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.

<u>DoS/CA submits the following data elements:</u>

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.

<u>DoS/CA receives the following data elements from IDENT</u>:

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 "H" 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.

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.

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

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 "H" 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: 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[2] (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 "H" 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.

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.

---

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

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.[3] 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.

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.

[3] 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.

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 "H" 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 "H" 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 "H" 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 "H" 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 "H" 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 "H" 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)[4]. 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 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.

---

[4] 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.

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."[5] 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 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.

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

Data Elements:

Biometric data: digital facial photograph and fingerprints

Biographic data:

- Known or Suspected Terrorist Identifiers
- Fingerprint Identification Number (FIN)
- Encounter Identification Number (EID)
- 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
- 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[6] 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).

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