAs on this data exchange:

- Canada: http://www.cic.gc.ca/english/department/atip/pia-fcc.asp.
- UK: http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/pia.pdf?view=Binary.
- New Zealand: http://www.immigration.govt.nz/NR/rdonlyres/06901144-1618-4523-A5B9-340697315688/0/PrivacyImpactAssmt.pdf.
- Australia: Australia conducts PIAs, but does not publicly post those documents.

Retention by Partner:

In general, all shared biometric information is destroyed securely as soon as the receiving country completes searching (whether or not a match is achieved). Shared biometric information is not used for any other purpose. When there is a legitimate purpose connected with a match and

the information is still relevant, an FCC partner may store, process, and transmit further biometric and biographical information, in accordance with applicable laws and established information retention policies. When or if the case file includes shared information (either electronic or paper) for the individual to whom the data relates, that information may be retained as part of that case file in accordance with the domestic laws and data retention policies of the receiving country.

Compliance Reporting:

Any country may request assurance from another country that satisfactory safeguards are being maintained with respect to the information shared. This may include an audit of the safeguards, by an appropriate internal or external auditor with agreed terms of reference between the countries. The countries will also produce comprehensive, joint performance and management information about the operation of the protocol, which will explicitly identify the number and severity of any security or privacy breaches and remedial actions taken.

Onward Transfer:

Information received by any FCC partner is limited to use for determining the handling of an immigration case in that country only. FCC partners do not share information exchanged under this protocol with non-FCC partners without the permission of the FCC partner(s) that originally provided the information. For search requests resulting in matches against two or more countries, information may only be exchanged initially on a bilateral basis; however, the requesting country may inform each providing country about the existence of another matching record and the identity of the other FCC partner(s) with a matched record.

Training:

Privacy training for FCC partner participants complies with the appropriate training requirements defined by each FCC partner. All FCC Partner countries require that their employees complete Privacy and Security training.

Correction and Redress:

If an individual believes that the information held on him/her is incorrect, he or she may submit an inquiry to the following points of contact in each country;

- Australia: DIAC, Minister for Immigration and Citizenship, Local Member of Parliament, Commonwealth Ombudsman or the Australian Privacy Commissioner.
- New Zealand: A person may seek redress from one or all of the following: Immigration NZ, Minister of Immigration, Ombudsman or directly to the NZ Privacy Commissioner.
- UK: If the negative decision attracts a right of appeal, the appeal must be lodged with whichever part of U.K. Border Agency (UKBA) made the decision (for example, asylum for asylum cases, or the overseas visa hub for visa applications). If the person wants to simply know what information UKBA holds about them on its systems, they can make a

request to the Subject Access Bureau at http://www.ukba.homeoffice.gov.uk/navigation/personal-data/.

- Canada: For access to personal information held by Citizenship and Immigration Canada please refer to their website at: http://www.cic.gc.ca/english/department/atip/requests-personal.asp.

Appendix B-1

U.S. Canada Biometric Visa and Immigration Information Sharing

Background

On February 4, 2011, the Prime Minister of Canada and the President of the United States issued a joint statement: "Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness."[2] The declaration established a new long-term partnership to work together to increase security, counter fraud, promote mobility, and improve efficiency within, at, and beyond our shared border. On December 7, 2011, the Canada-U.S. Beyond the Border Perimeter Security and Economic Competitiveness Action Plan ("Action Plan")[3] established a common approach to perimeter screening to promote security and border efficiency as one of its priorities. The two countries committed to screening travelers seeking to enter either country in order to:

- Identify individuals who seek to enter the perimeter for *mala fide* purposes;
- Prevent individuals from assuming different identities within each country;
- Identify individuals who have committed serious crimes or violated immigration law in the other country to enable informed decisions; and
- Create a shared responsibility concerning those entering the Canada-United States perimeter, while facilitating on-going efforts to streamline procedures at the shared border.

Canada and the United States committed to develop and implement a systematic, automated process for conducting immigration information exchanges. 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* ("the Agreement"), which lays out mutual obligations for relevant biographic[4] and biometric-based information sharing.

In order to carry out the biometric information sharing called for in the Agreement, Canada and the United States ("the Participants") developed the *Implementing Arrangement between the*

---

[2] Declaration by President Obama and Prime Minister Harper of Canada -Beyond the Border (February 4, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord.

[3] United States-Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness (December 2011), included as an addendum to this Appendix (beginning on page 14), and *available at* http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf. "To preserve and extend the benefits our close relationship has helped bring to Americans and Canadians alike, we intend to pursue a perimeter approach to security, working together within, at, and away from the borders of our two countries to enhance our security and accelerate the legitimate flow of people, goods, and services between our two countries."

[4] *See* DHS/CBP/PIA-023 Biographic Visa and Immigration Information Sharing with Canada may be accessed at http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_biographicvisa_feb2014.pdf.

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 Biometric Visa and Immigration Information Sharing ("the Arrangement").[5] The Arrangement establishes guidelines for vetting biometrics associated with visa application and immigration matters against the other parties appropriate biometric repositories through automated processes. The implementation of biometric immigration information sharing (IIS) was developed to support the Action Plan and to assist in the effective administration and enforcement of the Participants' respective immigration laws. The outline below summarizes how Canada and the United States intend to achieve its high-level objectives:

- Expand existing biometric information sharing of asylum claimants, in a phased approach, with the goal of sharing 100% of this population;
- Expand biometric information sharing to include overseas refugees applying for resettlement to either country, in accordance with domestic and international obligations; and
- Implement a systematic and automated sharing capability to support admissibility screening of visa-required third-country nationals, and in support of other administrative and enforcement actions.

This sub-appendix to Appendix B provides public notice about information sharing under this program, and resulting privacy impacts. Information shared pursuant to the Agreement and its implementing arrangement falls under the scope of work for both the Five Country Conference and Beyond the Border Action Plan. As such, Canada and the United States incorporated the Beyond the Border Privacy Principles[6] into the Agreement and Arrangement to guide and inform sharing under this initiative. The Beyond the Border Privacy Principles are aligned with the *DHS Fair Information Practice Principles* (FIPPs). Information shared is consistent with the Participants' respective domestic laws and policies.

Overview of Sharing

The biometric visa and immigration information sharing initiative allows Canada and the United States to make electronic fingerprint queries against each other's fingerprint database(s). When a biometric match is made in the database, exchange and subsequent use of relevant information, listed below, may occur.

Organizations

For Canada:

[5] The Arrangement is also included as an addendum to this Appendix, following the Agreement.
[6] Beyond the Border Action Plan: Statement of Privacy Principles by the United States and Canada (May 30, 2012), *available at* http://www.dhs.gov/xlibrary/assets/policy/beyond-the-border-action-plan-statement-of-privacy-principles.pdf.

The Department of Citizenship and Immigration Canada

The Canada Border Services Agency

For the United States:

The U.S. Department of State

The U.S. Department of Homeland Security

Purpose and Use

The purpose of this initiative is to assist in the effective administration and enforcement of the Participants' respective immigration laws. Information exchanged under this initiative will be used to enforce or administer the Participant's respective immigration laws.

Individuals Impacted

The Participants will make queries on individuals whom the requesting Participant believes to be nationals of a third country, based on data such as application responses, identity documentation, or the nature of the application or investigation, and who have applied for admission or a visa or other immigration benefit. The Participants will query individuals believed to be third country nationals and who are a subject of an investigation in order to establish the basis for admissibility, eligibility for a visa or other immigration benefit, or their eligibility to remain in the territory of the requesting country.

Data Elements

The Participants intend to send, in response to a query, the following data elements when there is a biometric match, subject to availability and practicability in the providing Participant's applicable database or databases (for the United States, IDENT; for Canada, Global Case Management System (GCMS)):

(a) Providing Participant subject specific reference number;

(b) Providing Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Current immigration status;

(m) Other names;

(n) Alias last name(s);

(o) Alias first name(s);

(p) Travel document number;

(q) Travel document type;

(r) Travel document issuing authority/country;

(s) Travel document expiry date;

(t) Reason for alert;[7]

(u) Visa Refusal code;

(v) Watchlist Indicator;[8]

(w) Scan of travel document biodata page;

(x) Scan of other marked travel document pages;

(y) Facial image;

(z) Previous immigration status;

(aa) Date removed;

(bb) Date of arrival;

(cc) Location of arrival;

(dd) Date of departure;

(ee) Location of departure;

(ff) Date of immigration application or non-biometric encounter;

---

[7] Alerts are from the DHS enforcement process where a flag has been placed on a person primarily as a Recidivist. "Recidivist with alert" categories include categories for officer safety, smuggling, and individuals flagged for expedited removal.

[8] For purposes of this sharing, "watchlist indicator" is an indication of derogatory information held in IDENT. For a full description of the IDENT watchlist, please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012) at page 6, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf. Canadian responses to U.S. queries will not populate the "watchlist indicator" field because the Global Case Management System (GCMS) does not contain such holdings.

(gg) Type of immigration application or non-biometric encounter;

(hh) Date of outcome of immigration application;

(ii) Outcome of immigration application;

(jj) Reason for outcome of immigration application; and

(kk) Expiry date of current leave/stay or visa.

Following the receipt of a match response, the providing Participant may request that the requesting Participant provide the following data elements for the individual who was the subject of the initial query in order to support further domestic operations relevant to the original record.

(a) Requesting Participant subject specific reference number;

(b) Requesting Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Other names;

(m) Alias last name(s);

(n) Alias first name(s);

(o) Travel document number;

(p) Travel document type;

(q) Travel document issuing authority/country;

(r) Scan of travel document biodata page;

(s) Facial image;

(t) Current immigration status;

(u) Previous immigration status; and

(v) Date removed.

Applicable SORN Routine Uses

Biometrics/Biographic Information

DHS/USCIS-001 Alien File, Index, and National File Tracking SORN,[9]

> Routine Use H: To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws.

DHS/USCIS-003 Biometric Storage System SORN,[10]

> Routine Use F: 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

DHS/CBP-007 Border Crossing Information (BCI) SORN,[11] and

> Routine Use I: To the CBSA for law enforcement and immigration purposes, as well as to facilitate cross-border travel when an individual enters the United States from Canada.

DHS/CBP-006 Automated Targeting System (ATS) SORN[12] (*for legacy NSEERS data only*[13])

> Routine Use G: To appropriate federal, state, tribal, local, 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, or license, where CBP believes the information would assist enforcement of applicable civil or

---

[9] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, 78 FR 69864 (November 21, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-11-21/html/2013-27895.htm.
[10] DHS/USCIS-003 Biometric Storage System SORN, 72 FR 17172 (April 6, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-04-06/html/07-1643.htm.
[11] DHS/CBP-007 Border Crossing Information (BCI) SORN, 80 FR 26937 (May 11, 2015), *available at* http://www.regulations.gov/#!documentDetail;D=DHS_FRDOC_0001-1331.
[12] DHS/CBP-006 Automated Targeting System (ATS) SORN, 77 FR 30297 (May 22, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.
[13] NSEERS was first implemented in 2002 as a temporary measure in the aftermath of the September 11, 2001 terrorist attacks and was designed to record the arrival, stay, and departure of individuals from certain countries chosen based on an analysis of possible national security threats emanating from those locales. DHS officially ended the NSEERS program in 2011. DHS is sharing this information in the same manner as all other entry-exit information. Any match to individuals who were required to register under NSEERS should not be treated as derogatory information absent any other information. For additional information, please *see* http://www.dhs.gov/dhs-removes-designated-countries-nseers-registration-may-2011.

criminal laws.

Derogatory Information

DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) SORN,[14]

> Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens to other nations; and to international, foreign, and intergovernmental agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

DHS/CBP-011 - U.S. Customs and Border Protection (TECS) SORN[15]

> Routine Use G. 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.

Transactional Information

DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) SORN,[16]

> Routine Use A: To appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice

http://www.cic.gc.ca/english/DEPARTMENT/atip/pia/ist.asp.

Retention

The Participants intend to destroy the fingerprints submitted as part of a query. Response data, sent in the case of a fingerprint match, will be retained only so long as necessary for the purpose for which the data was provided, in accordance with the receiving Participant's respective applicable retention and disposition schedules and respective domestic laws.

United States: With this PIA update, the United States will also query Canada and intends to retain responses from Canada in IDENT consistent with DHS policies and retention schedules.

---

[14] DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) SORN, 80 FR 24269 (April 30, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-04-30/html/2015-09615.htm.
[15] DHS/CBP-011 TECS SORN, 73 FR 77778 (December 19, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.
[16] DHS/NPPD/USVISIT-004 Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm.

Canada: Citizenship and Immigration Canada (CIC) intends to retain information consistent with the departmental "Temporary & Permanent Migration Retention and Disposition Schedule." The Canada Border Services Agency (CBSA) intends to retain information consistent with the "Institution Specific Disposition Authority."

Review and Performance Monitoring

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:

- The number and severity of any security breaches and a summary of remedial actions taken.
- The number and severity of any privacy breaches and a summary of remedial actions taken.

The Participants intend to carry out regular quality assurance activities, including a review of applicable privacy safeguards. For Canada, quality assurance activities will be carried out by Citizenship and Immigration Canada's Centralized Information Sharing Unit (CISU). For the United States, quality assurance activities will be carried out by the Office of Biometric Identity Management. These activities may include, but are not limited to, determining:

- Whether information has been retained when it should have been destroyed.
- Whether information has been disclosed in a manner inconsistent with the Agreement.
- The number of correction requests and whether information has been corrected in a manner consistent with the Agreement.

Access, Correction, and Redress

Individuals who wish to access response data held by the Government of Canada may visit:

- CIC Website: http://www.cic.gc.ca/english/department/atip/requests-atip.asp.
- CBSA Website: http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/req-dem-info-eng.html for additional information on how to make an online or written request to access their personal information.

Individuals who wish to request access to response data held by the Government of the United States may contact:

U.S. Department of State:

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

U.S. Department of Homeland Security:
http://www.dhs.gov/freedom-information-act-and-privacy-act or
Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
245 Murray Lane SW, STOP-0655
Washington, D.C. 20528-0655

Individuals who wish to correct response 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, Ontario
K1A 1L1

or to:

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

Individuals who wish to correct response data held by the Government of the United States, or to request to add a notation to indicate a correction request was made, may submit a correction request to the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP):

http://www.dhs.gov/dhs-trip, or:
United States Department of Homeland Security
Traveler Redress Inquiry Program (DHS TRIP)
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

Correction requests, or requests to add a notation to indicate a correction request was made, may also be directed to:

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

The DHS Office of Citizenship and Immigration Services Ombudsman also assists individuals who wish to resolve issues regarding applications submitted 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
cisombudsman@dhs.gov

Privacy Risks and Mitigation

Information exchanged under this program will be done in accordance with the Participants' respective laws and policies, as well as the Beyond the Border Privacy Principles. In addition to risks and mitigations already addressed in the IDENT PIA[17], the following are specific risks associated with the biometric visa and immigration information sharing program:

Privacy Risk: 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.

Mitigation: The Participants intend to send queries only on individuals believed to be third country nationals based on data such as benefit application responses, identity documentation provided, or the nature of the benefit application of investigation. Unintentional sharing could happen if the individual withholds information from the providing Participant that indicates he or she is a citizen, resident, or national, as applicable, of the United States or Canada.

To mitigate this privacy risk:

- The providing Participant will not return information on individuals believed to be U.S. citizens, nationals, and LPRs, or Canadian citizens and permanent residents.
- DHS has limited the categories of information that it will return to only those that have been identified as unlikely to include U.S. citizens, nationals, and LPRs.
- These exchanges will undergo review and performance monitoring to ensure that information is exchanged in accordance with the Agreement. While these records may be shared on a case-by-case basis under the terms of the Statement of Mutual Understanding, DHS will review the responses it provides to Canadian queries and make adjustments as necessary to exclude any further exchanges of information likely to be out of scope of the Agreement.

Additional privacy risks first mentioned in the original IDENT PIA are particularly applicable to this information sharing initiative. There is a risk of sharing IDENT data with foreign partners, where it is more difficult for DHS to externally impose the same controls that govern the data internally. These risks are mitigated by those foreign partners' audit and redress provisions, which

[17] Please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012) at page 7, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.

are identified in the process of negotiating a data sharing agreement. This sub-Appendix details how individuals may contact the United States or Canada for redress options. Also noted above, the Participants will conduct regular quality assurance checks on data exchanged.

Finally, there is a risk of information about special, legally protected classes of individuals being shared inappropriately. IDENT contains information related to aliens who receive special legal protections generally prohibiting disclosure to anyone beyond DHS, the U.S. Department of Justice, and the U.S. Department of State, unless the disclosure fits within certain delineated exceptions (e.g., to a law enforcement official for a legitimate law enforcement purpose). IDENT has technological filters in place that check if a record belongs to an individual in a protected class (VAWA, T, or U visa holders). If so, the record is filtered out from the response that is sent to the foreign partner.

Appendix B-2

U.S. - Australia Biometric Visa and Immigration Information Sharing

Background

Australia and the United States committed to developing and implementing a systematic process for conducting immigration information exchanges under the scope of the Five Country Conference (FCC). On December 12, 2014, the Government of Australia and the Government of the United States of America signed the *Visas and Immigration Information Exchange Agreement* (the *Agreement*) to achieve the following objectives:

- Assist in the administration and enforcement of each country's respective immigration laws;
- Further the prevention, detection, or investigation of criminal acts that would render an individual inadmissible or removable; and
- Facilitate determination of eligibility for a visa, admission, or other immigration benefit, or of whether there are grounds for removal.

On September 9, 2015, in order to perform the biometric information exchange contemplated in the *Agreement*, Australia and the United States ("the Participants") signed an *Implementing Arrangement between the Department of Immigration and Border Protection of Australia, on the One Side, and the Department of State and the Department of Homeland Security of the United States of America, on the Other Side, concerning the sharing of visa and immigration information* (*Implementing Arrangement*). The Implementing Arrangement establishes guidelines for vetting biometric (and associated biographic) information for visa applications and immigration matters against the other Participant's appropriate biometric repositories through an automated process in the following manner:

- Expanding existing biometric information sharing of asylum claimants;
- Expanding biometric information sharing to include overseas refugees applying for resettlement to either country, in accordance with domestic and international obligations; and
- Implementing a systematic and automated sharing capability to support admissibility screening of visa-required third-country nationals, and in support of other administrative and enforcement actions.

This Sub-Appendix B-2 to the IDENT PIA considers the privacy impacts arising from the information sharing under this program. Any information shared must be consistent with the scope of the FCC and the Participants' respective domestic laws and policies.

Overview of Sharing

The biometric visa and immigration information sharing initiative allows Australia and the United States to make electronic fingerprint queries against each other's fingerprint database(s) for the purposes of assisting in the effective administration and enforcement of each Party's respective immigration laws, preventing immigration fraud or other exploitations of immigration, or travel systems by Nationals of a Third Country, and to identify threats to national or public security related to immigration or travel systems. When a biometric match is made in the database, exchange and subsequent use of relevant information, listed below, may occur.

Organizations

For Australia:

Department Immigration and Border Protection of Australia

For the United States:

The U.S. Department of State

The U.S. Department of Homeland Security

Purpose and Use

The purpose of this initiative is to assist in the effective administration and enforcement of the Participants' respective immigration laws. Information exchanged under this initiative will be used to enforce or administer the Participant's respective immigration laws.

Individuals Impacted

The Participants will make queries on:

- individuals who have applied for admission to enter the Requesting Participant's country, or for a visa or an immigration benefit from the Requesting Participant;
- individuals who are the subject of an investigation in relation to a possible immigration-related violation or issue of non-compliance; or
- to establish the basis for a determination relative to admissibility, eligibility for a visa or other immigration benefit, or eligibility to remain in the territory of the Requesting Participant's country.

Queries may be made about individuals who are citizens of either the US or Australia or who are nationals of a third country. The United States will not return information on individuals determined to be applicants for or beneficiaries of certain applications under U.S. law, including applications pertaining to Victims of Human Trafficking (T) or Victims of Criminal Activity (U) non-immigrant status, and Violence Against Women Act (VAWA) relief.

Data Elements

The Participants intend to send, in response to a query, the following data elements when there is a biometric match, subject to availability and practicability in the providing Participant's applicable database or databases (for the United States, IDENT; for Australia, Biometric Acquisition and Matching System (BAMS):

(a) Providing Participant subject specific reference number;

(b) Providing Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Current immigration status;

(m) Other names;

(n) Alias last name(s);

(o) Alias first name(s);

(p) Travel document number;

(q) Travel document type;

(r) Travel document issuing authority/country;

(s) Travel document expiry date;

(t) Reason for alert;[18]

(u) Visa Refusal code;

[18] Alerts are from the DHS enforcement process where a flag has been placed on a person primarily as a Recidivist. "Recidivist with alert" categories include categories for officer safety, smuggling, and individuals flagged for expedited removal.

(v) Watchlist Indicator;[19]

(w) Scan of travel document biodata page;

(x) Scan of other marked travel document pages;

(y) Facial image;

(z) Previous immigration status;

(aa) Date removed;

(bb) Date of arrival;

(cc) Location of arrival;

(dd) Date of departure;

(ee) Location of departure;

(ff) Date of immigration application or non-biometric encounter;

(gg) Type of immigration application or non-biometric encounter;

(hh) Date of outcome of immigration application;

(ii) Outcome of immigration application;

(jj) Reason for outcome of immigration application; and

(kk) Expiry date of current leave/stay or visa.

Following the receipt of a match response, the providing Participant may request that the requesting Participant provide the following data elements for the individual who was the subject of the initial query in order to support further domestic operations relevant to the original record.

(a) Requesting Participant subject specific reference number;

(b) Requesting Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

[19] For purposes of this sharing, "watchlist indicator" is an indication of derogatory information held in IDENT. For a full description of the IDENT watchlist, please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012) at page 6, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf. Canadian responses to U.S. queries will not populate the "watchlist indicator" field because the Global Case Management System (GCMS) does not contain such holdings.

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Other names;

(m) Alias last name(s);

(n) Alias first name(s);

(o) Travel document number;

(p) Travel document type;

(q) Travel document issuing authority/country;

(r) Scan of travel document biodata page;

(s) Facial image;

(t) Current immigration status;

(u) Previous immigration status; and

(v) Date removed.

Applicable SORN Routine Uses

Biometrics/Biographic Information

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN,[20]

> Routine Use H: To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws.

DHS/USCIS-003 Biometric Storage System SORN,[21]

> Routine Use F: To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the

[20] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, 78 FR 69864 (November 21, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-11-21/html/2013-27895.htm.
[21] DHS/USCIS-003 Biometric Storage System SORN, 72 FR 17172 (April 6, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-04-06/html/07-1643.htm.

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

DHS/CBP-006 Automated Targeting System (ATS) SORN[22] (*for legacy NSEERS data only*[23])

Routine Use G: To appropriate federal, state, tribal, local, 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, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-007 Border Crossing Information (BCI) SORN[24]

Routine Use G. 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, when 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.

Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-023 Border Patrol Enforcement Records (BPER) SORN[25]

Routine Use G. 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, when

---

[22] DHS/CBP-006 Automated Targeting System (ATS) SORN, 77 FR 30297 (May 22, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

[23] NSEERS was first implemented in 2002 as a temporary measure in the aftermath of the September 11, 2001 terrorist attacks and was designed to record the arrival, stay, and departure of individuals from certain countries chosen based on an analysis of possible national security threats emanating from those locales. DHS officially ended the NSEERS program in 2011. DHS is sharing this information in the same manner as all other entry-exit information. Any match to individuals who were required to register under NSEERS should not be treated as derogatory information absent any other information. For additional information, please *see* http://www.dhs.gov/dhs-removes-designated-countries-nseers-registration-may-2011.

[24] DHS/CBP-007 Border Crossing Information (BCI), January 25, 2016, 81 FR 404, available at http://www.regulations.gov/#!documentDetail;D=DHS-2016-0006-0001.

[25] DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016. 81 FR 72601, available at https://www.regulations.gov/document?D=DHS-2016-0067-0001.

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.

Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS/CBP believes the information would assist in the enforcement of applicable civil or criminal laws.

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN[26]

Routine Use M: 0To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

Derogatory Information

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN[27]

Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

DHS/CBP-011 U.S. Customs and Border Protection (TECS) SORN[28]

Routine Use G. 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.

[26] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records October 19, 2016, 81 FR 72080, *available at* https://www.regulations.gov/document?D=DHS_FRDOC_0001-1513.
[27] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records October 19, 2016, 81 FR 72080, *available at* https://www.regulations.gov/document?D=DHS_FRDOC_0001-1513.
[28] *available at* 1

DHS/ALL- 030 Use of the Terrorist Screening Database System of Records (TSDB) SORN[29]

> Routine Use A: To the Department of Justice (DOJ)/FBI/TSC in order to receive confirmations that the information has been appropriately transferred and any other information related to the reconciliation process so that DHS is able to maintain a synchronized copy of the TSDB.
>
> DHS will share information contained in this system to Components internal to DHS pursuant to subsec. 552a(b)(1) of the Privacy Act, and subsequently may be shared externally outside DHS at the programmatic level pursuant to routine uses described in the following published system of records notices:
>
> (5) DHS/US-VISIT-004, DHS Automated Biometric Identification System (IDENT), 72 FR 31080, June 5, 2007.

Transactional Information

DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) SORN,[30]

> Routine Use A: To appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice

Biometrics/Biographic Information

Australia provides public notice of how the Department of Immigration and Border Protection manages personal information under the Privacy Act 1988.[31]

Form 1243i[32] explains the Department of Immigration and Border Protection's authority to collect personal identifiers, how they may be collected, the purpose of collection, how they may be used, how they will be protected, and how they may be disclosed. It is publically available and includes notification relevant to the SRTP data exchanges.

Australia completes a Privacy Impact Assessment, which may be publically available under an Australian Freedom of Information request.

---

[29] DHS/ALL- 030 Use of the Terrorist Screening Database System of Records SORN (TSDB) SORN (April 6, 2016, 81 FR 19988), *available at* https://www.regulations.gov/#!documentDetail;D=DHS-2016-0024-0001.
[30] DHS/NPPD/USVISIT-004 Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm.
[31] Australia Privacy Act of 1988, *available at* http://www.border.gov.au/about/access-accountability/plans-policies-charters/policies/privacy.
[32] Australia 1243i Public Notice Form, *available at* http://www.border.gov.au/Forms/Documents/1243i.pdf#search=form%201243i.

Retention

The Participants intend to destroy the fingerprints submitted as part of a query. Response data, sent in the case of a fingerprint match, will be retained only as long as necessary for the purpose for which the data was provided, in accordance with the receiving Participant's respective applicable retention and disposition schedules and respective domestic laws.

For the United States: The United States intends to retain responses from Australia in IDENT consistent with DHS policies and retention schedules. At this time, DHS is in the process of properly aligning the records received from Australia to an approved retention schedule.

For Australia: the Department Immigration and Border Protection of Australia intends to follow information retention consistent with the Department of Immigration and Citizenship Records Authority and Section 336k and 336L of the Migration Act.[33]

Review and Performance Monitoring

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:

- The number and severity of any security breaches and a summary of remedial actions taken; and
- The number and severity of any privacy breaches and a summary of remedial actions taken.

The Participants intend to carry out regular quality assurance activities, including a review of applicable privacy safeguards. For Australia, quality assurance activities will be carried out by the Department Immigration and Border Protection of Australia. For the United States, quality assurance activities will be carried out by the Office of Biometric Identity Management. These activities may include, but are not limited to, determining:

- Whether information has been retained when it should have been destroyed;
- Whether information has been disclosed in a manner inconsistent with the Agreement; and
- The number of correction requests and whether information has been corrected in a manner consistent with the Agreement.

Access, Correction, and Redress

Persons who wish to access Information held by the Australian Participants may visit the Department of Immigration and Border Protection (DIBP) Website:

Visit the Freedom of Information website, http://www.border.gov.au/about/access-accountability/freedom-of-information-foi and complete Form 424A Request for access to

documents of information.[34]

Where to send request:

The DIBP processes requests for documents in Melbourne, Sydney and Canberra. Requestors who live in Victoria, Western Australia or South Australia may submit requests to:

> Freedom of Information Melbourne
> Department of Immigration and Border Protection
> GPO Box 241
> MELBOURNE VIC 3001
> Email: foi.vic@border.gov.au

Requestors who live in New South Wales, Queensland, the Australian Capital Territory, the Northern Territory or Tasmania may submit requests to:

> NSW Freedom of Information
> Department of Immigration and Border Protection
> GPO Box 9984
> SYDNEY NSW 2001
> Email: foi.nsw@ border.gov.au

Requestors who live overseas may send requests to:

> FOI and Privacy Policy Section
> Department of Immigration and Border Protection
> PO Box 25
> BELCONNEN ACT 2616
> AUSTRALIA
> Email: foi@ border.gov.au

Individuals who wish to request access to response data held by the Government of the United States may contact:

> U.S. Department of State:
> Director
> Office of Information Programs and Services (A/GIS/IPS)
> U.S. Department of State
> 515 22nd Street NW, Room 8100, SA-2
> Washington, D.C. 20522-6001
>
> U.S. Department of Homeland Security:
> http://www.dhs.gov/freedom-information-act-and-privacy-act or
> Chief FOIA Officer
> The Privacy Office
> U.S. Department of Homeland Security
> 245 Murray Lane SW, STOP-0655

[34] Freedom of Information Request Form 424A, Request for Access, *available at,* http://www.border.gov.au/Forms/Documents/424a.pdf.

Washington, D.C. 20528-0655

Privacy complaints and enquires can also be directed to DIBP as follows:

- Telephone our Global Feedback Unit on 133 177 during business hours
  Complete the following online feedback form
  http://www.border.gov.au/about/contact/provide-feedback/compliments-complaints-suggestions/visa-citizenship-service.

  Write to the:
  The Manager
  Global Feedback Unit
  GPO Box 241
  Melbourne Vic. 3000
  Australia

- Contact us directly through any of our offices

Individuals who wish to correct response data held by the Government of the United States or to request to add a notation to indicate a correction request was made may submit a correction request to the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP):

http://www.dhs.gov/dhs-trip, or:
United States Department of Homeland Security
Traveler Redress Inquiry Program (DHS TRIP)
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

Correction requests, or requests to add a notation to indicate a correction request was made, may also be directed to:

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

The DHS Office of Citizenship and Immigration Services Ombudsman also assists individuals who wish to resolve issues regarding applications submitted 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
cisombudsman@dhs.gov

Appendix B-3

U.S. - New Zealand Biometric Visa and Immigration Information Sharing

Background

New Zealand and the United States committed to developing and implementing a systematic process for conducting immigration information exchanges under the scope of the Five Country Conference (FCC). On February 10, 2011, the Government of New Zealand's Department of Labor and the Government of the United States of America signed the *Memorandum of Understanding For the Purposes of Implementation of the High Value Data Sharing Protocol between the Nations of the Five Country Conference* (the *Memorandum of Understanding*) to achieve the following objectives:

- Assist in the administration and enforcement of each country's respective immigration laws;
- Further the prevention, detection, or investigation of criminal acts that would render an individual inadmissible or removable; and
- Facilitate determination of eligibility for a visa, admission, or other immigration benefit, or of whether there are grounds for removal.

The High Value Data Sharing Protocol was envisioned as a manual one-off matching through the SFTP (Simple File Transfer Protocol) of biometrics for high value cases against each country's respective biometric holdings. In order enhance mutual cooperation for visa and immigration purposes, and to allow for automated biometrics-based sharing, New Zealand and the United States signed the *Agreement between the Government of the United States of America and the Government of New Zealand for the Sharing of Visa and Immigration Information* (*Visa and Information Agreement*) on May 4th, 2017. *The Visa and Information Sharing Agreement* outlines the terms and conditions for regular information sharing in order to administer or enforce immigration laws, determine visa eligibility and immigration benefits, and increase collaboration on border security, and identity fraud.

On November 7th, 2017, in order to perform the biometric information exchange contemplated in the *Visa and Information Sharing Agreement*, New Zealand and the United State signed the "*Implementing Arrangement between the Department of State and the Department of Homeland Security of the United States of America, on the one side, and the New Zealand Ministry of Business, Innovation and Employment, on the other side, concerning the sharing of visa and immigration information including on a systematic basis* (*Implementing Arrangement*). The *Implementing Arrangement* establishes guidelines for vetting biometric (and associated biographic) information for visa applicants and immigration matters against the Participant's appropriate biometric repositories through an automated process in the following manner:

- Expanding existing biometric information sharing of asylum claimants;

- Expanding biometric information sharing to include overseas refugees applying for resettlement to either country, in accordance with domestic and international obligations; and
- Implementing a systematic and automated sharing capability to support admissibility screening of visa-required third-country nationals, and in support of other administrative and enforcement actions.

This Sub-Appendix B-3 to the IDENT PIA considers the privacy impacts arising from the information sharing under this program. Any information shared must be consistent with the scope of the FCC and the Participants' respective domestic laws and policies.

Overview of Sharing

The biometric visa and immigration information sharing initiative allows New Zealand and the United States to make electronic fingerprint queries against each other's fingerprint database(s) for the purposes of assisting in the effective administration and enforcement of each Party's respective immigration laws, preventing immigration fraud or other exploitations of immigration, or travel systems by Nationals of a Third Country, and to identify threats to national or public security related to immigration or travel systems. When a biometric match is made in the database, exchange and subsequent use of relevant information, listed below, may occur.

Organizations

For New Zealand:

Immigration New Zealand

For the United States:

The U.S. Department of State

The U.S. Department of Homeland Security

Purpose and Use

The purpose of this initiative is to assist in the effective administration and enforcement of the Participants' respective immigration laws. Information exchanged under this initiative will be used to enforce or administer the Participant's respective immigration laws.

Individuals Impacted

The Participants will make queries on:

- individuals who have applied for admission to enter the Requesting Participant's country, or for a visa or an immigration benefit from the Requesting Participant;

- individuals who are the subject of an investigation in relation to a possible immigration-related violation or issue of non-compliance;
- or to establish the basis for a determination relative to admissibility, eligibility for a visa or other immigration benefit, or eligibility to remain in the territory of the Requesting Participant's country.

Queries may be made about individuals who are citizens of either the U.S. or New Zealand or who are nationals of a third country. The United States will not return information on individuals determined to be applicants for or beneficiaries of certain applications under U.S. law, including applications pertaining to Victims of Human Trafficking (T) or Victims of Criminal Activity (U) non-immigrant status, and Violence Against Women Act (VAWA) relief.

Data Elements

The Participants intend to send, in response to a query, the following data elements when there is a biometric match, subject to availability and practicability in the providing Participant's applicable database or databases (for the United States, IDENT; for New Zealand, IDMe):

(a) Providing Participant subject specific reference number;

(b) Providing Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Current immigration status;

(m) Other names;

(n) Alias last name(s);

(o) Alias first name(s);

(p) Travel document number;

(q) Travel document type;

(r) Travel document issuing authority/country;

(s) Travel document expiry date;

(t) Reason for alert;[35]

(u) Visa Refusal code;

(v) Watchlist Indicator;[36]

(w) Scan of travel document biodata page;

(x) Scan of other marked travel document pages;

(y) Facial image;

(z) Previous immigration status;

(aa) Date removed;

(bb) Date of arrival;

(cc) Location of arrival;

(dd) Date of departure;

(ee) Location of departure;

(ff) Date of immigration application or non-biometric encounter;

(gg) Type of immigration application or non-biometric encounter;

(hh) Date of outcome of immigration application;

(ii) Outcome of immigration application;

(jj) Reason for outcome of immigration application; and

(kk) Expiry date of current leave/stay or visa.

Following the receipt of a match response, the providing Participant may request that the requesting Participant provide the following data elements for the individual who was the subject of the initial query in order to support further domestic operations relevant to the original record.

(a) Requesting Participant subject specific reference number;

---

[35] Alerts are from the DHS enforcement process where a flag has been placed on a person primarily as a Recidivist. "Recidivist with alert" categories include categories for officer safety, smuggling, and individuals flagged for expedited removal.

[36] For purposes of this sharing, "watchlist indicator" is an indication of derogatory information held in IDENT. For a full description of the IDENT watchlist, please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012) at page 6, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.

(b) Requesting Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Other names;

(m) Alias last name(s);

(n) Alias first name(s);

(o) Travel document number;

(p) Travel document type;

(q) Travel document issuing authority/country;

(r) Scan of travel document biodata page;

(s) Facial image;

(t) Date removed.

Applicable SORN Routine Uses

Biometrics/Biographic Information

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN,[37]

> Routine Use P: To appropriate Federal, State, tribal, and local government law enforcement and regulatory agencies, foreign governments, and international organizations, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates to elicit information required by DHS to carry out its functions and statutory mandates.

[37] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, 82 FR 43556 (Sept. 18, 2017).

DHS/USCIS-002 Background Check Service SORN,[38]

> Routine Use G: 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, or license, where USCIS believes the information would assist enforcement of civil or criminal law.

DHS/USCIS-003 Biometric Storage System SORN,[39]

> Routine Use F: 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.

DHS/USCIS-007 Benefits Information System,[40]

> Routine Use J: To appropriate Federal, State, tribal, and local government law enforcement and regulatory agencies, foreign governments, and international organizations, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates to elicit information required by DHS to carry out its functions and statutory mandates.

DHS/USCIS-010 Asylum Information and Pre-Screening SORN,[41]

> Routine Use I: To other federal, state, tribal, and local government agencies, foreign governments, intergovernmental organizations and other individuals and organizations as necessary and proper during the course of an investigation, processing of a matter, or during a proceeding within the purview of U.S. or foreign immigration and nationality laws, to elicit or provide information to enable DHS to carry out its lawful functions and mandates, or to enable the lawful functions and mandates of other federal, state, tribal, and local government agencies, foreign governments, or intergovernmental organizations as limited by the terms and conditions of 8 CFR 208.6 and any waivers issued by the Secretary; and
>
> Routine Use J: To a federal, state, tribal, or local government agency or foreign government seeking to verify or ascertain the citizenship or immigration status of any individual within

[38] DHS/USCIS-002 Background Check Service SORN, 72 FR 31082 (June 5, 2007).
[39] DHS/USCIS-003 Biometric Storage System SORN, 72 FR 17172 (April 6, 2007).
[40] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[41] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).

the jurisdiction of the agency for any purpose authorized by law as limited by the terms and conditions of 8 CFR 208.6 and any waivers issued by the Secretary pursuant to 8 CFR 208.6.

DHS/USCIS-017 Refugee Case Processing and Security Screening Information SORN,[42]

Routine Use G: 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, when 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; and

Routine Use J: To requesting foreign governments under appropriate information sharing agreements and there is a legitimate need to share information for law enforcement or national security purposes under 8 CFR 208.6.

DHS/CBP-006 Automated Targeting System (ATS) SORN,[43] (*for legacy NSEERS data only*[44])

Routine Use G: To appropriate federal, state, tribal, local, 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, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-007 Border Crossing Information (BCI) SORN,[45]

Routine Use G. 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, when 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

---

[42] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016).
[43] DHS/CBP-006 Automated Targeting System (ATS) SORN, 77 FR 30297 (May 22, 2012).
[44] NSEERS was first implemented in 2002 as a temporary measure in the aftermath of the September 11, 2001 terrorist attacks and was designed to record the arrival, stay, and departure of individuals from certain countries chosen based on an analysis of possible national security threats emanating from those locales. DHS officially ended the NSEERS program in 2011. DHS is sharing this information in the same manner as all other entry-exit information. Any match to individuals who were required to register under NSEERS should not be treated as derogatory information absent any other information. For additional information, please *see* http://www.dhs.gov/dhs-removes-designated-countries-nseers-registration-may-2011.
[45] DHS/CBP-007 Border Crossing Information (BCI), 81 FR 404 (Jan. 25, 2016).

disclosure.

Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-011 U.S. Customs and Border Protection TECS,[46]

Routine Use G. 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, when 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.

DHS/CBP-016 Nonimmigrant Information System (NIIS),[47]

Routine Use G. 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, when 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.

DHS/CBP-023 Border Patrol Enforcement Records (BPER) SORN,[48]

Routine Use G. 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, when 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.

Routine Use H. To appropriate federal, state, tribal, local, 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, or license,

[46] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008).
[47] DHS/CBP-016 Nonimmigrant Information System (NIIS), 80 FR 13398 (Mar. 13, 2015).
[48] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (Oct. 20, 2016).

when DHS/CBP believes the information would assist in the enforcement of applicable civil or criminal laws.

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN,[49]

> Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

Derogatory Information

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN,[50]

> Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

DHS/CBP-011 U.S. Customs and Border Protection (TECS) SORN,[51]

> Routine Use G. 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.

DHS/ALL-030 Use of the Terrorist Screening Database System of Records (TSDB) SORN,[52]

> Routine Use A: To the Department of Justice (DOJ)/FBI/TSC in order to receive confirmations that the information has been appropriately transferred and any other information related to the reconciliation process so that DHS is able to maintain a synchronized copy of the TSDB.
>
> DHS will share information contained in this system to Components internal to DHS

[49] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016).
[50] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016).
[51] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008).
[52] DHS/ALL-030 Use of the Terrorist Screening Database System of Records (TSDB) SORN, 81 FR 19988 (April 6, 2016).

pursuant to subsec. 552a(b)(1) of the Privacy Act, and subsequently may be shared externally outside DHS at the programmatic level pursuant to routine uses described in the following published system of records notices:

(5) DHS/US-VISIT-004, DHS Automated Biometric Identification System (IDENT), 72 FR 31080, June 5, 2007.

Transactional Information

DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) SORN,[53]

Routine Use A: To appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice

Biometrics/Biographic Information

New Zealand provides public notice of how New Zealand Immigration manages personal information under the Privacy Act of 1993.[54]

New Zealand provides the public with a Privacy Impact Assessment on how New Zealand uses biometric information.[55]

Retention

The Participants intend to destroy the fingerprints submitted as part of a query. Response data, sent in the case of a fingerprint match, will be retained only as long as necessary for the purpose for which the data was provided, in accordance with the receiving Participant's respective applicable retention and disposition schedules and respective domestic laws.

For the United States: The United States intends to retain responses from New Zealand in IDENT consistent with DHS policies and retention schedules. At this time, DHS is in the process of properly aligning the records received from our international partners to an approved retention schedule.

For New Zealand: Immigration New Zealand and the Privacy Commissioner intend to follow information retention consistent with New Zealand's applicable laws.

---

[53] DHS/NPPD/USVISIT-004 Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007).
[54] New Zealand Privacy Act of 1993, available at https://privacy.org.nz/the-privacy-act-and-codes/the-privacy-act/.
[55] Privacy Impact Assessment for FCC countries and biometrics sharing, *available at*, https://www.immigration.govt.nz/about-us/policy-and-law/identity-information-management/how-biometric-information-is-used.

Review and Performance Monitoring

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:

- The number of exchanges from which Information was provided to visa, immigration and border control decision makers before they made a decision;
- The number and percentage of matches;
- The number of cases of identity discrepancies detected;
- The number and severity of any security breaches and a summary of remedial actions taken; and
- The number and severity of any privacy breaches and a summary of remedial actions taken.

The Participants intend to carry out regular quality assurance activities, including a review of applicable privacy safeguards. For New Zealand, quality assurance activities will be carried out by the Privacy Commissioner.

For the United States, quality assurance activities will be carried out by the Office of Biometric Identity Management (OBIM). These activities may include, but are not limited to, determining:

- Whether information has been retained when it should have been deleted and destroyed;
- Whether Information exchanged under the Agreement has been marked as having been received from the other Participant;
- Whether information has been disclosed in a manner inconsistent with the Agreement; and
- The number of correction requests and whether information has been corrected in a manner consistent with the Agreement.

Access, Correction, and Redress

Persons who wish to access Information held by New Zealand Participants may visit the New Zealand Privacy Commissioner website:

Visit the website: https://www.privacy.org.nz/further-resources/aboutme-request-my-info-tool/.

Persons may also visit the Immigration New Zealand website. Visit the website: https://www.immigration.govt.nz/contact/request-information.

Where to send request:

Immigration New Zealand processes requests for documents at the following address:

New Zealand Immigration Ministry
Level 6
66 Hunter Street
Sydney
New South Wales 2000

Request Personal information:
https://www.immigration.govt.nz/contact/request-information.

You may also submit requests to the New Zealand Privacy Commissioner:

New Zealand Privacy Commissioner
PO Box 10 094, The Terrace, Wellington 6143
Fax: (04) 474 7595

Similarly, individuals who wish to request access to response data held by the Government of the United States may contact:

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

U.S. Department of Homeland Security:

http://www.dhs.gov/freedom-information-act-and-privacy-act or
Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
245 Murray Lane SW, STOP-0655
Washington, D.C. 20528-0655

Individuals who wish to correct response data held by the Government of the United States or to request to add a notation to indicate a correction request was made may submit a correction request to the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP):

http://www.dhs.gov/dhs-trip, or:
United States Department of Homeland Security
Traveler Redress Inquiry Program (DHS TRIP)
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

Correction requests, or requests to add a notation to indicate a correction request was made, may also be directed to:

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

The DHS Office of Citizenship and Immigration Services Ombudsman also assists individuals who wish to resolve issues regarding applications submitted 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
cisombudsman@dhs.gov

Appendix: C

Organizations:

U.K. Border Agency (UKBA) International Group Visas Services Project (formerly known as UKvisas) and DHS (USCIS and US-VISIT).

Purpose and Use:

DHS will provide information to the UKBA International Group Services Project to help UKBA determine whether visa applicants for entry to the United Kingdom are eligible to obtain visas or other travel documents according to applicable U.K. laws.

The purpose of this information sharing is to assist UKBA in making visa or travel document determinations while supporting the DHS mission. This information sharing enables DHS to enhance the integrity of the U.S. immigration system by detecting, deterring, and pursuing immigration fraud, and to identify persons who pose a threat to national security and/or public safety. Although the DHS – UKBA MOU allows enrollment, the UKBA currently performs a search only; no data is enrolled in IDENT.

US-VISIT will use the biographic and biometric information received from the UKBA International Group Visa Services Project, and provided by the visa applicant, to determine whether the applicant's biometrics are currently included in the IDENT list of subjects of interest. In the event of a biometric match, US-VISIT will use additional biographic information provided by the United Kingdom to support any necessary law enforcement or immigration enforcement investigations.

Individuals Impacted:

This sharing impacts individuals applying for a U.K. visa from select locations, including the United States and Jamaica. The majority of those applying in the United States and Jamaica for a visa to enter the United Kingdom will be third-country nationals. However, U.S. citizens who intend to stay in the United Kingdom for longer than 3 months, or to enter the United Kingdom to engage in work, may also require a visa, according to U.K. immigration laws. Accordingly, U.S. persons may be included in data transfers between UKB and US-VISIT systems. As new locations are included in the project, those locations will be included in addenda to the DHS - UKBA MOU.

Data Elements:

Applicants submit their biographic information via the UKBA online visa application. Additionally, the applicant submits his or her biometric data (10 fingerprints and a digital facial photograph) at a USCIS ASC (which collects on behalf of UKBA) or a UKBA International Group Visa Services Project post. The following categories of information are required to complete the UKBA visa application:

Biometric data: digital facial photograph and 10 fingerprints

Biographic data: full name, date of birth, place of birth, country of citizenship, document identifier (e.g., document type, document number, and country of issuance), and gender.

The UKBA International Group Visa Service Project forwards the applicant's information, with the addition of a U.K. unique identification number, to US-VISIT. Only the 10 fingerprints will be queried against the IDENT list of subjects of interest. US-VISIT will not conduct name-based checks. If a match does *not* occur, US-VISIT will transmit two data elements back to the United Kingdom:

a) Status code: "None"

b) UK Unique Identifier.

US-VISIT will then delete all information pertaining to the applicant. If a match *does* occur, US-VISIT will transmit three data elements back to the United Kingdom:

a) Status code: "Watchlist"

b) UK Unique Identifier

c) Encounter ID.

The applicant's information may be stored in the Technical Reconciliation Analysis Classification System[56] (TRACS) for case management. In both cases (match or no-match), no information is stored in IDENT.

Applicable IDENT SORN Routine Uses:

This sharing between DHS and UKBA is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice:

As the UKBA is not subject to the Privacy Act, it does not have a SORN covering its visa data. However, additional notice is provided by the UKBA International Group Visa Services website at www.ukvisas.gov.uk.

[56] For a full discussion of TR ACS, see DHS/NPPD/USVISIT/PIA-004Technical Reconciliation Analysis Classification System (TRACS), June 6, 2008

Retention by Partner:

The UKBA International Group Visa Services Project will retain the information provided by DHS until such time that UKBA has no mission-related need or after 75 years of its receipt from DHS, whichever is sooner. The 75-year retention period is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.

Compliance Reporting:

Section 8 of the IDENT PIA covers US-VISIT compliance reporting. The corresponding MOU for this project did not establish any additional compliance-reporting requirements.

Onward Transfer:

The existing MOUs for this project do not outline any limitations.

Training:

The United Kingdom owns the biometric and biographic data of individuals who apply for visas and travel documents to the United Kingdom, and that nation provides privacy training to employees who access that data.

Correction and Redress:

The UKBA International Group Visa Services Project is solely responsible for granting or denying UKBA International Group Visa Services Project applications. The UKBA International Group Visa Services Project will determine whether any change to an applicant's information by US-VISIT, as a result of a successful redress request, will impact the adjudication process of the UKBA International Group Visa Services Project. The appeals process for handling inaccurate or erroneous information on behalf of the UKBA International Group Visa Services Project is solely the responsibility of the United Kingdom and can be found on the UKBA International Group Visa Services website at www.ukvisas.gov.uk.

If the applicant is denied a visa to enter the United Kingdom, the UKBA International Group Visa Services Project will provide a letter of visa denial and visa appeal to the applicant. The appeals process of the UKBA International Group Visa Services Project varies based on the circumstances upon which the applicant was denied a visa. The denial letter will detail the process the applicant must follow to appeal the visa decision. Individuals who are denied visas to enter the United Kingdom may refer to the UKBA website at http://www.ukba.homeoffice.gov.uk/visas-immigration/visiting/general/appeals/ for more information.

Appendix: D

Organization:

United States (U.S.) Department of Defense (DOD)

Purpose and Use:

Information sharing with DOD supports the missions of DOD and DHS. For DOD, relevant missions include active military operations, warfighter, detainee affairs, force protection efforts, anti-terrorism, special operations, stability operations, homeland defense, counterintelligence, and intelligence. For DHS, relevant missions include critical infrastructure protection, transportation and border security, law enforcement, administration of immigration benefits, emergency management, intelligence, and other interests of the United States.

Current biometric data sharing between DOD and the Office of Biometric Identity Management (OBIM) is mostly through manual processes. The Automated Biometric Identification System (ABIS) is DOD's multi-modal biometric system for matching, storing, and sharing biometrics in support of military operations with government agencies and with partner nations. The DOD Biometric Enabled Watchlist (BEWL) is located in ABIS. The National Ground Intelligence Center (NGIC) is responsible for adding persons to BEWL. The BEWL includes known or suspected terrorists, national security threats, and DOD detainees.[57] Those identities are subsequently transmitted to OBIM by DOD's Biometric Identity Management Agency (BIMA) through a secure file transfer protocol (SFTP) site. The biometric records are then enrolled in the DHS Automated Biometric Identification System (IDENT) and added to the IDENT watchlist, which is available to all DHS stakeholders searching IDENT. OBIM in turn provides information to DOD on matches in IDENT where permissible, on those enrolled records from the BEWL. OBIM checks IDENT for any subsequent encounters on these DOD BEWL records and shares this information with DOD, where permissible.

To support the DHS mission, DHS also receives DOD latent prints on a daily basis through the Federal Bureau of Investigation (FBI). All submissions to the FBI's Universal Latent File are also submitted for search against the entire IDENT gallery.

Going forward, OBIM and DOD recognize the need to increase biometric data sharing through an automated connection between IDENT and ABIS to create interoperability. Through IDENT-ABIS interoperability, DHS and DOD will directly link IDENT and ABIS to enable searches by end users of each system. Through IDENT-ABIS interoperability in the future, both DHS and DOD will have access to expanded datasets from the other system.

[57] Detainees are individuals who are detained by DOD for at least 2 weeks and are issued an internment serial number, but who have not been vetted by NGIC analysts for a formal threat determination.

Individuals Impacted:

KSTs, national security threats, DOD detainees and individuals of interest to DOD and DHS. Information shared may contain information about U.S. Persons.

Data Elements:

ABIS is DOD's authoritative, multi-modal biometric system for matching, storing, and sharing biometrics in support of military operations, with government agencies, and with partner nations.

ABIS encounter information could contain data elements such as: ABIS encounter specific identifier, reason fingerprinted, date fingerprinted, arrest segment literal, fingerprinting agency, fingerprints, iris images, facial images, palmprints, name, aliases, date of birth, place of birth, country of citizenship, and gender.

IDENT encounter information could contain data elements such as: digital facial photographs, fingerprints, IDENT unique identifiers, IDENT organization/unit/sub-unit, encounter information, encounter specific identifier, name, aliases, date of birth, place of birth, country of citizenship, nationality, gender, and date fingerprinted.

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

The sharing of PII outside of DHS is compatible with the original collection of that information and is covered by the IDENT SORN, 72 FR 31080 (June 5, 2007).

All or a part of the data contained in IDENT records may be disclosed as a routine use to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions as determined by DHS (Routine Use J).

Partner Notice:

This information is covered by two DOD SORNs: Defense Biometric Services, 74 Fed. Reg. 48237 (Sep. 22, 2009), available at http://dpclo.defense.gov/privacy/SORNS/dod/A0025-2_SAIS_DoD.html, and Department of Defense Detainee Biometric Information System, 72 Fed. Reg. 14534 (Mar. 28, 2007), available at http://dpclo.defense.gov/privacy/SORNs/dod/A0025-2c_SAIS_DoD.html.

Retention by Partner:

DHS and DOD will retain the data only as long as is needed to fulfill the purposes of the project. In no instance will the retention period of any data item exceed the maximum period permissible by applicable legal and regulatory requirements or official retention policies.

Compliance Reporting:

Both DHS and DOD may audit the access, use, handling, and maintenance of each other's data to ensure compliance. DHS and DOD may independently audit and inspect the other's use of data provided and review the audit records of the other agency. The agencies may also accept the results of internal agency audits (such as Inspector General audits) conducted in lieu of an audit.

Onward Transfer:

Both agencies acknowledge that data stored on behalf of third parties, or subsequent matches to that data, will not be shared without the consent of the data owner.

Where a Party receives a third party request for information shared under the MOA, such as a request under the Freedom of Information Act or the Privacy Act, or through Congressional or media request, or any other method, that Party will ensure that it does not adjudicate such requests for the other Party. The Party receiving a third party request for information which is owned or originated by the other Party shall immediately consult with the other Party as to how to respond to the request.

Training:

DOD personnel with access to data shared are trained in the protection and proper treatment of all data, to ensure overall safeguarding of the information, in accordance with the Privacy Act and other applicable laws and policies, including but not limited to confidentiality regulations associated with particular immigration benefits.

DOD abides by DHS' privacy policies, ensures that its employees, including contractors and detailees from third agencies with access to any of DHS' data, have completed any required privacy and information assurance training on the handling of all data.

DOD also trains designated users on techniques to effectively query any shared systems, if requested. The training will include an explanation of data fields and be closely coordinated by DHS.

Correction and Redress:

OBIM redress measures are discussed in Section 7 of the PIA.

Both agencies maintain an ability to locate and correct PII maintained by the other department. Additionally, DOD corrects any disseminated information based on the information that is later deemed to be erroneous. DOD must provide written confirmation to DHS of the

corrections made. The applicable SORNs cited above provide instructions for submitting a redress request to DOD.

Appendix: E

Organizations:

The Governments of the United States of America and the Republic of Estonia.

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, such as terrorism-related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

The government of the U.S.A. and the Republic of Estonia will share information on citizens and third party nationals who are suspected or convicted of committing serious crimes.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Estonia is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE), 75 Fed. Reg. 23274 (May 3, 2010); DHS/USVISIT-0004 - DHS Automated Biometric Identification System (IDENT), 72 Fed. Reg. 31080 (Jun. 5, 2007).

Partner Notice: Estonia provides public notice on the collection of personal information through the public website for legal acts (www.riigiteataja.ee) and also through the websites of the responsible authorities, as required by the Estonian Public Information Act of 2000 and the Estonian Personal Data Protection Act of 2008.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

All system users receive basic training and also a follow up training as ongoing training needs and changes in legislation dictate.

Correction and Redress:

Individuals may request access to personal information through the Police and Border Guard Board or through the Ministry of Justice. Information requests can be filed by mail or email. Estonian residents (including foreign nationals who possess an Estonian residence permit) also have the option to access their personal information through the e-governance state portal (www.eesti.ee), which allows them to view a log of others who have accessed their data. Individuals may request correction to personal information pursuant to legislation, regulations and guidelines.

Police and Border Guard Board
Pärnu mnt 139, Tallinn 15060
+372-612-3000
E-mail: ppa@politsei.ee

Ministry of Justice
Tõnismägi 5a, Tallinn 15191
+372-620-8100
E-mail: info@just.ee

Appendix: F

Organizations:

The Governments of the United States of America and the Czech Republic

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offences and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, such as terrorism-related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals impacted:

The governments of the U.S.A. and the Czech Republic will share information on citizens and third party nationals who are suspected or convicted of committing serious crimes.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information). Other information held in US-VISIT and ICE systems may also be exchanged.

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Czech Republic is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE), 75 Fed. Reg. 23274 (May 3, 2010).

Partner Notice:

Public notice of the collection and processing of personal information in the Czech Republic is contained in law. According to Section 60 of the Act 273/2008 Coll., the Czech police is entitled to collect and process personal information to the extent necessary for performance of its tasks (which according to Section 2 of the same Act, include prevention of crime, along with protection of persons, property and public order). The Act also lists essential information on access of Police to various state or public databases and information systems, along with the powers of the police to collect and process personal data. Pursuant to Section 83 of this Act, any individual has right to ask about personal information that is processed by the police and to request correction, erasure, amendment, or blocking of incorrect or inaccurate personal data.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records where permissible.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The Police Presidium's Personal Data Department trains and advises police personnel on processing of personal data. Aside from organizing periodic training sessions for police personnel on data privacy and handling procedures, the department also advises police personnel on handling of individual cases and supervises all data privacy programs within the Police Presidium.

Correction and Redress:

Written requests for access or redress can be sent to:

Police Presidium of the Czech Republic
Strojnická 27 (PO BOX 62/K-SOU)
170 89 Prague 7
Czech Republic

Requests may be also filed in person to any police station during public hours. The requests are free of charge. Follow-up or repeat requests can be filed six months after the original inquiry.

In order to process a request, the data subject must provide information necessary for identification (name and surname, date of birth, place of residence or address for correspondence). If a lawyer makes request on behalf of another person, a notarized power of attorney must be enclosed. Otherwise, the signatures on a request will have to be verified in person.

Replies are sent within 60 days by certified mail.

Appendix: G

Organizations:

The Governments of the United States of America and the Slovak Republic

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offences and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals impacted:

The governments of the U.S.A. and the Slovak Republic will share information on citizens and third party nationals who are suspected or convicted of committing serious crimes.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Slovak Republic is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE), 75 Fed. Reg. 23274 (May 3, 2010).

Partner Notice:

Sections 69 through 69g of Act No. 171/1993 Coll. on the Police Force provide notice about the processing of personal data by the Police Force.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records where permissible.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

All police officers who process personal data while carrying out service tasks are required to take special training on international agreements as well as Acts of the Slovak Republic and

internal regulations of the Police Force, which contain provisions relevant to data protection and processing of personal data.

Correction and Redress:

Written requests for access and correction of personal data can be sent to:

Ministry of Interior of the Slovak Republic
Pribinova 2
812 72 Bratislava
skis@minv.sk

The Police Force must respond to the applicant no later than 30 days from the receipt of the request. The request is free of charge.

Appendix: H

Organizations:

The Governments of the United States of America and the Kingdom of Spain

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

The governments of the U.S.A. and the Kingdom of Spain will share information on citizens and third party nationals who are suspected or convicted of committing serious crimes.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Kingdom of Spain is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE), 75 Fed. Reg. 23274 (May 3, 2010).

Partner Notice:

The Spanish Personal Data Protection Law of 1999 in its Article 5 gives notice to individuals as to how personal data will be collected, treated, handled and stored.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The Spanish Data Protection Agency trains and monitors on a continuous basis all the agents involved in the collection and handling of personal data as mandated by Article 37 (f) of Spanish Personal Data Protection Law of 1999.

Correction and Redress:

Individuals can request access to their own personal information under the Spanish Personal Data Protection law by requesting it to the Spanish Data Protection Agency - Subdirectorate for the Inspection of the Data Protection Agency. The request for access of personal information has to be sent in writing to:

Subdirección General de Inspección de Datos

Agencia Española de Protección de Datos
Calle Jorge Juan, 6-28001-Madrid
Or by fax to +34 914 455 699

The POC for redress if the breach was caused by Government:

Spanish Data Protection Agency
Subdireccion General de Inspeccion
Calle Jorge Juan 6
Madrid 28001
Or by fax +34 914 455 699

Appendix: I

Organizations:

The Governments of United States of America and the Principality of Andorra

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Principality of Andorra.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Principality of Andorra is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

According to the Law 15/2003, of 18th December, on personal data protection, the creation, rectification and erasure of public files has to be regulated by a decree published in the Official Journal of the Principality of Andorra unless otherwise regulated by a specific Law.

Files with private purposes must be registered before its creation by the controller of the data in the public registry run by the supervisory authority: the Andorran Data Protection Agency (ADPA). Privacy notices for private organizations are available on the APDA website. Privacy notices for public organizations are published in the Official Gazette.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The ADPA publishes two *Good practice manuals* with tips on how to use and handle personal information properly. One of these is specifically addressed to officials who handle personal information. The manuals are on the Agency's website, https://www.apda.ad/. All Andorran Police officials who handle personal information are trained via the manual.

Correction and Redress:

Individuals may request access to personal information by writing to:

Andorran Police (Cos de Policia d'Andorra)
Despatx Central de Policia, Ed. Administratiu de l'Obac, Crta. de l'Obac s/n,
Escaldes-Engordany
Andorra
Tel: (+376) 872 000
Fax: (+376) 872 004
policia@andorra.ad

Individuals may request correction of personal data by writing to:

Andorran Police (Cos de Policia d'Andorra)
Despatx Central de Policia, Ed. Administratiu de l'Obac, Crta. de l'Obac s/n,
Escaldes-Engordany
Andorra
Tel: (+376) 872 000
Fax: (+376) 872 004
policia@andorra.ad

For any issues or concerns regarding proper handling of personal information, access, or redress, please contact the Andorran Data Protection Agency.

Andorran Data Protection Agency (L'Agència Andorrana de Protecció de Dades)
Carrer Dr. Vilanova núm. 15, planta -5
Andorra la Vella
Telèfon: (+376) 808 115
Fax: (+376) 808 118
https://www.apda.ad/contact/

Appendix: J

Organizations:

The Governments of United States of America and the Portuguese Republic

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Portuguese Republic.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Portuguese Republic is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Portugal provides public notice on the collection of personal information through regulation published at the Official Journal (Lei 67/98; Lei 5/2008 and Deliberação 3191/2008).

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Portugal: provides training to all authorized systems users according to their roles, including training in the handling of personal information and organizes meeting to discuss practical questions.

Correction and Redress:

For access and redress requests, contact:

Instituto Nacional de Medicina Legal e Ciências Forenses, I.P.
Largo da Sé Nova
3000-213 Coimbra
Tel.: (+351) 239 854 220
Fax: (+351) 239 836 470

and

Laboratório de Polícia Científica da Polícia Judiciária
Rua Gomes Freire, 174
1169-007 Lisboa
Tel: (+351) 218 641 587
Fax: (+351) 213 570 161
e-mail: lpc.sij@pj.pt

Appendix: K

Organizations:

The Governments of United States of America and the Republic of Malta

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Malta.

Data Elements:

Biometric data: digital facial photograph and fingerprints.

Biographic data: Data exchanged under this project may include (but not limited to): Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Malta is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The Republic of Malta provides notice to individuals on an individual basis through a subject access request as provided in the Data Protection Act.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The Republic of Malta provides regular basic training on the handling of personal data and data protection matters to all serving members of the force at various levels. The regular basis of these trainings ensure timely updates to these officers with respect to legislative amendments and/or practical arrangements

Correction and Redress:

For Access:

Any individual may make a subject access request to check about the processing of his/her personal data to the Malta Police Data Protection officer. The contact details are:

Data Protection Office
Police General Headquarters
Floriana
Tel.No. +35622942196
Email:sandro.camilleri@gov.mt

For Redress:

Individuals may request correction to personal information by submitting a request to the Malta Police Data Protection Officer and they may also appeal within thirty days from the decision of the Malta Police Data Protection Officer to the Information and Data Protection Commissioner on the following contact details:

Office of the Information and Data Protection Commissioner
Airways House, Second Floor
High Street
Sliema SLM 1549
MALTA.
Tel: (+356) 2328 7100
Fax: (+356) 23287198
Email: idpc.info@gov.mt

Appendix: L

Organizations:

The Governments of United States of America and Hungary

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and Hungary.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from Hungary is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Hungary provides public notice to the data subjects on the collection of personal information according to Act CXII of 2011 (On Informational Self-determination and Freedom of Information).

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

According to Hungarian data protection legislation, at any entity that deals with personal data, new employees receive a general training that includes the rules to be adhered to when dealing with databases of personal data. In case of changes as regards regulations of data protection, employees receive a follow-up training focusing on changes.

Correction and Redress:

For access:

The Hungarian National Authority for Data Protection and Freedom of Information in accordance with Section 66 of Act CXII of 2011 registers data processing undertaken in respect to personal data in a data protection file or registry in order to facilitate access to information for the data subject. The registry is public, the data subjects can for the moment obtain information on request, but the whole registry will be soon available and searchable on the authority's website (http://www.naih.hu/).

For redress:

After consulting the public registry, the data subject may turn to the data controller and in accordance of the Section 14 of the Privacy Act may request the following from the controller:

a. information on the control of personal data,
b. correction of personal data, and
c. deletion, blocking of personal data, with the exception of mandatory control.

In cases where the data subjects deem that the answer given by the data controller is inappropriate or the denial for giving him/her information was unlawful he/she may turn to the National Authority for Data Protection and Freedom of Information (NAIH) for redress.

H-1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Telefon: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: privacy@naih.hu, web: www.naih.hu

Appendix: M

Organizations:

The Governments of United States of America and Commonwealth of Australia

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally has the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Commonwealth of Australia.

Data Elements:

Biometric data: digital facial photograph and fingerprints.

Biographic data: Data exchanged under this project may include (but not limited to): Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Commonwealth of Australia is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Australia provides public notice on the collection of personal information through the Personal Information Digest (PID) published in accordance with the *Privacy Act 1988.* The PID is available through the Office of the Australian Information Commission (OAIC) website http://www.oaic.gov.au.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Australia provides training to authorized system users in accordance with their roles, procedures and on basic application of relevant legislation.

Correction and Redress:

Individuals may request access to personal information under the Privacy Act through the Freedom of Information Act.

The Australian Federal Police
Freedom of Information contact officer
Phone: +61 2 61316131
Email: foi@afp.gov.au

Australia Government
Office of the Australian Information Commissioner
Phone: +61 2 9284 9666
Email: enquiries@oaic.gov.au

Individuals may request correction to personal information pursuant to Commonwealth law, regulations, and guidelines.

The Australian Federal Police
Freedom of Information contact officer
Phone: +61 2 61316131
Email: foi@afp.gov.au

Australia Government
Office of the Australian Information Commissioner
Phone: +61 2 9284 9666
Email: enquiries@oaic.gov.au

Appendix: N

Organizations:

The Governments of United States of America and the Republic of Austria

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Austria.

Data Elements:

Biometric data: digital facial photograph and fingerprints.

Biographic data: Data exchanged under this project may include (but not limited to): Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Austria is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The Republic of Austria does not provide public notice. Individuals have the right to access their personal information, but personal data is not available to the general public, pursuant to Article 26 Data Protection Law of 2000. Requests must be made to the ordering party (owner) of the collected data (public authorities or companies) in written form. Requests on personal data in the Central Criminal Data Register must be made to the relevant police authority.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Provides basic training to authorized system users.

Correction and Redress:

Individuals have the right to access their personal information, but personal data is not available to the general public, pursuant to Article 26 Data Protection Law of 2000. Requests must be made to the ordering party (owner) of the collected data (public authorities or companies) in written form. Requests on personal data in the Central Criminal Data Register must be made to the relevant police authority.

Individuals may request access to personal information to all public and private holders of their personal data, pursuant to the Austrian Data Protection Act from 2000. In case of doubt on who is in charge of the data or for general information the Point of Contact is:

Austria Data Protection Commission (Datenschutzkommission)
Hohenstaufengasse 3
A-1010 Vienna
Phone: +43 1 531 15-202525
Fax: +43 1 531 15-202690
Email: dsk@dsk.gv.at

Individuals may request correction to (or deletion of) personal information pursuant to Article 27 of the Data Protection Law of 2000 to the holders of their personal data. If the request is not accepted, the individual can lodge a complaint to the:

Austria Data Protection Commission (Datenschutzkommission)
Hohenstaufengasse 3
A-1010 Vienna
Phone: +43 1 531 15-202525
Fax: +43 1 531 15-202690
Email: dsk@dsk.gv.at

Appendix: O

Organizations:

The Governments of United States of America and the Kingdom of Denmark

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Kingdom of Denmark.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Kingdom of Denmark is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The Kingdom of Denmark provides public notice on the collection of personal information through the public website for the Danish Police (www.politi.dk) and the official website for the Danish Data Protection Agency (www.datatilsynet.dk).

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The Kingdom of Denmark provides basic training for all system users and also a follow up training as ongoing training needs and changes in legislation dictate.

Correction and Redress:

Access: Individuals may request access to personal information through the local police district or through the Danish National Police. Information requests can be filed by mail or email. Contact information is available through the official website for the Danish Police (www.politi.dk).

Redress: Individuals may request correction to personal information pursuant to legislation, regulations, and guidelines through the local police district or through the Danish National Police. Requests can be filed by mail or email. Contact information is available through the official website for the Danish Police (www.politi.dk).

In addition, individuals may file a complaint with the Danish Data Protection Agency on whether personal data has been processed in accordance with the Danish Act on Processing of Personal Data (www.datatilsynet.dk).

Appendix: P

Organizations:

The Governments of United States of America and the Republic of Finland

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally has the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Finland.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Finland is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The Republic of Finland provides public notice of how personal information is collected and handled through different registers in various acts, but especially in the Personal Data Act (523/1999). Other relevant legislation giving notice to individuals are the Act on the Processing of Personal Data by the Police (761/2003), the Act on the Protection of Privacy in Working Life (759/2004) as well as the Act on the Protection of Privacy in Electronic Communications (516/2004). When data is given from a register belonging to a public authority, the Act on the Openness of Government Activities (621/1999) applies.

All the legal acts related to the handling of personal data can be found on the public website for legal acts (www.finlex.fi). Additionally, information on the handling of personal data can be found on the websites of the Data Protection Ombudsman (www.tietosuoja.fi).

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

There is no specific clause in the Finnish legislation regarding training on processing of data, but the legislation implies that the personnel in charge of the processing of the data is adequately trained for the purpose. The Data Protection Ombudsman and the Office of the Data Protection Ombudsman provide guidance and advice on the processing of personal data, organize trainings on demand, and control the observance of the law.

Correction and Redress:

When a data subject wants to use one of the rights granted by the Personal Data Act (right of information on the processing of data; right of access, rectification, right to prohibit processing) or when the data subject has a query about the handling of his/her data, they should first contact the controller in charge of processing the data. If the matter cannot be dealt with the controller, the data subject can contact the Data Protection Ombudsman. If the processing of the data seems unlawful, the data subject can ask the Police to investigate the matter.

Office of the Data Protection Ombudsman
P.O. Box 315
FIN-00181 HELSINKI
FINLAND

Address:
Albertinkatu 25 A, 3rd floor
E-mail: tietosuoja@om.fi
Tel: +358 29 56 66700 (exchange)

Appendix: Q

Organizations:

The Governments of United States of America and the Federal Republic of Germany

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally has the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Federal Republic of Germany.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Federal Republic of Germany is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

In Germany, the relevant information on notifications can be found directly in the specific laws regulating the respective data processing. These laws include – similar to the "Systems of Record Notices"– information on the purpose of processing data and rights of individuals (such as transmission/retention of data) and duties (such as deletion) of the respective agency processing the data. Relevant legal bases include the Federal Data Protection Act (BDSG) that contains general requirements (e.g. section 12 et seq) and in the case of PCSC, the Federal Criminal Police Office Act (Bundeskriminalamtgesetz- BKAG) (e.g. section 7 et seq) as *lex specialis*.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

All public service employees who work with personal data are trained accordingly. Data protection officers of government agencies are required by law to provide advising and training.

Correction and Redress:

Under Section 19 of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) in conjunction with Section 12 (5) of the Federal Criminal Police Office Act (Bundeskriminalamtgesetz, BKAG), individuals may request information about their personal data on file. If a request is refused, individuals may have recourse to the administrative courts. Individuals may also request the assistance of the Federal Commissioner for Data Protection and Freedom of Information.

For access to information held on them, individuals may reach out to:

Bundeskriminalamt (Federal Criminal Police Office)
Der Datenschutzbeauftragte (Data protection officer)
65173 Wiesbaden
dsrecht@bka.bund.de

For correction and redress:

Bundesministerium des Innern (Federal Ministry of the Interior)
Arbeitsgruppe ÖS I 3 (Task Force ÖS I 3)
Alt-Moabit 101 D
10559 Berlin
OESI3AG@bmi.bund.de

Appendix: R

Organizations:

The Governments of United States of America and Taiwan

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and Taiwan.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from Taiwan is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Notifications of collections of personal information are in accordance with Articles 8, 15, and 19 of the Personal Information Protection Act (PIPA) and notifications of usage of personal information are in accordance with Articles 9, 15, and 19 of the PIPA

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Training is provided to all authorized users.

Correction and Redress:

International Criminal Affairs Division of
National Police Agency's Criminal Investigation Bureau
Republic of China (Taiwan)
Email: CIBPCSC@email.cib.gov.tw
Telephone: +886 2 27697390

Redress:

International Criminal Affairs Division of
National Police Agency's Criminal Investigation Bureau
Republic of China (Taiwan)
Email: CIBPCSC@email.cib.gov.tw
Telephone: +886 2 27697390
(Forensic Biology Office, Fingerprint Office, Criminal Records Section
Criminal Intelligence Office
Internal Affairs Office of National Police Agency's Criminal Investigation Bureau
Republic of China (Taiwan))

Appendix: S

Organizations:

The Governments of United States of America and the Republic of Latvia

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

The governments of the U.S.A. and the Republic of Latvia will share information on citizens and third country nationals who are suspected or convicted of committing serious crimes.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Latvia is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Information on Systems that collect and process information on individuals can be found on the public website: http://www.vvc.gov.lv/advantagecms/LV/tulkojumi/dokumenti.html?folder=%2fdocs%2fLRTA%2fLikumi%2f&currentPage=16 under the link State information systems.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Republic of Latvia, Centre of the Ministry of the Interior (the Centre) thoroughly trains users of the information systems for which it is responsible.

Correction and Redress:

According to the Personal Data Protection Law, any person has a right to request any information held on him/her in any of the personal data processing system/registry. The disclosure of such information is subject to some exemptions. For access and redress requests, contact:

Information Centre of the Ministry of the Interior
Bruninieku street 72b
Riga
LV-1009
Latvia
e-mail: kanceleja@ic.iem.gov.lv

The Centre also maintains multiple e-services which allow individuals to access a limited amount of information on themselves stored in the information systems held by the Centre. Links to all of the e-services provided by the Centre may be found on the Centre's webpage: http://www.ic.iem.gov.lv/en/node/33, while the interfaces of these services are located on the central national web-portal for public services: www.latvija.lv.

Appendix: T

Organizations:

The Governments of United States of America and the Republic of Ireland

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Ireland.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Ireland is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The Freedom of Information Central Policy Unit in the Department of Public Expenditure & Reform is centrally responsible for the provision of information, guidelines, and other resources relevant to the Irish Freedom of Information Acts. Further information can be found at www.foi.gov.ie.

Each Government Department has within it a Freedom of Information Unit which manages requests under that legislation of relevance to the remit of the Department in question.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The Republic of Ireland provides training to all authorized system users according to their roles. This includes training in the handling of personal information.

Correction and Redress:

For access:

The Freedom of Information (FOI) Acts, 1997 and 2003 establishes three statutory rights:

- a legal right for each person to access information held by public bodies;
- a legal right for each person to have official information relating to him/herself amended where it is incomplete, incorrect or misleading; and
- a legal right to obtain reasons for decisions affecting oneself.

Under the Freedom of Information Act, anyone is entitled to apply for access to information not otherwise publicly available.Each person has a right to:

- access records held by a Government Department;
- correct personal information relating to oneself held by the Department where it is inaccurate, incomplete or misleading; and
- access to reasons for decisions made by the Department directly affecting oneself.

Requests for information under the FOI Acts, 1997 and 2003 should be addressed to the Freedom of Information Officer in the relevant Government Department. For example:

Freedom of Information Officer,
Department of Justice and Equality,
51 St. Stephen's Green,
Dublin 2
Ireland

Requests for Information held by An Garda Síochána (Irish Police):

An individual may also apply to the Garda Síochána for a disclosure under Section 4 of the Data Protection Act 1988 (as amended) for a copy of the personal data which is maintained by An Garda Síochána. Such a disclosure is made to the individual to whom the data relates. An individual seeking access to their information should complete a Data Protection Access Request form - F20 and return it with relevant enclosures to the Garda Criminal Records Office, Racecourse

Road, Thurles, Co. Tipperary, Ireland. For further information see http://www.garda.ie/.

For redress:

Individuals may request correction to personal information by contacting Freedom of Information Officer in the relevant Government Department.

For redress in relation to incorrect information held by An Garda Siochana (Irish Police) the Garda Criminal Records Office, Racecourse Road, Thurles, Co. Tipperary, Ireland should be contacted.

Appendix: U

Organizations:

The Governments of United States of America and the Republic of Lithuania

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Lithuania.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Lithuania is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Public information on how personal information is collected and processed is accessible through the State Register of Personal Data Controllers available on the official website of the State Data Protection Inspectorate of the Republic of Lithuania (www.ada.lt). It provides the information on each data controller and the categories of data processed by them.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Training on the use of information systems, data registers and the personal data protection regime is provided to all authorized systems users depending on their functions. All authorized system users get periodic training. Special trainings are initiated pursuant to the changes in legislation or implementing legal acts.

Correction and Redress:

Data subjects may implement right of access to his or her personal data provided for in the Law on Legal Protection of Personal Data of the Republic of Lithuania by applying to the data controller.

Points of contact for access and redress:

Police Department under the Ministry of the Interior of the Republic of Lithuania
Saltoniskiu str. 19, LT-08105 Vilnius
Tel. +370 5 271 9731, fax +370 5 271 9978
E-mail: info@policija.lt

Information Technology and Communications Department under the Ministry of the Interior of the Republic of Lithuania

Sventaragio str. 2, LT-01510 Vilnius
Tel. +370 5 271 7177, fax +370 5 271 8921
E-mail: ird@vrm.lt

In case of non-compliance the data controller to the obligation mentioned above, the data subject may complain to the State Data Protection Inspectorate of the Republic of Lithuania.

State Data Protection Inspectorate of the Republic of Lithuania
A. Juozapaviciaus str. 6
LT-09310 Vilnius
Lithuania
Tel. +370 5 279 1445
Fax +370 5 261 9494
E-mail: ada@ada.lt

Appendix: V

Organizations:

The Governments of United States of America and Croatia

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and Croatia.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from Croatia is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The Ministry of Interior just as any other data controller shall notify the data subject according to the provisions of the Personal Data Protection Act (OG 106/12 – hereinafter: PDP Act) and to the Police Duties and Powers Act (OG 76/09).

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Data protection training is provided to all authorized users.

Correction and Redress:

Data subjects may request access to personal information under the Personal Data Protection Act (PDP Act) and the Police Duties and Powers Act (OG 76/09). The data subjects need to contact the data controller's (Ministry of Interior's) data protection official to request access to their personal information.

Data subjects may also request the correction of their incomplete, inaccurate, or outdated personal information under the Personal Data Protection Act (PDP Act) and the Police Duties and Powers Act (OG 76/09). The data subjects need to contact the data controller's (Ministry of Interior's) data protection official to request such correction of data.

Point of contact for access and redress:

Ministry of Interior
Ulica grada Vukovara 33
10 000 Zagreb
Alen Canjar, Personal Data Oficial
Telephone: +385 1 6122 054
E-mail:acanjar@mup.hr

In case the data subject considers his/her rights have been infringed he/she has the right to lodge a complaint to the Croatian Personal Data Protection Agency.

Appendix: W

Organizations:

The Governments of United States of America and Slovenia

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and Slovenia.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from Slovenia is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The main systemic piece of legislation of the Republic of Slovenia regulating data protection (data privacy) is the Personal Data Protection Act of the Republic of Slovenia (of 2004, with amendments up to 2007)[58]. This Act provides for strict rules concerning the duties of data controller to prepare a filing system catalogue (Article 26), which includes, inter alia, data on the data controller, legal basis for processing personal data, description of data subjects, categories of personal data to be processed in the filing system, purpose(s) of processing, duration of storage of personal data. The Register of Filing Systems (Articles 27 and 28) with relevant information from filing systems is published at the web page Information Commissioner at: https://www.ip-rs.si/?id=159.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This

[58] The Republic of Slovenia's Personal Data Protection Act is found here: http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/PDF/zakonodaja/130730_Personal_Data_Protection_Act_of_Slovenia_status_2013_final....pdf.

documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Data protection training is provided to all authorized users.

Correction and Redress:

Individuals can ask for access to their personal data, for the purpose for which they were collected and for the users of their data at the data controller directly.

Point of contact for access and redress:

The Ministry of Interior of the Republic of Slovenia
General Police Directorate
Štefanova ulica 2
1000 Ljubljana
gp.policija@policija.si

It is also possible for data subjects to have indirect (and corrective) access to their personal data and achieve their corrections, if data are inaccurate, not up-to-date, or are processed without legal grounds or contrary to purpose(s) of processing. This indirect access can be performed via their complaint to the Information Commissioner (the national data protection supervisory body) - see Articles 53, 54 and 56 of the Personal Data Protection Act of the Republic of Slovenia. But such supervision (monitoring) and its activities and results are limited in the specific case of the PCSC Agreement - in accordance with Article 20, paragraph 2 of the PCSC Agreement.

Contact information on the Information Commissioner:

INFORMACIJSKI POOBLAŠČENEC
Zaloška cesta 59
SI-1000 LJUBLJANA
Republika Slovenija
Phone: +386(0)1 230 97 30
Fax: +386(0)1 230 97 78
Email: gp.ip@ip-rs.si
Web page: https://www.ip-rs.si/.

Appendix: X

Organizations:

U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Terrorist Screening Center (TSC).

Purpose and Use:

The Department of Homeland Security (DHS) currently uses the Terrorist Screening Database (TSDB), a consolidated database maintained by the DOJ FBI TSC, to identify information about those known or reasonably suspected of being involved in terrorist activity, or those known or reasonably suspected to have ties to those committing such activities, in order to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities. The TSC provides DHS with this data through DHS's "Watchlist Service."[59] Through this mechanism, the TSC provides DHS with near real-time synchronization of the TSDB, while ensuring the TSC remains the authoritative source of this information.

The Watchlist Service has a biographic and a biometric element. As the biometric service provider at DHS, Office of Biometric Identity Management's (OBIM) Automated Biometric Identification System (IDENT) facilitates the biometric element of the Watchlist Service. Due to technical hurdles, OBIM received TSDB information in a semi-manual way through the FBI Criminal Justice Information Services (CJIS) Division Integrated Automated Fingerprint Identification System (IAFIS). The TSC developed a mechanism to directly interface IDENT with the TSDB, which eliminates the need for IDENT to receive information through CJIS. Through this interface, IDENT will have the same synchronization capability as the Watchlist Service, but with biometric-based identities. Receiving data straight from the authoritative source in a near real-time manner will improve IDENT's ability to provide accurate, timely, and authoritative information on known or suspected terrorists to its users.

Further, because of the direct interface with IDENT, the TSC will receive timely updates from DHS about subsequent encounters of TSDB identified individuals due to IDENT's encounter notification services. IDENT checks biometrics received from the TSDB against its database of fingerprints and provides information on those matches back to the TSC, subject to filtering and dissemination rules mandated by law and policy. The TSC, and its submitting agencies, are ultimately responsible for the data quality of a TSDB record. However, as with any biometric submission to IDENT, biometric mismatches, poor quality biometrics, and splits and merges of biometric identities are reviewed by OBIM's Biometric Support Center in order to determine whether a questionable biometric match is legitimate or should be remedied. Likewise, any changes or corrections made to identities within the TSDB as the result of TSC quality control efforts promulgate to IDENT. Should an individual believe they are incorrectly impacted by this

[59] Watchlist Service PIA - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf.

exchange, they are able to submit redress requests to the appropriate mechanisms referenced in the *Correction and Redress* section below.

Individuals Impacted:

Known or Suspected Terrorists (KST) and national security threats associated with KSTs.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data:

- Known or Suspected Terrorist Identifiers;
- Fingerprint Identification Number (FIN);
- Encounter Identification Number (EID); and
- National Unique Identification Number (NUIN).

Biographic Information from Subsequent Encounter(s) including but not limited to:

- Organization, Unit, Sub-unit (OUS) (encounter owner);
- Encounter Identification Number (EID) specific to the subsequent encounter(s);
- First Name;
- Last Name;
- Date of Birth;
- Encounter Date;
- Activity Reason; and
- Activity Type.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on subsequent encounters of TSDB identified individuals is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice:

DOJ FBI TSC provides public notice on the collection of personal information through DOJ/FBI-019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073), http://www.fbi.gov/foia/privacy-act/72-fr-47073.

Retention by Partner:

For records maintained by the Terrorist Screening Database, active records are maintained for 99 years and inactive (archived) records are maintained for 50 years. Records of possible encounters with individuals in the Terrorist Screening Database are maintained for 99 years.

Compliance Reporting:

The exchange of information between the TSDB and IDENT is governed by the *Memorandum of Understanding between the Department of Homeland Security and the Terrorist Screening Center regarding the Use of Terrorist Identity Information for the Department of Homeland Security Watchlist Service* (DHS-TSC MOU). In this agreement, each party may audit handling and maintenance of their information by the receiving party to ensure compliance with any term in the agreement, including those related to privacy, security, and civil liberties. The audits can be performed at either party's discretion, but solely for the purpose of assessing compliance with the agreement.

Onward Transfer:

TSDB information incorporated into IDENT will be shared in accordance with the IDENT PIA and SORN. TSC will share terrorism information received from subsequent encounters derived from IDENT pursuant to the DHS-TSC MOU, the Intelligence Reform and Terrorism Prevention Act of 2004, and applicable legal authorities pursuant to current business processes and security measures.

Training:

TSC personnel with access to the data shared are trained in the protection and proper treatment of all data to ensure the overall safeguarding of the information, in accordance with the Privacy Act and other applicable laws and policies, including confidentiality regulations associated with particular immigration benefits.

Correction and Redress:

The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) allows travelers to submit a redress inquiry in a single request via a secure website. DHS TRIP works with the Department's component agencies, such as U.S. Customs and Border Protection, the Transportation Security Administration, and other government agencies including the Department of State and the TSC, as appropriate, to make an accurate determination about any traveler who has sought redress (See Section 7.2 of this PIA). Please see the DHS TRIP

website[60] for more information on TRIP, or to file a request for redress related to your travel screening.

The TSC does not accept redress inquiries directly from the public. Instead, members of the public should contact the relevant screening agency with their questions or concerns about screening. The screening agency is in the best position to identify and resolve issues related to that agency's screening process.

Additionally, an individual may submit redress requests directly to the OBIM Privacy Office (See Section 7.3 of this PIA).

[60] http://www.dhs.gov/dhs-trip.

Appendix: Y

Organizations:

The Governments of United States of America and the Republic of Iceland

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Iceland.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Iceland is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

The right to respect for private life and the right to the integrity of the person are protected by Art. 71 of the Constitution, and Art. 8 of the European Convention on Human Rights that is a part of Icelandic legislation with the Act on the Convention no. 64/1994.

The Data Protection Act No 77/2000, which deals with the processing of Personal Data as well as the functions of the Data Protection Authority, implements EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The purpose of the Act is to promote the practice of personal data being processed in conformity with the fundamental principles of data protection and the right to privacy. The Act applies to any automated processing of personal data and to manual processing of such data if it is, or is intended to become, a part of a file.

Article 18 of the Government Employees Act no. 70/1996 ensures that public officials with access to data preserve the confidentiality of information.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

The National Commissioner of the Police in Iceland ensures that necessary training for personnel entrusted with personal information is provided to all authorized users of the data.

Correction and Redress:

The Access to Information Act No 50/1996 and the policy on governance facilitate appropriate access to public information. The Act governs the release of records held by state and municipal administrations and private parties exercising state power that affects individual rights or obligations. It was adopted in 1996 and came into effect in 1997. Under the Act, individuals, including non-residents, and legal entities, have a legal right to documents and other materials without having to show a reason why they are asking for these documents. Individuals can obtain records that contain their personal information from public and private bodies under the Data Protection Act No 77/2000. The Act is enforced by the Data Protection Authority.

Points of Contact for Access:
Ríkislögreglustjóri
Skúlagötu 21
101 Reykjavík
Iceland

Individuals may request correction to personal information pursuant to Article 43 of the Data Protection Act No 77/2000.

Points of Contact for Redress:
Ríkislögreglustjóri
Skúlagötu 21
101 Reykjavík
Iceland

Appendix: Z

Organizations:

The Governments of United States of America and the Kingdom of Belgium

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and Belgium.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether

further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from Belgium is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 - Immigration Enforcement Operational Records System (ENFORCE) May 3, 2010, 75 FR 23274.

Partner Notice:

Belgium provides public notice on how personal data is collected and processed through the public website of the Belgian Data Protection Authority (also known as "the Privacy Commission") to whom the notification of the processing of personal data is required by the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (also known as "the Privacy Act"). The notifications are held in a registry which is published on the public website of the Privacy Commission.

Furthermore, as required by the Constitution and the Privacy Act, the rules on processing of personal data are incorporated in legal acts, such as the Police Function Act of 5 August 1992 which has been recently modified by the Police Information Management Act of 18 March 2014.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface

Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

System users of the databases are provided requisite training. Furthermore, follow up trainings are organized, if necessary, due to important modifications in the processing systems. For the police forces, there also exists an internal website providing communication concerning the processing systems and information on rules about data protection.

Correction and Redress:

As far as the police or justice databases are concerned, the Belgium legislation provides an indirect access, which means that individuals can request access to personal data concerning them by contacting the national Data Protection Authority as a single point of contact.

Point of contact for access and redress:

Commission for the Protection of Privacy
Rue de la Presse 35, 1000 Brussels

Tel. +32 (0)2 274 48 00
Fax +32 (0)2 274 48 35
E-mail: commission(at)privacycommission.be

Appendix: AA

Organizations:

The Governments of United States of America and the Republic of Bulgaria

Purpose and Use:

The purpose of the Preventing and Combating Serious Crime (PCSC) agreements is to enhance and expedite cooperation between the Parties in preventing and combating serious crime. The PCSC agreements are designed to facilitate the timely exchange of case specific information between the signatories regarding the prevention, detection, and investigation of serious criminal activities. Serious criminal activity excludes minor criminal offenses and generally may have the effect of rendering an individual inadmissible or removable from the United States. This includes inquiries at the border when an individual has been identified for further inspection.

PCSC agreements do not provide for bulk screening or bulk sharing of data. The Agreements enable the parties' national contact points to query individual fingerprint records through an automated system. In individual cases where there is a match and in compliance with the supplying country's national law, the supplying country may supply the requesting country further information to assist with law enforcement efforts in both countries. In certain cases, for example terrorism related cases, with the foreign partner's permission data may be enrolled in IDENT. The PCSC agreement can facilitate near real-time law enforcement-to-law enforcement cooperation critical to the prevention and investigation of serious crime.

Individuals Impacted:

Information will be shared on individuals that are suspected or convicted of committing serious crimes. In addition to third party nationals, this can include citizens of both the United States and the Republic of Bulgaria.

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data: Data exchanged under this project may include (but not limited to):

Name (first and last, other), Date fingerprinted, Reason fingerprinted, Location fingerprinted, Aliases, Nationality, Place of Birth, Date of Birth, Gender, Travel and Identity document information, Encounter information (Transaction-identifier data includes the sending organization; timestamp; reason sent, such as entry, visa application, credentialing application, or apprehension; and any available encounter information).

In the event of an information match, the partners may further collaborate and review the match by exchanging additional information allowable under applicable law to determine

whether further action is required using other existing protocols (law enforcement or otherwise) between the countries.

Applicable IDENT SORN Routine Uses:

This sharing of information from IDENT on matches on biometric queries from the Republic of Bulgaria is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

For queries going out from DHS, this sharing is authorized by DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) April 30, 2015 80 FR 24269.

Partner Notice:

Data subjects are informed of how personal information is collected and handled through the regulations included in the Ministry of Interior Act and the Personal Data Protection Act. Additionally, in the Ministry of Interior, there are legal acts which contain detailed regulation on the procedures for personal data processing in the framework of the ministry, e.g., "Instruction № 8121z-*1122 of 12* September 2015 on the Procedure for the Processing of Personal Data in the Ministry of Interior," which was promulgated in the State Gazette.

In the Ministry of Interior there is also a Permanent Commission for Personal Data Protection with the Minister of Interior, which deals with the data protection issues in the framework of the ministry.

Retention by Partner:

If there is no match to the initial query, all transmitted biometric information is deleted. The receiving country is required to destroy the biometric information in a secure manner and use it for no other purpose once the search against its relevant biometric systems is complete. If there is a match in the receiving country's database, the supplying country will determine whether or not sharing further information on the subject is permissible under its national law. When there is a legitimate purpose connected with a match, either country may store, process, and transmit biometric and biographical information shared through a follow-up exchange, in accordance with applicable national laws and established information retention policies.

Compliance Reporting:

Under the Agreement, the Parties are required to maintain documentation, such as audit logs of the transmission and receipt of data communicated under the Agreement. This documentation, and the systems which collect and store the subject data, will be periodically

evaluated to ensure compliance with the terms set forth in the Agreement, applicable Interface Control Documents, and any other implementing arrangements. The Parties have agreed to cooperate with each other on requests for such documentation records.

Onward Transfer:

The PCSC agreement does not permit the further communication of data provided under the Agreement to any third State, international body, or private entity without the consent of the country that provided the data and without the appropriate safeguards.

Training:

Bulgaria will provide training to all authorized system users according to their roles. The training will relate to the handling of personal information in accordance with the relevant data protection legal acts.

In the Ministry of Interior, additional trainings for the authorized system users will be periodically conducted.

The Bulgarian Commission for Personal Data Protection organizes and coordinates the training of personal data controllers in the field of personal data protection.

Correction and Redress:

Individuals can exercise their rights related to handling of their personal data, including their right to request access to their personal information, in accordance with the Ministry of Interior Act and the Personal Data Protection Act.

In this regard, individuals can address their requests both to the controller of personal data in the framework of the Ministry of Interior, or to the national data protection supervisory authority, i. e., the Bulgarian Commission for Personal Data Protection:

Ministry of Interior of the Republic of Bulgaria
Sofia 1000
29, Shesti Septemvri Str.
+35929825000 - Central Ministry of Interior

Commission for Personal Data Protection of the Republic of Bulgaria
Address: 2 Prof. Tsvetan Lazarov Blvd., Sofia 1592
Call centre - tel. 3592/91-53-518
E-mail: kzld@cpdp.bg
Website: www.cpdp.bg

Legal Affairs, Training and International Cooperation Directorate
Legal Opinions and International Cooperation Department
tel. 3592/91-53-531- international cooperation
tel. 3592/91-53-565, 3592/91-53-563- legal opinions

Legal Procedures and Supervision Directorate
Legal Procedures and Representation Department
tel. 3592/91-53-535
Control and Administrative-Penal Proceedings Department
tel. 3592/91-53-527

Appendix: BB

Organization:

United States Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM), Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division, Department of State (DOS) Bureau of Consular Affairs (CA) and the State of Texas Department of Public Safety (TXDPS).

Purpose and Use:

The purpose of IDENT latent print interoperability is to assist Federal, state, and local law enforcement agencies (LEAs) in the investigation of criminal and terrorist cases through the identification of potential suspects, criminals, and other individuals who may pose a threat to the security of the United States, as well as in the identification of missing or unknown deceased individuals, when conditions of the decedent's fingerprints do not allow for a 10-print search. DHS and DOS derive mission value from the Texas LEA investigative actions that establish a derogatory nexus to DHS or DOS populations (i.e., law enforcement, benefits, and travel/access privileges). Because a manual search for latent fingerprints can be labor intensive and time consuming, latent print interoperability will provide LEAs with increased matches and efficiencies through an automated process. As such, LEAs will be able to leverage DHS-DOJ Interoperability[61] to search latent fingerprints against fingerprints that are stored in IDENT and NGI.

OBIM is working through the TXDPS to begin latent fingerprint interoperability with Texas LEAs. The effort will allow TXDPS, in coordination with Texas State and Local Law Enforcement and other law enforcement agencies assisting in conjunction with a joint investigation or task force, to extend its latent feature and/or image search capabilities beyond the DOJ CJIS' Next Generation Identification (NGI) to include an automated search of IDENT. Texas Law Enforcement has the option to search NGI and IDENT separately or simultaneously. When searched simultaneously, the query will come to IDENT through DHS-DOJ Interoperability and retention may occur in both NGI and IDENT. OBIM anticipates the Texas latent interoperability effort will produce benefits for DHS including, but not limited to, the identification of criminal aliens for potential removal, identification of previously unknown events that may make an individual inadmissible, the confirmation and closure of certain overstay records and the closure of open immigration benefit applications.

The latent match results provided to the Texas LEA consists of a candidate list of the top 20 (or less, if 20 do not exist) unique, highest-scoring potential matches (fingerprints) authorized by DHS for automated sharing with the associated IDENT EID number. Candidate fingerprints not authorized by DHS for automated sharing, will be filtered out of the candidate list and

[61] For more information on biometric interoperability between DHS and DOJ please see: https://www.dhs.gov/sites/default/files/publications/privacy_pia_007-b-nppd_visit.pdf.

adjudicated manually by OBIM's Biometric Support Center (BSC) to determine if they are a match against the Texas LEA-submitted print. Should the OBIM BSC confirm that the Texas LEA-submitted print matches a filtered candidate, then OBIM will contact the DHS data owner of the record to seek authorization to share information on that individual with the Texas LEA.

If and when a match is confirmed by Texas Law Enforcement, it is up to the submitting Texas LEA to request more information on the individual from OBIM using the EID number provided by OBIM in the candidate list. TXDPS shall notify DHS OBIM of significant updates to TX LEA investigations that involve an identification made from an IDENT candidate list. These notifications shall occur as soon as reasonably practicable and only when the suspect has been prosecuted or cleared as a suspect in a crime. DHS shall also be notified when a case has been resolved, suspended, or terminated. DHS and DOS will use TXDPS data to establish a potential derogatory nexus to DHS or DOS population (law enforcement action, benefits, or certain access/travel privileges).

Individuals Impacted:

Texas Law Enforcement may submit latent prints from any individual, including those who are subsequently determined to be U.S. persons whose latent prints are found at the scene of a crime/event that has already occurred, or from unknown deceased individuals.

Data Elements:

Texas Law Enforcement may submit the following data elements to IDENT: Latent fingerprint images.

IDENT may return the following data elements to Texas Law Enforcement: A candidate list of the top 20 (or less, if 20 do not exist) unique highest-scoring potential matches (fingerprints) authorized by DHS for automated sharing with the associated IDENT EID number. IDENT may also return additional information to the Texas Law Enforcement after the match has been made. Such information may include, but is not limited to, full name, DOB, and FIN.

This response is provided when Texas Law Enforcement is only seeking to identify an individual. If Texas Law Enforcement seeks more information for their investigation, they will contact DHS Immigration and Customs Enforcement (ICE) who may provide additional data.

Applicable IDENT SORN Routine Uses:

This sharing between DHS and Texas is authorized by Routine Use "A" of the IDENT SORN, which states that records may be disclosed to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions as determined by DHS. Additionally, the sharing is authorized by the respective Routine

Uses "G" ("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, when 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.") of the following component source system SORNs: Border Crossing Information, Border Patrol Enforcement Records (forthcoming), Automated Targeting System, Persons Engaged in International Trade in U.S. CBP Licensed/Regulated Activities, ENFORCE, External Biometric Records (forthcoming), and USCG Law Enforcement.

Partner Notice:

As the TXDPS is not subject to the Privacy Act, it does not have a SORN covering its biometric data.

DOJ FBI CJIS provides public notice on the collection of personal information through Next Generation Identification (NGI)/FBI-009 System of Records Notice (pending release).

Retention by Partner:

For all identifications, the Texas Law Enforcement may (consistent with applicable laws and established record retention policies) retain information relating to those individuals who are under criminal investigation or identified as potential suspects in a criminal investigation as well as unknown deceased. The Texas Law Enforcement shall not retain, and will immediately destroy, all candidate fingerprints and other associated information with the fingerprints (e.g., EID) relating to those individuals who fall outside of any identification made. Furthermore, Texas Law Enforcement shall not retain any fingerprints associated with individuals who are cleared as suspects in a criminal investigation.

Compliance Reporting:

The OBIM Compliance Review Team may conduct periodic reviews as needed for compliance within the program and externally with CJIS and Texas Law Enforcement to ensure that the information is used in accordance with stated acceptable uses documented in the *Memorandum of Understanding among the Department of Homeland Security, the Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division, the Department of State Bureau of Consular Affairs and the State of Texas Department of Public Safety for Latent Fingerprint Interoperability*, hereafter called the "Latent Fingerprint Interoperability MOU."

Onward Transfer:

Texas Law Enforcement may not disseminate any information received from IDENT to third parties who are external to the state and local authorities that comprise Texas Law Enforcement, subject to the following exception: for the purposes allowed for criminal investigations, prosecutions, and identification of deceased individuals.

Before any information (including biographic and biometric information) originating from DHS's IDENT can be disclosed to a third party, defined in the Latent Fingerprint Interoperability MOU as entities that are neither Parties nor Authorized Users that seek to query or use TXDPS or IDENT data through the TXDPS or DHS for an Authorized Use, or authorized by DHS through separate agreement, TXDPS and/or TX LEAs shall contact OBIM to determine the appropriate action or response.

Training:

CJIS provides annual privacy and security training to its authorized users of IDENT data. Additionally, state and local LEAs are trained on how to appropriately handle PII according to the guidelines set forth in the Latent Fingerprint Interoperability MOU.

Correction and Redress:

To correct inaccurate or erroneous information believed to reside in IDENT, individuals may submit redress requests via email to OBIM, DHS Chief Privacy Officer, or Civil Rights and Civil Liberties at: OBIMprivacy@ice.dhs.gov, privacy@dhs.gov, or crcl@dhs.gov.

The Attorney General has exempted NGI from the contest procedures of the Privacy Act. However, the subject of the requested record may request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in subject's record or provide the information needed to make the record complete. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to FBI CJIS, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data and request that the agency verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which contributed the original information, FBI CJIS will make any changes necessary in accordance with the information supplied by that agency.

Appendix CC

U.S. Mexico Biometric Immigration Information Sharing

Background

On April 29, 2011, an Interconnection Security Agreement (ISA) was signed between Jose Francisco Blake Mora the Secretariat of Governance for the United Mexican States (SEGOB) and Janet Napolitano, the Secretary of the Department of Homeland Security (DHS). This ISA created a partnership between the Government of Mexico and DHS to "efficiently, securely, and uniformly facilitate and regulate the flow of information among relevant agencies, areas, and components", as well as to establish the individual and organizational technical security responsibilities associated with the proper protection and handling of data. On April 17, 2013, a Memorandum of Cooperation between the Department of Homeland Security and the Secretariat of Government of the United Mexican States was signed by Secretary Napolitano and Secretary of Interior Osorio Chong. The Memorandum established a new long-term partnership and solidified an associated action plan to ensure that the Government of Mexico and the United States:

- Manage efficiently the flows of travelers and focusing on third country nationals;
- Facilitate the safe repatriation of Mexican nationals;
- Combat criminal activities associated with migration flows;
- Strengthen security conditions in the border region of the United States of America and the United Mexican States;
- Prevent threats to the security of both countries; and
- Collaborate in the addressing of natural disasters and emergencies.

To ensure management of migratory flows, increased security between the two countries, border strengthening, threat prevention, and to combat criminal activities, DHS signed a Statement of Cooperation (SOC) with the Secretariat of the Governance of the United Mexican States, National Migration Institute in January of 2017. This SOC outlines the exchange of identity information associated with migratory populations and non-immigrant travelers encountered by either Government. The SOC, enabled by the aforementioned Memorandum of Cooperation and action plan, governs the exchange of biometric and biographic data between both countries to increase the safety and security of their respective nations. Both participants seek to exchange identity information on Third Country Nationals seeking authorization to travel, work or live in the United Mexican States or the United States, consistent with their respective domestic laws and policies, to:

- Enforce or administer the immigration laws of the Participants;

- Prevent, investigate, or sanction acts that would constitute a crime rendering a Third Country National inadmissible or removable under the immigration laws of the Requesting Participant; and
- Facilitate the Participants' adjudication of an application by said Third Country National for a visa, admission, or other immigration benefit, or determination of whether a person is to be ordered removed by providing information regarding the person's admissibility.

This Appendix CC-1 provides public notice about information sharing under this SOC and resulting privacy impacts.

Overview of Sharing

This biometric immigration information sharing initiative allows Mexico to submit electronic fingerprint queries to the DHS' fingerprint database, which provides interoperability with the Department of Justice (DoJ), and the Department of Defense (DoD), as described in the Overview of this PIA.[62] All biometric and associated biographic information obtained by Mexico on migrants will be enrolled in the fingerprint repository. DHS will not query the Mexico database but will instead query the Mexican holdings in IDENT. Once Mexico completes development of its biometric system, this PIA appendix will be updated to reflect the interoperable exchange of biometric queries, which is the end state goal of these interim procedures. When a biometric match is made in DHS's Automated Biometric Identification System, (IDENT), exchange and subsequent use of relevant information between the parties, listed below, may occur.

Organizations

For Mexico:

The National Institute of Migration (INM)

For the United States:

The U.S. Department of State;

The U.S. Department of Homeland Security;

The U.S. Department of Defense; and

The U.S. Department of Justice.

Purpose and Use

The purpose of this initiative is to assist in the effective administration and enforcement of the Participants' respective immigration laws. Information exchanged under this initiative will be

[62] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

used to enforce or administer those laws. DHS will not share information with third countries without the explicit consent of the providing country. The use of shared information external to the Government of Mexico is premised upon consent from DHS.

Individuals Impacted

During this present phase, the Government of Mexico will submit its collected biometric and biographic holdings, in bulk, to DHS, on behalf of the United States Government, on individuals whom they believe to be nationals of a third country (i.e., persons other than a citizen or lawful permanent resident of either the United States or the United Mexican States). Mexico will determine whether an individual is believed to be a national of a third country based on data such as application responses, identity documentation, or the nature of the application or investigation, and who have been interdicted, and detained at National Institute of Migration (INM) Migration Stations nationwide. The Government of Mexico will also make queries on individuals believed to be third country nationals and who are a subject of an admissibility inspection or investigation in order to confirm the basis for admissibility or eligibility to remain in Mexico.

Data Elements

In response to a submitted fingerprint from Mexico and subsequent match in IDENT, DHS, on behalf of the United States Government, intends to return the following data elements when legally permissible:

(a) Providing Participant subject specific reference number;

(b) Providing Participant event specific reference number;

(c) Date fingerprinted;

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Gender;

(l) Current immigration status;

(m) Other names;

(n) Alias last name(s);

(o) Alias first name(s);

(p) Travel document number;

(q) Travel document type;

(r) Travel document issuing authority/country;

(s) Travel document expiry date;

(t) Reason for alert;[63]

(u) Visa Refusal code;

(v) Watchlist Indicator;[64]

(w) Scan of travel document biodata page;

(x) Scan of other marked travel document pages;

(y) Facial image;

(z) Previous immigration status;

(aa) Date removed;

(bb) Date of arrival;

(cc) Location of arrival;

(dd) Date of departure;

(ee) Location of departure;

(ff) Date of immigration application or non-biometric encounter;

(gg) Type of immigration application or non-biometric encounter;

(hh) Date of outcome of immigration application;

(ii) Outcome of immigration application;

(jj) Reason for outcome of immigration application; and

(kk) Expiry date of current leave/stay or visa.

---

[63] Alerts are from the DHS enforcement process where a flag has been placed on a person primarily as a Recidivist. "Recidivist with alert" categories include categories for officer safety, smuggling, and individuals flagged for expedited removal.

[64] For purposes of this sharing, "watchlist indicator" is an indication of derogatory information held in IDENT. For a full description of the IDENT watchlist, please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012) at page 6, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.

Such exchanges may be manual or automated depending upon the IT capabilities of the respective parties (specifically, the United States will employ IDENT; the United Mexican States will employ, variously, manual reporting through the United States Embassy representation in Mexico City, Mexico, and a future automated system that is currently under development).

Applicable SORN Routine Uses

Biometrics/Biographic Information

DHS/USCIS-001 Alien File, Index, and National File Tracking SORN[65]

> Routine Use H: To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws.

DHS/USCIS-003 Biometric Storage System SORN[66]

> Routine Use F: 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.

DHS/CBP-006 Automated Targeting System (ATS) SORN[67] (*for legacy NSEERS data only*[68])

> Routine Use G: To appropriate federal, state, tribal, local, 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, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws.

---

[65] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, 78 FR 69864 (Nov. 21, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-11-21/html/2013-27895.htm.

[66] DHS/USCIS-003 Biometric Storage System SORN, 72 FR 17172 (April 6, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-04-06/html/07-1643.htm.

[67] DHS/CBP-006 Automated Targeting System (ATS) SORN, 77 FR 30297 (May 22, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

[68] NSEERS was first implemented in 2002 as a temporary measure in the aftermath of the September 11, 2001 terrorist attacks and was designed to record the arrival, stay, and departure of individuals from certain countries chosen based on an analysis of possible national security threats emanating from those locales. DHS officially ended the NSEERS program in 2011. DHS is sharing this information in the same manner as all other entry-exit information. Any match to individuals who were required to register under NSEERS should not be treated as derogatory information absent any other information. For additional information, please *see* http://www.dhs.gov/dhs-removes-designated-countries-nseers-registration-may-2011.

DHS/CBP-007 Border Crossing Information (BCI) SORN[69]

> Routine Use G. 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, when 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.
>
> Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-023 Border Patrol Enforcement Records (BPER) SORN[70]

> Routine Use G. 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, when 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.
>
> Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS/CBP believes the information would assist in the enforcement of applicable civil or criminal laws.

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN[71]

> Routine Use G: To an appropriate federal, state, local, tribal, territorial, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation, enforcing, or implementing a law, rule, regulation, or order,

---

[69] DHS/CBP-007 Border Crossing Information (BCI), 81 FR 4040 (Jan. 25, 2016), *available at* http://www.regulations.gov/?D=DHS-2016-0006-0001.
[70] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (Oct. 20, 2016) available at https://www.regulations.gov/document?D=DHS-2016-0067-0001.
[71] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016), *available at* https://www.regulations.gov/document?D=DHS_FRDOC_0001-1513.

when 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.

Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

Derogatory Information

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN,[72]

Routine Use G: To an appropriate federal, state, local, tribal, territorial, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation, enforcing, or implementing a law, rule, regulation, or order, when 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.

Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

DHS/CBP-011 U.S. Customs and Border Protection (TECS) SORN[73]

Routine Use G: 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.

[72] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records 81 FR 72080 (Oct. 19, 2016), *available at* https://www.regulations.gov/document?D=DHS_FRDOC_0001-1513.
[73] DHS/CBP-011 TECS SORN, 73 FR 77778 (Dec. 19, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

Transactional Information

DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) SORN[74]

> Routine Use A: To appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions.

Partner Notice

The Government of Mexico, consistent with its domestic laws including its Constitution, its Federal Law on the Protection of Personal Data, provides notice of collection, purpose, and use to the third country nationals from whom it obtains biometric and biographic information.

Retention

The United States will retain all biographic and biometric data associated with submissions from Mexico only so long as necessary for the purpose of the effective administration and enforcement of its respective immigration laws, in accordance with its applicable retention and disposition schedules and respective domestic laws, but in no instance will information be retained for longer than 75 years from the date of enrollment.

The Government of Mexico National Institute of Migration (INM) will retain all biographic data shared by the United States as a result of a biometric query only so long as necessary for the purpose of the effective administration and enforcement of its respective immigration laws, in accordance with its applicable retention and disposition schedules and respective domestic laws, but in no instance will information be retained for longer than 75 years from the date of enrollment.

Review and Performance Monitoring

The Participants will 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:

- The number and severity of any *security* breaches and a summary of remedial actions taken, and
- The number and severity of any *privacy* breaches and a summary of remedial actions taken.

The Participants will carry out regular quality assurance activities, including a review of applicable privacy safeguards. For Mexico, quality assurance activities will be carried out by the Government of Mexico National Institute of Migration (INM). For the United States, quality assurance activities will be carried out by the Office of Biometric Identity Management (OBIM).

---

[74] DHS/NPPD/USVISIT-004 Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm.

These activities may include, but are not limited to, determining:

- Whether information has been retained when it should have been deleted and destroyed;
- Whether information has been disclosed in a manner inconsistent with the Agreement and U.S. law; and
- The number of correction requests and whether information has been corrected in a manner consistent with the Agreement.

Access, Correction, and Redress

Individuals who wish to access response data held by the Government of Mexico may make a special request involving the following contact methods:

Mail Request for Information
Instituto Nacional de Migración
Calle Homero 1832
Los Morales Polanco, Del. Miguel Hidalgo, Ciudad de México. C.P. 11510

Telephone: 53872400
Attention to Citizenship: 01 800 00 46264
National Institute of Migration (Instituto Nacional de Migración)

Similarly, individuals who wish to access response data held by the U.S. Department of Homeland Security may submit a request as follows:

http://www.dhs.gov/freedom-information-act-and-privacy-act or
Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
245 Murray Lane SW, STOP-0655
Washington, D.C. 20528-0655

Individuals who wish to correct response data held by the Government of Mexico, or to request to add a notation to indicate a correction request was made, may submit a correction request to:

Mail Request for Information
Instituto Nacional de Migración
Calle Homero 1832
Los Morales Polanco, Del. Miguel Hidalgo, Ciudad de México. C.P. 11510

Individuals who wish to correct response data held by the Government of the United States, or to request to add a notation to indicate a correction request was made, may submit a correction request to the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP):

http://www.dhs.gov/dhs-trip, or:
United States Department of Homeland Security
Traveler Redress Inquiry Program (DHS TRIP)

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

Correction requests, or requests to add a notation to indicate a correction request was made, may also be directed to:

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

The DHS Office of Citizenship and Immigration Services Ombudsman also assists individuals who wish to resolve issues regarding applications submitted 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
cisombudsman@dhs.gov

Privacy Risks and Mitigation

Information exchanged under this program will be done in accordance with the Participants' respective laws and policies. In addition to risks and mitigations already addressed in the IDENT PIA[75], the following are specific risks associated with the biometric visa and immigration information sharing program:

Privacy Risk: Although the Agreement prohibits sharing information about U.S. citizens, nationals, and LPRs, or Mexican citizens and permanent residents, there is a risk that the Participants may unintentionally exchange this information.

Mitigation: The Government of Mexico intends to send queries only on individuals believed to be third country nationals based on data such as identity documentation provided, verbal admission by the migrant, or reasonable assertion. Uintentional sharing could happen if the individual withholds information from the Government of Mexico that indicates he or she is a citizen, resident, or national, as applicable, of the United States or Mexico. In this instance, the individual would be able to employ the redress provisions of the SOC to seek removal of her or his information.

To mitigate this privacy risk:

[75] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (Dec. 7, 2012) at page 7, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.

- The United States will not return information on individuals believed to be U.S. citizens, nationals, and LPRs, or permanent residents.
- Response data associated with biometric matches to submissions from the Government of Mexico will be returned to the Government of Mexico in an automated fashion. The IDENT system will be configured to automatically filter out encounters, identities, and derogatory information types that are not able to be shared in accordance with the SORNs listed above, or that would be inconsistent with US law or DHS policy.
- DHS has limited the categories of information that it will return to only those that have been identified as unlikely to include U.S. citizens, nationals, and LPRs.
- These exchanges will undergo review and performance monitoring to ensure that information is exchanged in accordance with the Agreement. While Mexico may inadvertently send queries of U.S. citizens, nationals, and LPRs, DHS will review the responses it provides to these queries and make adjustments as necessary to exclude any further exchanges of information likely to be out of scope of the Agreement.

Additional privacy risks first mentioned in the original IDENT PIA are particularly applicable to this information sharing initiative. There is a risk of sharing IDENT data with foreign partners, where it is more difficult for DHS to externally impose the same controls that govern the data internally. These risks are mitigated by those foreign partners' audit and redress provisions, which are identified in the process of negotiating a data sharing agreement. This Appendix details how individuals may contact the United States or Mexico for redress options. Also noted above, the Participants will conduct regular quality assurance checks on data exchanged.

Finally, there is also the risk of DHS disclosing information about special, legally protected classes of individuals inappropriately and illegally. IDENT contains information related to aliens who receive special legal protections generally prohibiting disclosure.[76] IDENT has technological filters in place that check if a record belongs to an individual in a protected class (VAWA, T, or U visa holders, asylum or refugee applicants[77] or Temporary Protected Classes (TPS)). If so, the record is filtered out from the response that is sent to the foreign partner.

---

[76] *See* 8 U.S.C. § 1367, 8 C.F.R § 208.6, 8 U.S.C. § 1255A(c)(5), 8 U.S.C. § 1160(b)(6), 8 U.S.C. § 1255A(c)(5), and 8 U.S.C. § 1160(b)(6). For more U.S. regulatory restrictions, *see also* DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 27, 2017), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[77] Information protected by 8 C.F.R. 208.6 may only be disclosed to a foreign government pursuant to a Secretarial Waiver. See also DHS Delegation 08505, "Delegation of Authority to Disclose Asylum and Refugee Data" dated 6/22/16 delegating limited authority to disclose asylum and refugee information to the Under Secretary for Intelligence and Analysis, the Assistant Secretary of United States Citizenship and Immigration Services, the Commissioner of U.S. Customs and Border Protection, the Director of United States Immigration and Customs Enforcement, and the Director of Operations Coordination for counterterrorism and intelligence purposes.

Appendix DD

U.S. Guatemala Biometric Immigration Information Sharing

Background

In May of 2019, a Memorandum of Cooperation (MOC) between the Department of Homeland Security (DHS) and the Ministry of Government of the Republic of Guatemala on Security Activities That Make It Possible to Address Irregular Migration was signed between Enrique A. Degenhart Asturias, Minister of Government for the Ministry of Government of the Republic of Guatemala and Kevin McAleenan, the Acting Secretary of the DHS. This MOC created a partnership between the Government of Guatemala (GOG) and DHS to cooperate on matters pertaining to:

- Border security, in order to reduce irregular migratory flows;
- Necessary training, in order to improve criminal investigations;
- Necessary concrete actions to counteract human trafficking and human smuggling; the interdiction of illicit drug trafficking; illegal trade in firearms, ammunition and explosives and illicit financial flows; and
- Necessary preparation, in order to improve the capacity to identify, manage and attend to irregular migrants.

In addition to the MOC, the Guatemalan Ministry of Government and DHS signed a Memorandum of Understanding (MOU) on Enhancing Cooperation to Prevent and Combat Crime and Other Threats to Public Security on August 22, 2019. The purpose of this MOU is to assist in the effective administration and enforcement of the respective immigration, migration, and criminal laws of the GOG and the United States.

In furtherance of these goals, DHS and the GOG will exchange identity information associated with migratory populations and non-immigrant travelers encountered by either Government in the course of their legally-authorized missions and activities. This exchange of biometric and biographic data between both countries will seek to increase the safety and security of their respective nations. Both DHS and the Ministry of Government seek to exchange identity information on third country nationals seeking authorization to travel, work, or live in the Republic of Guatemala, consistent with their respective domestic laws and policies, to:

- Administer or enforce the respective immigration and migration laws of the Participants;
- Further the prevention, detection, or investigation of acts that would constitute a crime under the laws of either Participant; and

- Facilitate a Participant's determination of eligibility for a visa, admission, protection, or other immigration or migration benefit, or of whether there are grounds for removal.

This Appendix DD provides public notice about information sharing under this MOC and resulting privacy impacts.

Overview of Sharing

This biometric immigration information sharing initiative allows the GOG to submit electronic fingerprint-based queries, additional biometric information (such as iris and face images), the nature of the encounter, transactional metadata, and any other information that may be determined to be appropriate, to DHS' Automated Biometric Identification System (IDENT) and its successor system, the Homeland Advanced Recognition Technology (HART)[78] biometric databases.[79] DHS will notify the GOG whether it has records that match to the fingerprint-based query, and will share relevant personal information, as discussed below. The GOG may subsequently provide additional information that was not included in the original query, such as additional biometric data.

All biometric and associated biographic information obtained by the GOG on migrants will be enrolled, based on fingerprints, in IDENT/HART. At this initial stage of the information sharing initiative, DHS will not query any Guatemalan fingerprint database but will instead query the enrolled Guatemalan holdings retained in IDENT/HART. Once the GOG completes development of a biometric system capable of conducting interoperable query-response exchanges, or in the event that the GOG and DHS agree to conduct queries based on biometric modalities other than fingerprints, DHS will update the appropriate privacy compliance documentation.

Organizations

For Guatemala:

The Ministry of Government Institute of Migration

For the United States:

The U.S. Department of Homeland Security

Purpose and Use

The purpose of this initiative is to assist in the effective administration and enforcement of the Republic of Guatemala's and the United States' immigration, migration, and criminal

[78] Homeland Advance Recognition Technology (HART) system will be replacing IDENT. *See* forthcoming HART Increment 1 PIA *available at* www.dhs.gov/privacy.
[79] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy. In the future, the IDENT PIA will be retired and replaced by an International Biometric Interoperability PIA which will describe the privacy risks of sharing biometric information as part of the BDSP.

laws. Information exchanged under this initiative will be used to enforce or administer those laws. The participants will not share information with third countries or other third parties without the explicit consent of the providing country. DHS will not share any biographic or biometric information associated with these submissions with any of IDENT/HART's international partners, except for the GOG.

Individuals Impacted

During this present phase, the GOG will submit its collected biometric and biographic holdings, in bulk or in individual queries, to DHS (acting on behalf of the United States Government) on individuals whom the Republic of Guatemala believes to be nationals of a third country (i.e., persons other than a citizen or lawful permanent resident of either the United States or the Republic of Guatemala). All collections of information will occur in Guatemala.

The Republic of Guatemala will determine whether an individual is believed to be a national of a third country based on information such as application responses, identity documentation, or the nature of the application or investigation, and the fact that an individual was interdicted and detained at facilities operated by the Ministry of Government in Guatemala. In particular, the Guatemalan Institute of Migration (GIM), the Guatemalan agency responsible for managing migration and immigration matters, will collect biometric information on individuals transiting the territory of Guatemala in accordance with its applicable authorities.[80]

The GOG will also make queries on individuals believed to be third country nationals and who are a subject of an admissibility inspection or investigation in order to confirm the basis for admissibility or eligibility to remain in Guatemala. In the case of Guatemala and under the context of the MOC, a third country national can be defined as any individual that is not a known citizen of the GOG or a citizen of the United States of America.

Data Elements

In response to a submitted fingerprint from Guatemala and subsequent match in IDENT, DHS, on behalf of the United States Government, intends to return the following data elements when legally permissible:

(a) Providing Participant subject specific reference number;

(b) Providing Participant event specific reference number;

(c) Date fingerprinted;

[80] While the Guatemalan Institute of Migration (*Instituto Guatemalteco de Migración*, in Spanish), or GIM, is a component agency of Guatemala's Ministry of Government, GIM will soon become an independent agency within the Government of Guatemala due to recent changes to Guatemalan law. The MOC and associated arrangements between the United States and the Government of Guatemala will continue to apply to GIM and any of its successor agencies. *See* http://igm.gob.gt/.

(d) Reason fingerprinted;

(e) Location fingerprinted;

(f) Last name;

(g) First name;

(h) Date of birth;

(i) Passport nationality;

(j) Country of birth;

(k) Sex;

(l) Current immigration status;

(m) Other names;

(n) Alias last name(s);

(o) Alias first name(s);

(p) Travel document number;

(q) Travel document type;

(r) Travel document issuing authority/country;

(s) Travel document expiry date;

(t) Reason for alert;[81]

(u) Visa Refusal code;

(v) Watchlist Indicator;[82]

(w) Scan of travel document biodata page;

(x) Scan of other marked travel document pages;

(y) Facial image;

(z) Previous immigration status;

---

[81] Alerts are from the DHS enforcement process where a flag has been placed on a person primarily as a Recidivist. "Recidivist with alert" categories include categories for officer safety, smuggling, and individuals flagged for expedited removal.

[82] For purposes of this sharing, "watchlist indicator" is an indication of derogatory information held in IDENT/HART. For a full description of the IDENT watchlist, please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012) at page 6, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf. The HART system will be replacing IDENT. *See* forthcoming HART Increment 1 PIA *available at* www.dhs.gov/privacy.

(aa) Date removed;

(bb) Date of arrival;

(cc) Location of arrival;

(dd) Date of departure;

(ee) Location of departure;

(ff) Date of immigration application or non-biometric encounter;

(gg) Type of immigration application or non-biometric encounter;

(hh) Date of outcome of immigration application;

(ii) Outcome of immigration application;

(jj) Reason for outcome of immigration application; and

(kk) Expiry date of current leave/stay or visa.

Such exchanges may be manual or automated depending upon the information technology capabilities of the respective participants (specifically, the DHS will employ IDENT/HART; the GOG will employ various manual reporting through the U.S. Embassy Guatemala City and a future automated system that is currently under development).

Applicable SORN Routine Uses

Biometrics/Biographic Information

DHS/ALL-041 External Biometric Records SORN[83]

> Routine Use H. 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, when 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.

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN[84]

> Routine Use H: To appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or

[83] DHS/ALL-041 External Biometrics Records SORN, 83 FR 17829 (April 24, 2018), *available at*: www.dhs.gov/privacy.
[84] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, 82 FR 43556 (Sept. 18, 2017), *available at* www.dhs.gov/privacy.

prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws.

DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records SORN[85]

Routine Use H: 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, when 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.

DHS/CBP-006 Automated Targeting System (ATS) SORN[86] (*for legacy NSEERS data only*[87])

Routine Use G: To appropriate federal, state, tribal, local, 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, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-007 Border Crossing Information (BCI) SORN[88]

Routine Use G. 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, when 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.

---

[85] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018), *available at* www.dhs.gov/privacy.
[86] DHS/CBP-006 Automated Targeting System (ATS) SORN, 77 FR 30297 (May 22, 2012), *available at* www.dhs.gov/privacy.
[87] NSEERS was first implemented in 2002 as a temporary measure in the aftermath of the September 11, 2001 terrorist attacks and was designed to record the arrival, stay, and departure of individuals from certain countries chosen based on an analysis of possible national security threats emanating from those locales. DHS officially ended the NSEERS program in 2011. DHS is sharing this information in the same manner as all other entry-exit information. Any match to individuals who were required to register under NSEERS should not be treated as derogatory information absent any other information. For additional information, please *see* http://www.dhs.gov/dhs-removes-designated-countries-nseers-registration-may-2011.
[88] DHS/CBP-007 Border Crossing Information (BCI), 81 FR 4040 (Jan. 25, 2016), *available at* www.dhs.gov/privacy.

Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS believes the information would assist enforcement of applicable civil or criminal laws.

DHS/CBP-023 Border Patrol Enforcement Records (BPER) SORN[89]

Routine Use G. 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, when 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.

Routine Use H. To appropriate federal, state, tribal, local, 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, or license, when DHS/CBP believes the information would assist in the enforcement of applicable civil or criminal laws.

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN[90]

Routine Use G: To an appropriate federal, state, local, tribal, territorial, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation, enforcing, or implementing a law, rule, regulation, or order, when 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.

Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

[89] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (Oct. 20, 2016), *available at* www.dhs.gov/privacy.
[90] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016), *available at* www.dhs.gov/privacy.

Derogatory Information

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN,[91]

> Routine Use G: To an appropriate federal, state, local, tribal, territorial, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation, enforcing, or implementing a law, rule, regulation, or order, when 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.
>
> Routine Use M: To foreign governments for the purpose of coordinating and conducting the removal of aliens from the United States to other nations under the Immigration and Nationality Act (INA); and to international, foreign, intergovernmental, and multinational agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

DHS/CBP-011 U.S. Customs and Border Protection (TECS) SORN[92]

> Routine Use G: 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.

Transactional Information

DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) SORN[93]

> Routine Use A: To appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, where consistent with a DHS mission-related function as determined by DHS.

Partner Notice

---

[91] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records 81 FR 72080 (Oct. 19, 2016), *available at* www.dhs.gov/privacy.
[92] DHS/CBP-011 TECS SORN, 73 FR 77778 (Dec. 19, 2008), *available at* www.dhs.gov/privacy.
[93] DHS/NPPD/USVISIT-004 Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007), *available at* www.dhs.gov/privacy. Please note that OBIM is replacing the IDENT SORN with the Enterprise Biometrics Administrative Records (EBAR) SORN. *See* forthcoming EBAR SORN *available at* www.dhs.gov/privacy.

The GOG, consistent with its domestic laws including its Constitution and its Law of Access to Public Information,[94] provides notice of collection, purpose, and use to the third country nationals from whom it obtains biometric and biographic information.

Retention

The United States will retain all biographic and biometric data associated with submissions from the GOG in accordance with the Section 6 on Retention and further use of Query Data in the MOU and only so long as necessary for the purpose of the effective administration and enforcement of its respective immigration laws, in accordance with its applicable retention and disposition schedules and respective domestic laws, but in no instance will information be retained for longer than 75 years from the date of enrollment.

The GOG will retain all biographic data shared by the United States as a result of a biometric query in accordance with the MOU and only so long as necessary for the purpose of the effective administration and enforcement of its respective immigration laws, in accordance with its applicable retention and disposition schedules and respective domestic laws, but in no instance will information be retained for longer than 75 years from the date of enrollment.

Review and Performance Monitoring

The Participants will 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:

- The number and severity of any *security* breaches and a summary of remedial actions taken, and
- The number and severity of any *privacy* breaches and a summary of remedial actions taken.

The Participants will carry out regular quality assurance activities, including a review of applicable privacy safeguards. For Guatemala, quality assurance activities will be carried out by the Ministry of Government. For the United States, quality assurance activities will be carried out by the DHS Office of Biometric Identity Management (OBIM). These activities may include, but are not limited to, determining:

- Whether information has been retained when it should have been deleted and destroyed;

[94] https://www.right2info.org/resources/publications/laws-1/Guatemala_Decreto%2057-2008%20Ley%20Acceso%20Informacion%20Publica.pdf.

- Whether information has been disclosed in a manner inconsistent with the Agreement and U.S. law; and
- The number of correction requests and whether information has been corrected in a manner consistent with the Agreement.

Access, Correction, and Redress

Individuals who wish to access response data held by the GOG may make a special request involving the following contact methods:

Mail Request for Information
Migración de Guatemala
CA-2, Ciudad Pedro de Alvarado, Guatemala
Telephone: +502 2411 2411

Similarly, individuals who wish to access response data held by the U.S. Department of Homeland Security may submit a request as follows:

http://www.dhs.gov/freedom-information-act-and-privacy-act or
Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
245 Murray Lane SW, STOP-0655
Washington, D.C. 20528-0655

Individuals who wish to correct response data held by the GOG, or to request to add a notation to indicate a correction request was made, may submit a correction request to:

Mail Request for Information
Migración Dirreccion General de Migracion
6th Avenida 3-11 Zona 4, Guatemala, Guatemala
PBX (502) 2411-2411
Postal Code: 01004

Individuals who wish to correct response data held by the Government of the United States, or to request to add a notation to indicate a correction request was made, may submit a correction request to the DHS Traveler Redress Inquiry Program (DHS TRIP):

http://www.dhs.gov/dhs-trip, or:
United States Department of Homeland Security
Traveler Redress Inquiry Program (DHS TRIP)
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

Correction requests, or requests to add a notation to indicate a correction request was made, may also be directed to:

Chief Privacy Officer

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

The DHS Office of Citizenship and Immigration Services Ombudsman also assists individuals who wish to resolve issues regarding applications submitted 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
cisombudsman@dhs.gov

Privacy Risks and Mitigation

Information exchanged under this program will be done in accordance with the Participants' respective laws and policies. In addition to risks and mitigations already addressed in the IDENT PIA[95], the following are specific risks associated with the biometric visa and immigration information sharing program:

Privacy Risk: Although this program will not permit sharing information about U.S. citizens, U.S. nationals, and Lawful Permanent Residents (LPR) of the United States, or Guatemalan citizens and permanent residents of Guatemala, there is a risk that the Participants may unintentionally exchange this information.

Mitigation: This risk is not mitigated. The Republic of Guatemala and the United States intend to send queries only on individuals believed to be third country nationals based on data such as identity documentation provided, verbal admission by the migrant, or reasonable assertion. Both Guatemala and the United States have determined that they will not intentionally submit biometric queries on Guatemalan or U.S persons provided that Guatemalan or U.S. nationality is verified through a valid passport or other identification document. Unintentional sharing could happen if the individual misrepresents or withholds information from the Republic of Guatemala or the United States that indicates he or she is a citizen, resident, or national, as applicable, of the United States or Guatemala. In this instance, the individual would be able to

[95] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (Dec. 7, 2012) at page 7, *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf. Please note that the Homeland Advance Recognition Technology (HART) system will be replacing IDENT. *See* forthcoming HART Increment 1 PIA *available at* www.dhs.gov/privacy.

employ the redress provisions established under Section 10 of the MOU to seek Correction, Blockage, an Deletion of data.

OBIM will not return information on individuals believed to be U.S. citizens, nationals, and LPRs. OBIM maintains encounter filtering by Organization/Unit/Subunit (O/U/S) to prevent encounter data that is not permissible to be shared or sanctioned to be returned by DHS. Encounter filtering uses configuration settings to filter encounters from responses being returned using the designated activity category stored in the Activity Type field. Encounter filtering considers both the O/U/S and Activity Type of the requestor and data provider when making a sharing determination. OBIM also does identity level flagging and filtering which establishes the capability for an O/U/S to submit a flag indicating that an individual belongs to a defined population, either during the process of encounter enrollment or separately to add or update an existing encounter. This flag acts to filter an individual's entire identity, including every encounter that exists for them in IDENT/HART, from a requesting O/U/S that is unauthorized from receiving information on (including the existence of) identities belonging within that population. Unauthorized requestors will receive a response indicating that there was no match to the identity.

DHS has developed business rules to limit the categories of information that OBIM will return to the Ministry of Government in accordance with applicable international and domestic law and relevant policies, and will include datasets that are unlikely to include U.S. citizens, nationals, and LPRs. Response data associated with biometric matches to submissions from the GOG will be returned to the GOG in an automated fashion in accordance with these business rules and identity level flagging and filtering capabilities in IDENT. The IDENT system will be configured to automatically filter out encounters, identities, and derogatory information types that are not able to be shared in accordance with the SORNs listed above, or that would be inconsistent with US law or DHS policy.

OBIM maintains encounter filtering by Organization/Unit/Subunit to prevent encounter data from being returned that is not sanctioned by DHS. Encounter filtering removes USC heavy encounter types from the response to the foreign partner. IDENT contains information related to aliens who receive special legal protections generally prohibiting disclosure.[96] IDENT has technological filters in place that check if a record belongs to an individual in a special protected class (SPC) (Violence Against Women Act (VAWA), Human Trafficking (T), or Victims of Criminal Activity (U) visa holders, asylum or refugee applicants[97] or Temporary Protected

[96] See 8 U.S.C. § 1367, 8 C.F.R § 208.6, 8 U.S.C. § 1255A(c)(5), 8 U.S.C. § 1160(b)(6), 8 U.S.C. § 1255A(c)(5), and 8 U.S.C. § 1160(b)(6). For more U.S. regulatory restrictions, see also DHS Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 27, 2017), available at https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[97] Information protected by 8 C.F.R. 208.6 may only be disclosed to a foreign government pursuant to a Secretarial Waiver. See also DHS Delegation 08505, "Delegation of Authority to Disclose Asylum and Refugee Data" dated

Classes (TPS)). and Special Agricultural Worker (SAW)/Legal Immigration Family Equity (LIFE). Identity flagging and filtering blocks the entirety of the identity from being returned to a foreign partner in a response once identified by U.S. Citizenship and Immigration Services (USCIS)as a SPC.

These exchanges will undergo review and performance monitoring to ensure that information is exchanged in accordance with the Agreement. While the GOG may inadvertently send queries of U.S. citizens, nationals, and LPRs, OBIM will review the responses it provides to these queries and make adjustments as necessary to exclude any further exchanges of information likely to be out of scope of the [A]MOC.

Additional privacy risks first mentioned in the IDENT PIA are particularly applicable to this information sharing initiative. There is a risk of sharing IDENT/HART data with foreign partners, where it is more difficult for DHS to externally impose the same controls that govern the data internally. These risks are mitigated by those foreign partners' transparency, audit, and redress provisions, which are identified in the process of implementing a data sharing agreement. In particular, this includes the Republic of Guatemala's Open Government Initiative, which has culminated in a government-wide action plan which will address, among other things, government accountability and citizen participation.[98] This Appendix details how individuals may contact the United States or Guatemala for redress options. Also noted above, the Participants will conduct regular quality assurance checks on data exchanged.

Ultimately, the operational and technical controls put in place by DHS will limit the dissemination or sharing of U.S. person data under this program, if information confirming U.S. person status is available at the point of biometric collection. Some privacy risk may remain because some individuals may take steps to hide or misrepresent their citizenship status or other identifying information.

Privacy Risk: There is a risk that the information provided by Guatemala is inaccurate.

Mitigation: This risk is unmitigated. Guatemala will provide the biometric and biographic information to DHS, and DHS will have no independent means of confirming the accuracy. IDENT/HART system users will have the choice to access information provided by Guatemala and to make decisions based on that information. Annual reviews and performance monitoring may build confidence in data accuracy and reliability.

6/22/16 delegating limited authority to disclose asylum and refugee information to the Under Secretary for Intelligence and Analysis, the Assistant Secretary of United States Citizenship and Immigration Services, the Commissioner of U.S. Customs and Border Protection, the Director of United States Immigration and Customs Enforcement, and the Director of Operations Coordination for counterterrorism and intelligence purposes.

[98] Guatemala se une a Gobierno Abierto, http://gobiernoabierto.gob.gt/gobierno-abierto-en-guatemala-2/ (last accessed August 23, 2019).

Privacy Risk: Finally, there is also the risk of DHS disclosing information about special, legally protected classes of individuals inappropriately and illegally.

Mitigation: IDENT/HART contains information related to aliens who receive special legal protections generally prohibiting disclosure.[99] As noted above, the DHS will implement business rules to prevent the transmission of information that cannot be lawfully transmitted to the Ministry of Government. OBIM maintains encounter filtering by Organization/Unit/Subunit to prevent encounter data from being returned that is not sanctioned by DHS. Encounter filtering removes USC heavy encounter types from the response to the foreign partner. IDENT contains information related to aliens who receive special legal protections generally prohibiting disclosure.[100] IDENT has technological filters in place that check if a record belongs to an individual in a special protected class, VAWA, T, or U visa holders, asylum or refugee applicants,[101] TPS, or SAW/LIFE. Identity flagging and filtering blocks the entirety of the identity from being returned to a foreign partner in a response once identified by USCIS as a SPC.

OBIM's Biometric Support Center (BSC) has a Standard Operating Procedure that requires BSC operators to manually check USCIS systems for Section 1367 protected status before sharing information based on a latent fingerprint match. However, this disclosure is on an automated basis through IDENT/HART. OBIM asserts that IDENT/HART's automated data sharing settings, known as the Data Access and Security Controls (DASC), directly implement Section 1367 confidentiality provisions.

---

[99] *See* 8 U.S.C. § 1367, 8 C.F.R § 208.6, 8 U.S.C. § 1255A(c)(5), 8 U.S.C. § 1160(b)(6), 8 U.S.C. § 1255A(c)(5), and 8 U.S.C. § 1160(b)(6). For more U.S. regulatory restrictions, *see also* DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 27, 2017), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[100] See 8 U.S.C. § 1367, 8 C.F.R § 208.6, 8 U.S.C. § 1255A(c)(5), 8 U.S.C. § 1160(b)(6), 8 U.S.C. § 1255A(c)(5), and 8 U.S.C. § 1160(b)(6). For more U.S. regulatory restrictions, see also DHS Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 27, 2017), available at https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[101] Information protected by 8 C.F.R. 208.6 may only be disclosed to a foreign government pursuant to a Secretarial Waiver. See also DHS Delegation 08505, "Delegation of Authority to Disclose Asylum and Refugee Data" dated 6/22/16 delegating limited authority to disclose asylum and refugee information to the Under Secretary for Intelligence and Analysis, the Assistant Secretary of United States Citizenship and Immigration Services, the Commissioner of U.S. Customs and Border Protection, the Director of United States Immigration and Customs Enforcement, and the Director of Operations Coordination for counterterrorism and intelligence purposes.