


# MIGRATION5

Security · Service · Savings 

## **STATEMENT OF INTENT AMONG THE PARTNERS OF THE MIGRATION FIVE (M5) FOR NOTIFICATION REGARDING BILATERAL SECURE REAL-TIME PLATFORM ACTIVITY**

The Partners of the M5, which include the agencies primarily responsible for the administration and enforcement of immigration laws for the Government of Australia, the Government of Canada, the Government of New Zealand, the Government of the United Kingdom, and the Government of the United States, (hereinafter referred to individually as "Participant" or "M5 Partner", or collectively as "the Participants" or "M5 Partners"),

Seeking to close gaps in M5 Partners' access to information that bilateral arrangements have not addressed;

Mindful that many of the bilateral agreements or arrangements between M5 Partners for systematic sharing of visa and immigration information include provisions establishing the parameters of onward disclosure of information to third-party governments.

Mindful that this Statement of Intent will not create, maintain or govern legally binding rights or obligations between the M5 Partners.

Hereby express their mutual intent as follows:

1. The Participants have jointly decided that, when responding to a Secure Real-Time Platform biometric query from an M5 Partner, wherever practicable, the responding M5 Partner intends to identify any additional M5 Partners that may have related information identified through one or more earlier transactions or encounters.
2. The Participants recognise that to enable this solution in the near term they may need to adjust existing bilateral agreements or arrangements or enter into new agreements or arrangements, as appropriate, subject to the necessary domestic authorisations.

3. Over the longer-term, participants intend to continue examining opportunities to maximise the value of Secure Real Time Platform, to the extent permitted under applicable laws and policies.

(b)(6)

FOR THE GOVERNMENT OF AUSTRALIA

19/11/19  
Date

(b)(6)

FOR IMMIGRATION, REFUGEES AND CITIZENSHIP CANADA

Nov. 19 2019  
Date

(b)(6)

FOR THE CANADA BORDER SERVICES AGENCY

Nov. 19. 2019  
Date

(b)(6)

FOR THE GOVERNMENT OF NEW ZEALAND

19 Nov 2019  
Date

(b)(6)

FOR THE HOME OFFICE OF THE GOVERNMENT OF THE UNITED KINGDOM

19.11.2019  
Date

(b)(6)

FOR THE GOVERNMENT OF THE UNITED STATES

19 Nov 2019  
Date



**Implementing Arrangement  
under the Agreement between the Government of the United States of  
America and the Government of the Hellenic Republic  
on Enhancing Cooperation in Preventing and Combating Serious Crime**

**The Government of the United States of America and the Government of the Hellenic Republic** (herein “Participants),

**Deciding** to implement this Arrangement through the Hellenic Police and the U.S. Department of Homeland Security,

**Having regard** for the Joint Statement, signed on March 31, 2016, for continued designation in the U.S. Visa Waiver Program,

**Having regard** for the Arrangement between the Special Violent Crime Division of the Hellenic Police and the Terrorist Screening Center of the United States of America for the exchange of information concerning terrorist acts,

**Having regard** for the Agreement Between the Government of the Hellenic Republic and the Government of the United States of America on Enhancing Cooperation in Preventing and Combating Serious Crime (herein the “PCSC Agreement”), and, in particular, Article 7 thereof, which permits implementing arrangements to set forth technical and procedural details for automated queries conducted under Articles 4 and 5 of the PCSC Agreement,

**Recalling**, in particular, Articles 2 (Purpose and Scope), 4 (Automated querying of fingerprint data), 6 (Supply of further personal and other data), and 11 (Supply of personal and other data in order to prevent serious criminal and terrorist offences) of the PCSC Agreement,

**Prompted** by the urgency of the current humanitarian and mass migration crisis, due primarily from conflicts in Syria and Iraq,

**Prompted** also by the desire to systematically screen migrants and refugees, including at the border where an individual for whom the additional data is sought has been identified for further inspection,

**Desiring** to cooperate as partners to prevent and combat serious crime, particularly terrorism, including through the identification of criminals during border and immigration screening consistent with Article 5 of the PCSC Agreement,

**Recognizing** the critical importance of timely access to accurate information for the prevention and combating of serious crime, including terrorist travel,

**Recognizing** also that information sharing between the Participants should respect fundamental rights and freedoms, notably privacy, taking into account relevant national legislation as well as the international obligations of each Participant,

**Have reached** the following understanding:

### **1. Purpose of this Arrangement**

- a. Under this Arrangement, the Participants intend to utilize the PCSC Agreement in order to identify criminals, including potential terrorists or other threats to national security, attempting to exploit the international movement of migrants, refugees and asylum seekers for mala fide purposes, including obtaining documents valid for VWP travel.
- b. The Participants may also supply any available further personal data and other data, pursuant to Article 6 of the PCSC Agreement, when particular circumstances are met. This data includes, for the United States, the Federal Bureau of Investigation's criminal history information, when the Special Violent Crime Division of the Hellenic Police submits a query on a subject for suspicion of engaging in a criminal or terrorism offense.
- c. The Participants hereby provide their prior consent, if needed, under Article 13(1)(d) of the PCSC Agreement, to process personal data for the purposes described in this Section.

### **2. Definitions**

- a. As an implementing arrangement under the PCSC Agreement, the definitions in Article 1 of the PCSC Agreement apply.
- b. "Encounter information" means the information necessary to illustrate why a Participant holds the fingerprint of an individual and whether such individual is believed to have ties to serious crime and/or terrorism.
- c. "Requesting Participant" means the Participant to this Implementing Arrangement that has initiated the query.
- d. "Providing Participant" means the Participant to this Implementing Arrangement that receives the query from the Requesting Participant

### **3. Automated querying of fingerprint and other biometric data**



- a. For the purposes set forth in Section 1, each Participant intends to allow the other Participant through the national contact points referred to in Section 6 of this Arrangement, hit/no hit access to the reference data in its automated fingerprint identification systems to conduct automated queries by comparing fingerprint data as provided by Article 4 of the PCSC Agreement. Queries may be conducted only in individual cases and in compliance with the Requesting Participant's national law.
- b. An automated query is expected to include the following without human intervention:
  - (i) the electronic receipt of a fingerprint and reference data from the Requesting Participant;
  - (ii) comparison of the fingerprint supplied by the Requesting Participant against the automated identification systems of the Providing Participant;
  - (iii) electronic confirmation of whether the supplied fingerprint matches a record in the automated identification system;
  - (iv) confirmation of whether the Providing Participant knows the fingerprint supplied by the Requesting Participant to be associated with an individual or act known or suspected of having ties to serious crime and terrorism, and;
  - (v) provision of appropriate personal data and encounter information which may include, subject to availability and practicality, information such as surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, photographs, current and former nationalities, passport data, numbers from other identity documents, immigration history and descriptions of past enforcement actions.
- c. Where applicable and mutually decided by the Participants, queries, comparisons and further analysis may also be made concerning other data. In particular, the Participants intend to pursue a Memorandum of Understanding or other appropriate mechanism to document additional cooperative efforts to further facilitate the ability to identify, prevent, and counter serious crime through the exchange of biographic information as part of the initial vetting to match against derogatory information that may be linked only to biographic information.

#### **4. Supply of further personal and other data**

- a. Should the procedure referred to in Section 3 show a match between fingerprint or other biometric data, [and the requirements of subparagraph c of Section 4 are met] the Requesting Participant intends to supply the Providing Participant with personal data and encounter information it has collected or generated during the immigration proceeding that motivated its query.
- b. The Requesting Participant intends to supply relevant personal data and encounter information to the Providing Participant including, if available and practical, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, photographs, current and former nationalities, passport data, numbers

from other identity documents and applicable encounter data. The personal data to be supplied may also include, when available, biometric data, facial recognition or iris scan data.

- c. This Section is intended to apply when, as evidenced either by a match against relevant information held by the Providing Participant or as defined under the Requesting Participant's laws, the data subject(s):
- (i) May be planning to commit or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association; or
  - (ii) Is undergoing or has undergone training to commit the offenses referred to in clause (i);
  - (iii) May be planning to commit or has committed a serious criminal offense, is the subject of a criminal investigation, or participates in an organized criminal group or association; or
  - (iv) May be planning to commit or has committed a serious criminal offense in one country and the offender is in or intends to travel to another country.

#### **5. Terrorist Verification Procedures**

When the Requesting Participant encounters an individual who is a potential match to terrorism information supplied by the Providing Participant, both Participants intend to take measures consistent with the terms of the Arrangement between the Special Violent Crime Division of the Hellenic Police and the Terrorist Screening Center of the United States of America for the Exchange of Information Concerning Terrorist Acts.

#### **6. National contact points and implementing Arrangements**

For the purpose of the supply of data as referred to in Sections 4 through 7, the Participants designate the following as national contact points:

For the Government of the United States of America:

For implementation of this Arrangement, U.S. Department of Homeland Security.

For terrorist identity verification under Article 5 of this implementing Arrangement, the Terrorist Screening Center, U.S. Federal Bureau of Investigation.

For the Government of the Hellenic Republic: Hellenic Police, Special Violent Crime Division

#### **7. Supply of personal and other data in order to prevent serious criminal and terrorist offences**

Pursuant to Article 11 of the PCSC Agreement and consistent with its terms and the objectives in Section 1 of this Arrangement, for the purposes of detecting, combating, and investigating serious criminal and terrorist offences, a Participant may, in compliance with its national law, in individual cases, without being requested to do so, supply the other Participant's relevant national contact point, as referred to in Section 6, with the personal data specified in Article 11 of the PCSC Agreement.

## **8. Privacy and Data Protection**

The Participants recognize that the appropriate handling and processing of personal data acquired from each other is of critical importance to preserving confidence in the implementation of this Arrangement. The Participants intend to comply with their respective laws and their obligations under the PCSC Agreement, in particular Articles 12 through 19 thereof.

## **9. Review**

- a. The Participants intend to consult each other regularly on the implementation of this Arrangement. As part of such consultations, the Participants intend to
  - i. review the number of automated queries made and the number and percentage of matches; and
  - ii. share, to the extent practical, additional statistics and case studies demonstrating how the exchange of information under this Arrangement has assisted in encountering serious crime and terrorism.
- b. The Participants should consult each other on any privacy incidents (including unauthorized access or disclosure) of personal information shared under this Arrangement, as well as a summary of remedial actions taken in response to any such incidents.

## **10. Relationship to PCSC Agreement**

This Arrangement serves as an implementing arrangement to the PCSC Agreement and the Participants recognize that all of the provisions of the PCSC Agreement apply to this Arrangement. In the event of a conflict between the provisions of this Arrangement and

the provisions of the PCSC Agreement, the provisions of the PCSC Agreement are intended to prevail.

### 11. Expenses

Each Participant intends to bear its own expenses under this Arrangement. In special cases, the Participants may jointly decide on other Arrangements.

### 12. Discontinuance of this Arrangement

Either Participant may discontinue cooperation under this Arrangement at any time, intending to give three months' written notice to the other Participant. The Participants intend to continue to apply the terms of the Arrangement to personal data supplied before such discontinuation.

### 13. Consultations

- a. In the event of any dispute arising out of the interpretation or the implementation of this Arrangement, the Participants intend to consult each other in order to reach resolution.
- b. This Arrangement may be modified by mutual consent of the Participants.

### 14. Commencement

The Participants intend to begin cooperation under this Arrangement on the date of receipt of written notification through diplomatic channels from the Government of the Hellenic Republic informing the Government of the United States of America that it has completed its internal legal procedures to implement this Arrangement.

Signed in duplicate.

<b>FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA</b>	<b>FOR THE GOVERNMENT OF THE HELLENIC REPUBLIC</b>
(b)(6)	(b)(6)

AT: Washington DC

AT: Athens

DATE: 11/7/2016

DATE: 10.11.2016.

## **STATEMENT OF INTENT ON**

### **ENHANCING BILATERAL COOPERATION TO PREVENT AND COMBAT SERIOUS CRIME AND TERRORISM IN THE CONTEXT OF MIGRATION FLOWS**

The Secretary of Homeland Security of the United States of America and the Minister of the Interior of the Italian Republic, having met today in Rome, within the framework of the G6 consultations under the Italian Presidency, have acknowledged their excellent cooperation on matters of security.

In this regard, fully aware of the risks deriving from the intensification of terrorist and criminal activities, illegal migration, and transnational challenges having a direct impact on security, they have expressed their common willingness to reinforce operational cooperation between their respective agencies, including by fully implementing all existing tools to prevent and counter serious crime and terrorism.

Of particular note is the "Agreement between the Government of the United States of America and the Government of the Italian Republic on Enhancing Cooperation in Preventing and Combating Serious Crime" done at Rome on May 28, 2009.

The Secretary of Homeland Security of the United States of America and the Minister of the Interior of the Italian Republic intend to give priority to completing a technical arrangement that, in the respect of the laws of the two countries and implementing the above mentioned Agreement of May 28, 2009, allows the United States and Italy to identify criminals, including potential terrorists, or other threats to national security attempting to exploit international movement of migrants, refugees and asylum seekers for mala fide purposes through information sharing, including the use of automatic systems to query biometric data (the Secure Real Time Platform).

The Secretary of Homeland Security of the United States of America and the Minister of the Interior of the Italian Republic intend for the two countries to swiftly finalize the aforesaid arrangement and expect to begin operational cooperation upon the arrangement's signature in order to deepen information sharing on security matters.

Signed at Rome, October 21, 2016.

The Secretary of Homeland Security  
of the United States of America

(b)(6)

The Minister of the Interior  
of the Italian Republic

(b)(6)

**Memorandum of Understanding**

**Between**

**The Secretary of State for the Home Department  
Acting through the United Kingdom Border Agency**

**and**

**The United States Department of Homeland Security**

**Regarding the Exchange of Data Between the United Kingdom and United States,  
as part of the High Value Data Sharing Protocol Between the Nations of the Five  
Country Conference**

The Secretary of State for the Home Department, acting through the United Kingdom (U.K.) Border Agency (UKBA), as the U.K. Participant, and the United States (U.S.) Department of Homeland Security (DHS) as the U.S. Participant, (hereafter referred to collectively as the "Participants"),

HAVING REGARD FOR the long-standing co-operative relationship between the immigration authorities in the United Kingdom and the United States of America;

CONSIDERING the increasing global patterns of both regular and irregular migration, and that the compelling need to welcome genuine migrants, whilst tackling identity fraud and abuse of our countries' immigration laws, is important to maintaining the prosperity and security of our respective societies;

RECOGNISING that Australia, Canada, New Zealand, the United Kingdom and the United States of America, as the countries of the Five Country Conference (FCC), have developed a High Value Data Sharing Protocol ("the FCC Protocol") whose operation is set out in bilateral arrangements such as this MOU.

CONFIRMING that this arrangement is intended to facilitate the matching of immigration and nationality cases against each others' biometric databases, and to exchange relevant information on cases where biometric matches are made, for the collective benefit of both Participants;

Have mutually decided as follows:



## **1 PURPOSE**

1.1 This MOU is intended to enable the exchange of data between the Participants for immigration and nationality purposes in order to assist the Participants in the maintenance of fair and effective immigration controls. As part of the FCC effort to improve immigration controls, the FCC partner countries have undertaken biometric matching trials. Those trials showed the potential value of biometric data exchange to help establish the identities, and confirm or deny the claims, of migrants to FCC countries, and to assist processing and removal of those who remain illegally in, or are due to be removed from, one of the FCC partner countries.

1.2 Obtaining information from another FCC country is an important component of maintaining fair and effective immigration controls and, for the Participants to this MOU, is in the substantial public interest.

1.3 In the context of this MOU, immigration and nationality purposes are the consideration, regulation and enforcement of whether, and on what basis, any person may enter or remain in the territory of one of the Participants.

1.4 Nothing in this MOU, including its discontinuation, if applicable, is intended to affect the sharing of information between the Participants under other established arrangements, or any other Agreement or Arrangement, provided that no information shared pursuant to this agreement is shared in a manner inconsistent with the terms of this MOU.

1.5 All work under this MOU is to be carried out in accordance with all relevant provisions of both Participants' laws and their international obligations.

## **2 PROCEDURES FOR THE EXCHANGE OF INFORMATION**

### General

2.1 In respect of any case handled under this MOU, the Participant which supplies the fingerprints for matching is known as the "Requesting Participant" whilst the Participant which searches the fingerprints against its systems is known as the "Providing Participant".

2.2 Data exchange under this MOU is expected to be conducted securely between designated points of contact, through the FCC Secure File Share Server ("SFSS") which is to be hosted by the Government of Australia. The arrangements for management of the SFSS are set out in a separate Service Arrangement between each Participant and the Government of Australia. Notwithstanding any discontinuance or suspension of activities under the Protocol in accordance with paragraphs 6.21 or 11.2 of this MOU, the Participants expect that the Government of Australia will continue to host the SFSS in accordance with the Service Arrangement. In the event that the Government of Australia is unable to continue to host the SFSS, the Participants expect that it will give written notice of not less than 90 days to the other countries participating in the Protocol.

2.3 The countries participating in the FCC Protocol intend to maintain a mutually decided Search Code Guide, which sets out search codes to be attached to different types of

case that are to be matched, and will aid understanding of which information is desirable and appropriate to exchange in different circumstances.

#### Fingerprint matching requests

2.4 (b)(7)(E)

(b)(7)(E) Each Participant may provide whichever cases it considers will provide high value from the exchange, which are likely to include, but not be limited to:

- Immigration cases where identity of the individual is unknown or uncertain;
- Immigration cases where the individual's whereabouts are unknown; and/or
- Immigration cases where there is reason to suspect that the person has been encountered by more than one of the countries participating in the Protocol;

2.5 (b)(7)(E)

(b)(7)(E)

2.6 The Participants intend to ensure that the fingerprints exchanged for searching under this MOU do **not** contain fingerprint data of known FCC nationals.

(b)(7)(E)

#### Fingerprint matching and response

2.9 Upon notification from the SFSS of the request, the Providing Participant is to then search the fingerprints against its relevant biometric systems.

2.10 The relevant biometric systems, in the first instance, in the case of the UK is to be the Immigration and Asylum Fingerprint System (IAFS) and, in the case of the U.S., is to be the DHS Automated Biometric Identification System (IDENT). The Participants may decide in writing to extend some or all of the searches to additional relevant systems to the extent authorized by applicable law and policy.

(b)(7)(E)

(b)(7)(E)

2.12 The Providing Participant is expected to destroy the fingerprints in a secure manner consistent with the Providing Participant's domestic law and policy, and use them for no other purpose once the search against its relevant biometric systems is complete.

Further information exchange

2.13 In order to facilitate efficient and proportionate exchange of relevant information, the Participants, in cooperation with the other countries participating in the FCC Protocol, have agreed to maintain a Search Code Guide which sets out the data elements that may be routinely provided when a match occurs, according to the search code given by the Requesting Participant and the nature of the information held by the Providing Participant.

2.14 For each matching case, the Providing Participant intends to review its records of the data subject and, in accordance with the Search Code Guide and the provisions of section 4 of this MOU, determine what further information is available to provide to the other Participant, consistent with its relevant domestic law and policy. The Providing Participant is expected to place any information it identifies for disclosure to the Requesting Participant onto the SFSS, along with a request for any information it identifies for disclosure by the Requesting Participant.

2.15 For each matching case, the Requesting Participant is expected to place onto the SFSS the equivalent data set out in paragraph 2.11 from its own system, to the extent that the data are available within its relevant biometric system and it is lawful for the data to be disclosed.

2.16 Either Participant may subsequently request in writing further data on matching cases from the other Participant, and is to provide sufficient reasons for such requests to enable the other Participant to determine the legality of disclosing such further information. The written request is to also set out the data elements requested and the name of the requestor. Subject to the provisions of section 4 below, each Participant is to endeavour to provide information requested by the other in a timely manner using the SFSS.

### **3 DESIGNATION OF OFFICIALS**

3.1 Each Participant is expected to designate officials in the responsible organization who are authorized to exchange information under this MOU, and to keep the other Participant informed in writing or by email of any such designations or changes. All fingerprint matching requests, and information provided in response thereto, made under this MOU are to be communicated between these designated officials as central contact points for information exchange between the Participants.

3.2 The officials designated under paragraph 3.1 are to work within each Participant's central team which administers the Protocol and has responsibility for that Participant's operation of the Protocol.

3.3 Each Participant is expected under paragraph 3.1 specifically to designate a Protocol Manager who is to be responsible for ensuring that Participant's implementation of the provisions of this MOU.

#### **4 INFORMATION WHICH MAY BE EXCHANGED**

4.1 The Participants may exchange, using the SFSS, relevant information on matching cases further to that set out at paragraph 2.11, which may include, but is not limited to:

- Immigration history and immigration status;
- Details of known or suspected immigration abuse and offences, including overstays of authorised presence in a country, or people smuggling;
- Criminality and other information that is pertinent to immigration and nationality purposes;
- Copies of travel documents or other identity documents;
- Such other information as the Participants may mutually consider appropriate.

4.2 Information may be exchanged under this MOU only to the extent that is relevant, necessary, and appropriate to the immigration and nationality purposes of the Participants, and is permitted by the Participants' domestic laws and international obligations.

4.3 Participants are expected to share information only to the extent that the information is available to them and the disclosure is practicable.

4.4 It is clearly understood that a Participant may not be at liberty to share information, wherever use or transfer of that information is restricted by law, policy or protocol, or is subject to another's consent (whether the consent of the data subject, or of another authority or person). The usefulness of the information exchanged, and the limitations thereon, are to be subject to ongoing review and constructive discussion between the countries participating in the FCC Protocol.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Limitations on use and disclosure

5.6 Disclosure or use of the information received under this MOU for any purpose or to any person other than as set out in paragraphs 5.1 to 5.5 is to be subject to the prior written approval of the Participant that supplied the information.

5.7 Any use or disclosure of information received under this MOU is expected to comply with the receiving Participant's applicable domestic laws and international obligations.

5.8 Specifically, neither Participant is to exchange, use or disclose information in any way pursuant to this MOU such that the information could become known to any government, authority or person from which the subject of the information is seeking or has been granted protection under the 1951 Convention Relating to the Status of Refugees, its 1967 Protocol, the Convention Against Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment or, in the case where the UK is the Requesting Participant,, under the European Convention on Human Rights, or under either Participant's domestic laws implementing the relevant Conventions or Protocol. Nor is a Participant to exchange, use or disclose information to a government, authority or person, in circumstances where, by virtue of the government, authority or person becoming aware of such information, the subject of the information may become eligible for such protection.

5.9 In any particular case, a Participant may, by way of protective marking or otherwise, apply additional restrictions as to the use or disclosure of information which it has provided under this MOU, including to ensure that treatment of the information is consistent with its applicable domestic policies, laws and international obligations. Where this is done the other Participant is expected to comply with the restrictions. Such restrictions may not preclude subject access as provided for by paragraph 5.5.

5.10 This MOU is not intended to preclude the use or disclosure of information to the extent that there is an obligation to do so under the laws of the receiving Participant. To the extent practicable, a Participant should notify the other in advance of any use or disclosure of information received under this MOU which is not otherwise consistent with the terms of the MOU. In addition, UKBA is expected first to seek written permission from the U.S. Department of State if it wishes to disclose U.S. visa data to the data subject or to a court (including an administrative tribunal). This is intended to provide Participants (and the U.S. Department of State) with the opportunity, where appropriate, to seek the non-disclosure or other protection of the information, to the extent permitted by the law of the receiving Participant.

## **6 INFORMATION TRANSFER AND SECURITY**

6.1 Each Participant is expected to apply at a minimum the standards set out herein with respect to the handling and safeguarding of the information received. In particular, each is expected to maintain any personal identifying information received in a manner at least as secure and with similar privacy and data protection rights and privileges being afforded to the data subject as is the case with its own citizens.

### Secure File Share Server

6.2 Other than in the contingencies set out in paragraphs 6.3 and 6.4, all data exchange under this MOU should be conducted securely between designated officials, through the SFSS. Processes, formats and media for data exchange should conform wherever applicable to the FCC Data Format Standard and such other standards and processes as may be mutually decided by the countries participating in the FCC Protocol.

### Contingencies for data transfer

6.3 In the event that the SFSS is unavailable, information may be transmitted between the Participants via direct country-to-country e-mail transfer, which is to be encrypted using an Advanced Encryption Standard (AES) 256 bit key.

6.4 In the unlikely event that the SFSS and encrypted e-mail are both unavailable, but either Participant urgently seeks information, that Participant may make arrangements for one of its designated officials to deliver the information by hand to the other Participant's Embassy. The information may then be transmitted between the relevant Participant's Embassy and home government within its secure e-mail network.

### Data security

6.5 Classification. Personal information received by the U.K. under this MOU is to be classed as "Restricted", and information received by the U.S. under this MOU is to be classed as "For Official Use Only", unless the Participant that supplied the information requests otherwise.

6.6 Identification, Authentication and Access Controls. Each Participant is to enforce strong authentication measures to ensure that access to information received under this MOU is so limited. Each Participant is expected to limit access to the information received under this MOU to those authorised personnel who have a need to know the information to carry out their official duties, for uses which are consistent with the purposes of this MOU.



6.7 Dissemination Controls. Each Participant is expected to ensure that information received under this MOU is protected from unauthorised dissemination.

6.8 Records Management on the SFSS. The Participant retrieving the information from the SFSS is responsible for the deletion of that information from the SFSS upon successful retrieval.

6.9 Records Storage. Personal and official information should be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information. Both Participants are expected at all times to store information obtained under this MOU in secure electronic and/or paper storage systems.

6.10 Personnel Training for Permitted Uses. All persons who have access to data received under this MOU are expected to have been appropriately educated and trained regarding the handling and restrictions on use of this information to ensure the overall safeguarding of the information and compliance with this MOU.

#### Integrity of Information

6.11 Information provided and received under this MOU should be accurate, complete and up to date to the maximum extent practicable for the purposes of this MOU. A Participant may not modify any information received under this MOU without the authorisation of the Participant that provided it.

6.12 If either Participant becomes aware that information it provided or received under this MOU is inaccurate, that Participant should advise the other Participant thereof and provide correct information.

6.13 The Participants are expected in a timely manner to take appropriate action with regard to any request made by the other Participant for access, additions, changes, deletions, or corrections to information provided.

6.14 Each Participant confirms that it maintains a system accessible by individuals that regardless of their nationality or country of residence, allows individuals to request information about them that was received under this MOU, and to request correction or notation of that information. Each Participant also confirms that it provides redress opportunities to persons seeking such access, correction or notation regardless of their nationality or country of residence.

#### Retention of Information

6.15 Subject to paragraph 2.12, each Participant is expected to assess the continued relevance of the information received under this MoU to its immigration and nationality purposes, and to destroy the information securely when it is no longer relevant. In particular:

- Data subject case file. Personal information which is retained on an electronic or paper case file relating to the data subject, because it has ongoing relevance to that file, may be retained as part of that file in accordance with the domestic laws and data retention policies of the Participant that has received it.
- Watchlists, Lookouts and Alert Lists. Personal information relating to:
  - o false identities and travel documents;

- multiple identities used by the same person;
  - persons engaged in derogatory activity that would render them inadmissible to the territory of the Participant that has received it;
- may also be retained for as long as it is relevant to that Participant's border controls, up to an initial maximum of ten years from the date of receipt. As part of their ongoing review of such entries the Participants intend to discuss the continued relevance of the information and seek approval before ten years on information appropriate for retention for a further period.

- Data held by central Protocol team. Personal information which is otherwise retained, in a central record of information received or otherwise, may be retained for no longer than two years from the date of receipt.

Any further retention is subject to the prior written approval of the Participant that supplied the information.

#### Notifications and remedies

6.16 To provide further safeguards for the privacy, security, confidentiality, integrity and availability of the information systems and the information they store, process and transmit, and in addition to the safeguards set out in the SFSS Service Arrangement described in paragraph 2.2, the Participants are expected to provide notice to each other of the following specific events:

- By immediately notifying the other Participant by telephone or e-mail in the event of a disaster or other situation that disrupts the intended transfer of information between them;
- By notifying the other Participant in writing as soon as reasonably practicable, but no later than 24 hours after becoming aware of any breach of the security of the information systems containing, or unauthorised use or disclosure of, any personal information shared under this MOU.

6.17 Prevention of Misuse. The Participants are expected to take appropriate action under their administrative, civil, and/or criminal laws in the event of misuse, unauthorised alteration, or deletion of, or unauthorised access to or dissemination of information obtained under this MOU by their own employees, agents or any third party.

#### Recording of transactions

6.18 The Participants are expected each to maintain records of information provided and received under this MOU using a mutually agreed reporting framework for the FCC Protocol. This is without prejudice to any further records they may keep in accordance with their applicable domestic laws and record retention policies and guidance.

#### Compliance and Audit

6.19 Either Participant may request assurance from the other that sufficient safeguards are being maintained with regard to the information provided under this MOU, which may include requesting an audit of the safeguards. A Participant from which an audit is requested may arrange for this to be carried out by an appropriate internal or external auditor, with terms of reference that are expected to be mutually determined by the Participants.

6.20 The Participants should endeavour to address any perceived deficiencies in safeguards under paragraph 6.19 of this MOU. However, if a situation arose whereby a Participant considered it necessary to decline to provide further information pending a

resolution of the issue, it is expected to provide written notice to the other Participant, and also to notify the other countries participating in the FCC Protocol. Such notification is to be the subject of immediate consultation between the countries participating in the FCC Protocol to decide upon the appropriate course of action.

## **7 PERFORMANCE AND MANAGEMENT REPORTING**

7.1 The Participants are to jointly prepare a report of the types of transactions, the outcomes and the timeliness of the matching activity based on mutually decided performance and management measurements. The joint report is to include, but not be limited to, the number and severity of any security/privacy breaches of the SFSS or personal information shared under this MOU as well as a summary of remedial actions taken.

## **8 MODIFICATION AND CONSULTATION**

8.1 Participants intend to inform each other of any changes to their respective laws, policies or international obligations that could materially affect the operation or interpretation of this MOU.

8.2 The Participants may modify this MOU from time to time, as mutually decided in writing by their Protocol Managers, and otherwise make changes to its operation as provided for by its specific terms, provided that such modification and changes are consistent with the original nature and scope of the MOU and with the effective operation of the FCC Protocol. Before making such modification or changes the Participants should first consult the Government of Australia as administrator of the SFSS for the FCC Protocol, and notify each of the other countries participating in the Protocol, in order to ensure effective understanding and operation of the Protocol is maintained.

## **9 GENERAL PROVISION**

9.1 This MOU embodies the understanding of the Participants. It is not intended to create legally binding obligations, nor to create or confer any right, privilege or benefit on any person or party, private or public.

9.2. Any differences between the Participants arising out of the interpretation, implementation or application of any aspect of this arrangement may be resolved by mutual consultation without reference to any third party or international tribunal.

9.3 Nothing in this MOU should be considered to prevent either Participant from co-operating or granting assistance in accordance with the provisions of other applicable international treaties and agreements, other arrangements, national laws and related practices.

## **10 FINANCING**

10.1 The Participants are to bear their own costs and use their own equipment and personnel resources in performing their activities under this MOU.

## **11 COMMENCEMENT AND DISCONTINUANCE**

11.1 Co-operation under this MOU may commence upon confirmation by both Participants, and the Government of Australia as administrator of the SFSS, that they are prepared for implementation, and is to continue indefinitely unless discontinued under paragraph 11.2.

11.2 Other than as provided for under paragraph 6.20 of this MOU, participation in this MOU is expected to continue whilst both Participants continue to participate in the FCC Protocol. In the event that either Participant wishes to discontinue its activities under the Protocol, it is expected to provide 60-day written notice to each of the other countries participating in the Protocol. Such notification should be the subject of immediate consultation by the countries participating in the Protocol to decide upon the appropriate course of action to effect discontinuation of that country's activities on the most economical and equitable terms. Discontinuation of a country's activities under the Protocol should be represented by discontinuation of activities under this MOU and under the similar arrangements which that country has with the other countries participating in the Protocol. Each country is expected to pay the costs it incurs as a result of discontinuation of activities under the arrangements for the Protocol.

11.3 The Participants reconfirm their commitment to work and share data with all countries participating in the FCC Protocol, as set forth in this MOU and the similar arrangements with the other partner countries. Excepting such unlikely circumstances as are specified and need resolution under paragraph 6.19 of this MOU, each Participant intends faithfully to continue this co-operation fully with all of the countries participating in the Protocol, for as long as the Protocol is in operation and each country remains a participant in the Protocol.

FOR THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

(b)(6)

Date 30/06/2010

(b)(6)

Assistant Secretary for Policy

FOR THE UNITED KINGDOM BORDER AGENCY

(b)(6)

Date 30/06/2010

(b)(6)

Chief Executive

**Implementing Arrangement between the Department of State and the Department of Homeland Security of the United States of America, on the one side, and the New Zealand Ministry of Business, Innovation and Employment, on the other side, concerning the sharing of visa and immigration information on a case-by-case basis.**

The Department of State and the Department of Homeland Security of the United States of America, on the one side, and the New Zealand Ministry of Business, Innovation and Employment (Immigration New Zealand), on the other side, each side hereinafter referred to as a "Participant" and the two sides referred to as "Participants";

**Regarding** the Agreement between the Government of the United States of America and the Government of New Zealand for the Sharing of Visa and Immigration Information, done at Wellington May 5, 2017 ("the Agreement");

**Considering** that the Government of the United States and the Government of New Zealand are Parties to the Agreement, which provides in Article 4 for the development of implementing arrangements consistent with their respective domestic laws;

**Noting** that the Department of State and the Department of Homeland Security are the departments primarily responsible for the administration and enforcement of immigration laws for the United States and that the Ministry of Business, Innovation and Employment is the ministry responsible for the administration and enforcement of immigration laws for New Zealand;

**Recognizing** that in Article 5 of the Agreement the Governments of the United States and New Zealand have undertaken not to use or further disclose Information except in accordance with the Agreement or otherwise as required under the domestic law of the government receiving the Information;

**Acknowledging** that the sharing of Information on a case-by-case basis between the Participants is an important component, and in the legitimate interests, of maintaining fair and effective immigration.

**HAVE COME** to the following understanding:

**1. General**

- A. Information exchanged pursuant to this Implementing Arrangement is subject to the terms, including any conditions included therein, of the Agreement. Any guidance on the interpretation, application, or implementation of this Implementing Arrangement is intended to be read consistent with the Agreement.
- B. Nothing in this Implementing Arrangement, nor its discontinuation, is intended to affect the exchange of Information between the Participants under other arrangements or agreements, including other implementing arrangements to the Agreement.
- C. The Participants acknowledge that they may decline to provide all or part of the Information consistent with Article 9 of the Agreement. For the U.S. side, this would include, but is not



limited to Information relating to applicants for and beneficiaries of certain applications under U.S. law, including applications pertaining to Victims of Human Trafficking (T) or Victims of Criminal Activity (U) non-immigrant status or Violence Against Women Act relief, which U.S. domestic law (currently codified at 8 U.S.C. section 1367) protects from disclosure; and Information derived from applications and associated documentation related to Temporary Protected Status.

## **2. Definitions**

For the purpose of this Implementing Arrangement:

- A. Definitions in the Agreement are intended to be incorporated by reference within this Implementing Arrangement.
- B. "Case-by-case basis" constitutes any request for Information or the proactive provision of Information, including but not limited to Personal Data, that is intended to support a specific individual case or operation conducted by either one or both Participants, and occurs outside of a recurring or systematic information sharing relationship.

## **3. Scope and Purpose**

Consistent with Articles 2, 3 and 4 of the Agreement, the purpose of this Implementing Arrangement is to establish the conditions under which the Participants intend to exchange Information on a case-by-case basis to assist in the effective administration and enforcement of the immigration laws of their respective countries.

## **4. Information to be Exchanged**

Information that may be exchanged under this Implementing Arrangement, where available, includes but is not limited to:

- A. Biographic personal identifying information, including aliases
- B. Biometric personal identifying information
- C. Travel document information, including scans of documents
- D. Immigration status
- E. Contact details
- F. Family details
- G. Relevant medical information
- H. Biometric transaction history
- I. Immigration history, including types of previous applications and their outcomes
- J. Other personal identifying information captured as part of an immigration application process
- K. Criminal history, including convictions and sentences, that is relevant to the effective administration and enforcement of immigration laws
- L. Intelligence that is relevant to the effective administration and enforcement of immigration laws
- M. Trend analysis that is relevant to the effective administration and enforcement of immigration laws
- N. Statistical data that is relevant to the effective administration and enforcement of immigration laws

## **5. Exchange of Information**

- A. Consistent with this Implementing Arrangement, each Participant may, on a case-by-case basis, request Information from or provide Information to the other Participant for the purpose of administering or enforcing its country's respective immigration laws.
- B. The Participants intend to designate officials authorised to exchange Information pursuant to this Implementing Arrangement. The Participants further intend to inform each other in writing of such designations or any changes therein. The Participants are to ensure that all Information exchanges, including requests, occur only between these designated officials.

## **6. Procedures for the Protection, Exchange, Use and Disclosure of Information**

- A. The Participants intend that protection, exchange, use and disclosure of Information will be consistent with the Agreement, including Article 7 (A), (C), (D), (E), and (F).
- B. Information exchanged between the Participants is intended to be protected by appropriate administrative, technical and physical safeguards, appropriately classified and disclosed only for uses that are consistent with the purposes described in Article 2 of the Agreement and paragraph 3 of this Implementing Arrangement.
- C. Information is intended to be transmitted via methods that conform to the approved standards of both Participants. Alternatively, Information may be hand delivered in hard copy by one Participant to the other.
- D. A Participant that has received Information under this Implementing Arrangement is expected to collect, use, disclose, store and protect such Information in accordance with the Agreement and as required by domestic law.
- E. Each Participant intends to limit access to Information received and the disclosure of that Information, to individuals authorized by that Participant who have the appropriate security clearance and a need to know. Such persons who have access to Information received under this Implementing Arrangement are expected to have been appropriately informed regarding the handling and restrictions on use of such Information, to promote the overall safeguarding of the Information, and to ensure compliance with the terms of this Implementing Arrangement.
- F. When the specific facts associated with Information provided under this Implementing Arrangement warrant additional restrictions, a Participant may impose conditions on the processing and use of such Information. If the other Participant accepts the Information, the Participants intend that the receipt itself demonstrates the other Participant's intention to apply such conditions to its processing or use of the Information.

## **7. Implementation and Review**

- A. The Participants intend to designate officials who are responsible for ensuring the implementation and administration of the provisions of this Implementing Arrangement. The Participants are to inform each other in writing of such designations and any changes.
- B. Consistent with Article 11 of the Agreement, the Participants understand that the usefulness of the Implementing Arrangement, Information shared under it, the limitations thereof, and its continued justification are subject to their ongoing domestic review and mutual consultation. Any difference in the interpretation, application or implementation of this Implementing Arrangement is to be resolved through such consultation.

#### **8. Access and Retention**

- A. The Participants intend to notify each other in writing of their respective mechanisms for providing individuals with access and correction opportunities for Information relating to those individuals that is received under this Implementing Arrangement.
- B. The Participants intend to mark Information retained as having been received from the other Participant.
- C. The Participants understand that Information obtained under this Implementing Arrangement may be retained, consistent with Article 8 (A) of the Agreement, in accordance with the receiving Participant's respective applicable retention and disposal schedules, and in accordance with the laws of the receiving country.

#### **9. Costs**

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

#### **10. Commencement, Modification and Discontinuation**

- A. This Implementing Arrangement is an expression of the purpose and intent of the Participants. Cooperation under this Implementing Arrangement is intended to be in accordance with the domestic legal authorities and resources of each Participant's country and the terms of the Agreement.
- B. The Participants intend for participation under this Implementing Arrangement to commence on the last date of signature by the Participants.
- C. The Participants may modify this Implementing Arrangement upon their mutual consent, which should be expressed in writing.

- D. A Participant intending to cease participation in this Implementing Arrangement is expected to give 90 days advance written notice to the other Participant. In such an event, the Participants intend for the provisions of paragraph 6 to continue to apply to Information exchanged under this Implementing Arrangement.

For the United States Side:

(b)(6)

THE DEPARTMENT OF STATE  
OF THE UNITED STATES OF AMERICA

At Washington

Date 13 Nov 2017

For the New Zealand Side:

(b)(6)

THE NEW ZEALAND MINISTRY OF BUSINESS,  
INNOVATION AND EMPLOYMENT

At Wellington

Date 12 Nov 2017

(b)(6)

THE DEPARTMENT OF HOMELAND SECURITY  
OF THE UNITED STATES OF AMERICA

At Washington, DC

Date 13 November 2017

We, the Participants of the "Statement of Mutual Understanding on Information Sharing" (the SMU), signed in February 2003,

Pursuant to Article 14 of the SMU, hereby decide to amend the SMU by adding a new Annex, entitled Annex Regarding the Sharing of Information Under the Five Country Conference High Value Data Protocol, attached hereto.

A French version of the Annex is to be prepared and conformed with the English language text through consultation between the participants.

Pursuant to Article 16 of the SMU, the activities enumerated under this Annex begin as of the latest signature date listed below:

For the Department of Citizenship and Immigration Canada:

(b)(6)

Neil Yeates, Deputy Minister

Nov. 20 / 09.

Date

For the Canada Border Services Agency:

Stephen Rigby, President

Date

We, the Participants of the "Statement of Mutual Understanding on Information Sharing" (the SMU), signed in February 2003,

Pursuant to Article 14 of the SMU, hereby decide to amend the SMU by adding a new Annex, entitled Annex Regarding the Sharing of Information Under the Five Country Conference High Value Data Protocol, attached hereto.

A French version of the Annex is to be prepared and conformed with the English language text through consultation between the participants.

Pursuant to Article 16 of the SMU, the activities enumerated under this Annex begin as of the latest signature date listed below:

For the Department of Citizenship and Immigration Canada:

\_\_\_\_\_  
Neil Yeates, Deputy Minister

\_\_\_\_\_  
Date

For the Canada Border Services Agency:

(b)(6)

\_\_\_\_\_  
Stephen Rigby, President

Nov. 24 / 09

Date



RESTRICTED/FOR OFFICIAL USE ONLY

FOR THE NEW ZEALAND  
DEPARTMENT OF LABOUR

(b)(6)

Date 22/2/11

Nigel Bickle, Deputy Chief Executive - Immigration

FOR THE UNITED STATES  
DEPARTMENT OF HOMELAND SECURITY

(b)(6)

Date 2/14/11

David Heyman, Assistant Secretary for Policy

FOR THE UNITED STATES  
DEPARTMENT OF STATE

(b)(6)

Date 2/10/11

Janice L. Jacobs, Assistant Secretary for Consular  
Affairs

**Memorandum of Understanding**  
**between the**  
**Government of the United States of America**  
**and**  
**the Government of Australia**  
**On Enhancing Cooperation in**  
**Preventing and Combating Crime**

**Memorandum of Understanding between  
the Government of the United States of America  
and  
the Government of Australia  
On Enhancing Cooperation in  
Preventing and Combating Crime**

The Government of the United States of America and the Government of Australia (herein "Participants"),

Prompted by the desire to cooperate as partners to prevent and combat crime, particularly terrorism, more effectively,

Recognizing that information sharing is an essential component in the fight against terrorism, while respecting fundamental rights and freedoms, notably privacy, and

Seeking to enhance and encourage cooperation between the Participants in the spirit of partnership,

Have reached the following understandings:

**1. Definitions**

For the purposes of this Memorandum,

1. DNA profiles (DNA identification patterns) means a letter or numerical code representing a number of identifying features of the non-coding part of an analyzed human DNA sample, i.e. of the specific chemical form at the various DNA loci.
2. Personal data means any information relating to an identified or identifiable natural person (the "data subject").
3. Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, sorting retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, combination or alignment, blocking, or deleting through erasure or destruction of personal data.
4. Reference data means a DNA profile and the related reference (DNA reference data) or fingerprint data and the related reference (fingerprint reference data). Reference data should not contain any data from which the data subject can be directly identified. Reference data not traceable to any individual (untraceables) should be recognizable as such.

## **2. Purpose and Scope of this Memorandum**

1. The purpose of this Memorandum is to enhance the cooperation between the United States and Australia in preventing and combating crime.
2. The querying powers provided for under this Memorandum are to be used only for prevention, detection and investigation of crime.
3. The scope of this Memorandum is to encompass crimes constituting an offense punishable under the laws of both Participants by a maximum deprivation of liberty of more than one year or a more serious penalty.
4. This Memorandum does not replace or limit the use of other legal assistance channels as required by the supplying Participant's laws.

## **3. Fingerprint data**

For the purpose of implementing this Memorandum, the Participants are to ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offenses. Reference data are only to include fingerprint data and a reference.

## **4. Automated querying of fingerprint data**

1. For the prevention and investigation of crime, and if permissible under the laws of both Participants, each Participant is to allow the other Participant's national contact points, as referred to in Paragraph 7, access to the reference data in the automated fingerprint identification system, which it has established for that purpose, with the power to conduct automated queries by comparing fingerprint data. Queries may be conducted only in individual cases and in compliance with the querying Participant's laws.
2. Comparison of fingerprint data with reference data held by the Participant in charge of the file is to be carried out by the querying national contact points by means of the automated supply of the reference data required for a clear match.
3. When needed, further analysis for the purpose of confirming a match of the fingerprint data with reference data held by the Participant in charge of the file is to be carried out by the requested national contact points.

## **5. Alternative means to query using identifying data**

Until Australia has a fully operational and automated fingerprint identification system that links to individual criminal records and is prepared to provide the United States with automated access to such a system, it is to provide an alternative means to conduct a query using other identifying data to determine a clear match linking the individual to additional data. Query powers are to be exercised in the same manner as provided in Paragraph 4 and a clear match is to be treated the same as a firm match of fingerprint data to allow for the supply of additional data as provided for in Paragraph 6.

## **6. Supply of further personal and other data**

Should the procedure referred to in Paragraph 4 show a match between fingerprint data, or should the procedure utilized pursuant to Paragraph 5 show a match, the supply of any available further personal data and other data relating to the reference data is to be governed by the laws, including those in relation to legal assistance, of the requested Participant, as well as the policies and guidelines based on essential interests of the requested Participant as understood in the context of the Treaty on Mutual Assistance in Criminal Matters between the United States and Australia. Further information provided under this paragraph is to be supplied in accordance with the procedures set forth in Paragraph 7.

## **7. National contact points and implementing arrangements**

1. For the purpose of the supply of data as referred to in Paragraphs 4 and 5, and the subsequent supply of further personal data as referred to in Paragraph 6, each Participant is to designate one or more national contact points. The contact point is to supply such data in accordance with the laws of the Participant designating the contact point.
2. The technical and procedural details for the queries conducted pursuant to Paragraphs 4 and 5 are to be set forth in one or more implementing arrangements.

## **8. Automated querying of DNA profiles**

1. If permissible under the laws of both Participants and on the basis of reciprocity, the Participants may allow each other's national contact point, as referred to in Paragraph 11, access to the reference data in their DNA analysis files, with the power to conduct automated queries by comparing DNA profiles for the investigation of crime. Queries may be made only in individual cases and in compliance with the querying Participant's laws.
2. Should an automated query show that a DNA profile supplied matches a DNA profile entered in the other Participant's file, the querying national contact point is to receive by automated notification the reference data for which a match has been found. If no match can be found, automated notification of this is to be given.

## **9. Alternative means to query DNA databases**

Until such time that the laws and technical arrangements of both Participants permit the type of DNA queries contemplated by Paragraph 8, a Participant is to conduct a search of its own DNA databases, in accordance with its laws, at the request of the other Participant.

## **10. Supply of further personal and other data**

Should the procedure referred to in Paragraph 8 show a match between DNA profiles, the supply of any available further personal and other data relating to the reference data is to be governed by the laws, including those in relation to legal assistance, of the requested Participant, as well as the policies and guidelines based on essential interests of the requested Participant as understood in the context of the Treaty on Mutual Assistance in Criminal Matters between the United States and Australia. Further information provided under this paragraph is to be supplied in accordance with Paragraph 11.

## **11. National contact point and implementing arrangements**

1. For the purposes of the supply of data as set forth in Paragraph 8, each Participant is to designate a national contact point. The contact point is to supply such data in accordance with the laws of the Participant designating the contact point.
2. The technical and procedural details for the queries conducted under Paragraph 8 are to be set forth in one or more implementing arrangements.

## **12. Supply of personal and other data in order to prevent serious criminal and terrorist offences**

1. For the prevention of serious criminal and terrorist offenses, the Participants may, in compliance with their respective laws, in individual cases, even without being requested to do so, supply the other Participant's relevant national contact point, as referred to in paragraph 7, with the personal data specified in subparagraph 12.2, in so far as is necessary because particular circumstances indicate that the data subject(s):

(b)(7)(E)



2. The personal data to be supplied are to include, if available, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, current and former nationalities, passport number, numbers from other identity documents, and fingerprint data, as well as a description of any conviction or of the circumstances giving rise to the belief referred to in paragraph 1.
3. A Participant may impose conditions on the other Participant before supplying data pursuant to this article. The participants intend to abide by any conditions that they accept in order to receive data.
4. Generic restrictions with respect to the legal standards of the receiving Participant for processing personal data should not be imposed by the transmitting Participant as a condition under subparagraph 12.3 to providing data.
5. In addition to the personal data referred to in subparagraph 12.2, the Participants may provide each other with non-personal data related to the offenses set forth in subparagraph 12.1.
6. Each Participant is to designate one or more national contact points for the exchange of personal and other data under this Paragraph with the other Participant's contact points. The powers of the national contact points are to be governed by the laws applicable.



### **13. Privacy and Data Protection**

1. The Participants recognize that the handling and processing of personal data that they acquire from each other is of critical importance to preserving confidence in the implementation of this Memorandum.
2. The Participants dedicate themselves to processing personal data fairly and in accord with their respective laws and:
  - (a) ensuring that the personal data provided are adequate and relevant in relation to the specific purpose of the transfer;
  - (b) retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Memorandum; and
  - (c) ensuring that possibly inaccurate personal data are timely brought to the attention of the receiving Participant in order that appropriate corrective action is taken.
3. Nothing in this Memorandum is intended to give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data. Rights existing independently of this Memorandum, however, are not to be affected.
4. Responsibility and powers for enforcing legal requirements that apply to the supply, receipt, processing, and recording of personal data lie with relevant data protection authorities or, where applicable, privacy officers and judicial authorities of the respective Participants as determined by their laws.

### **14. Additional Protection for Transmission of Special Categories of Personal Data**

1. Personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership or concerning health and sexual life should only be provided if they are particularly relevant to the purposes of this Memorandum.
2. The Participants, recognizing the special sensitivity of the above categories of personal data, are to take suitable safeguards, in particular appropriate security measures, in order to protect such data.

### **15. Limitation on processing to protect personal and other data**

1. Without prejudice to subparagraph 2.3, and in accordance with subparagraph 2.2, each Participant may process data obtained under this Memorandum:
  - (a) for the purpose of its criminal investigations;
  - (b) for preventing a serious threat to its public security;
  - (c) in its non-criminal judicial or administrative proceedings directly related to investigations set forth in subparagraph 15.1(a); or
  - (d) for any other purpose, only with the prior consent of the Participant which has transmitted the data.

2. The Participants are not to communicate data provided under this Memorandum to any third State, international body or private entity without the prior consent of the Participant that provided the data and without the safeguards required by that Participant.
3. A Participant may conduct an automated query of the other Participant's fingerprint or DNA files under Paragraphs 4 or 8, and process data received in response to such a query, including the communication whether or not a hit exists, solely in order to:
  - (a) establish whether the compared DNA profiles or fingerprint data match;
  - (b) prepare and submit a follow-up request for assistance in compliance with the its laws, including those in relation to legal assistance, if those data match; or
  - (c) conduct record-keeping, as required or permitted by its laws. Record keeping refers to keeping a record of the query, and the response following a query if there is a match.

The Participant administering the file may process the data supplied to it by the querying Participant during the course of an automated query in accordance with Paragraphs 4 and 8 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Paragraph 17. The data supplied for comparison are to be deleted immediately following data comparison or automated replies to queries unless further processing is necessary for the purposes mentioned under subparagraphs 15(3)(b) or (c).

## **16. Correction, blockage and deletion of data**

1. At the request of the supplying Participant, the receiving Participant is to correct, block, or delete, consistent with its laws, data received under this Memorandum that are incorrect or incomplete or if its collection or further processing is inconsistent with this Memorandum or the measures applicable to the supplying Participant.
2. Where a Participant becomes aware that data it has received from the other Participant under this Memorandum are not accurate, it is to take all appropriate measures to safeguard against erroneous reliance on such data, which is to include in particular supplementation, deletion, or correction of such data.
3. Each Participant is to notify the other if it becomes aware that material data it has transmitted to the other Participant or received from the other Participant under this Memorandum are inaccurate or unreliable or are subject to significant doubt.

## **17. Documentation**

1. Each Participant is to maintain a record of the transmission and receipt of data communicated to the other Participant under this Memorandum. This record is to serve to:

- (a) ensure effective monitoring of data protection in accordance with the laws of the respective Participant;
  - (b) enable the Participants to effectively make use of the rights granted to them according to Paragraphs 15 and 19; and
  - (c) ensure data security.
2. The record is to include:
  - (a) information on the data supplied;
  - (b) the date of supply; and
  - (c) the recipient of the data in case the data are supplied to other entities.
3. The recorded data are to be protected against inappropriate use and other forms of improper use and are to be kept for two years. After the conservation period the recorded data are to be deleted immediately, unless this is inconsistent with laws of the receiving Participant, including applicable data protection and retention rules.

## **18. Data Security**

1. The Participants are to ensure that the necessary technical measures and organizational arrangements are utilized to protect personal data against accidental or unlawful destruction, accidental loss or unauthorized disclosure, alteration, access or any unauthorized form of processing. The Participants in particular are to take reasonable measures to ensure that only those authorized to access personal data can have access to such data.
2. The implementing arrangements that govern the procedures for automated querying of fingerprint and DNA files pursuant to Paragraphs 4 and 8 are to provide:
  - (a) that appropriate use is made of modern technology to ensure data protection, security, confidentiality and integrity;
  - (b) that encryption and authorization procedures recognized by the competent authorities are used when having recourse to generally accessible networks; and
  - (c) for a mechanism to ensure that only permissible queries are conducted.

## **19. Transparency – Providing information to the data subjects**

1. Nothing in this Memorandum is to be interpreted to interfere with the Participants' legal obligations, as set forth by their respective laws, to provide data subjects with information as to the purposes of the processing and the identity of the data controller, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him or her and any further information such as the legal basis of the processing operation for which the data are intended, the time limits for storing the data and the right of recourse, in so far as such further information is necessary, having regard for the purposes and the specific circumstances in which the data are processed, to guarantee fair processing with respect to data subjects.

2. Such information may be denied in accordance with the respective laws of the Participants, including if providing this information may jeopardize:
  - (a) the purposes of the processing;
  - (b) investigations or prosecutions conducted by the competent authorities in the United States or by the competent authorities in Australia; or
  - (c) the rights and freedoms of third parties.

## **20. Information**

Upon request, the receiving Participant is to inform the supplying Participant of the processing of supplied data and the result obtained. The receiving Participant is to ensure that its answer is communicated to the supplying Participant in a timely manner.

## **21. Relation to Other Arrangements**

Nothing in this Memorandum is to be construed to limit or prejudice the provisions of any treaty, other arrangement, working law enforcement relationship, or laws allowing for information sharing between the United States and Australia.

## **22. Consultations**

1. The Participants are to consult each other regularly on the implementation of the provisions of this Memorandum.
2. In the event of any dispute regarding the interpretation or application of this Memorandum, the Participants are to consult each other in order to facilitate its resolution.

## **23. Expenses**

Each Participant is to bear the expenses incurred by its authorities in implementing this Memorandum. In special cases, the Participants may mutually consent to different arrangements.

## **24. Discontinuance of the Memorandum**

Cooperation under this Memorandum may be discontinued by either Participant. The Participants intend the Participant discontinuing cooperation to give three months' notice in writing to the other Participant. The Participants intend to continue to apply the terms of this Memorandum to data supplied prior to such discontinuation.

## **25. Revisions**

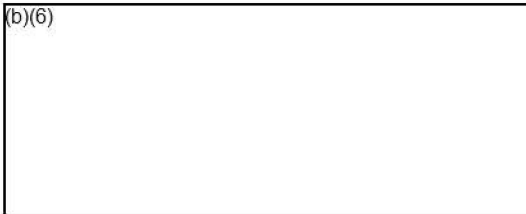
1. The Participants are to enter into consultations with respect to revisions to this Memorandum at the request of either Participant.
2. This Memorandum may be revised by the mutually written consent of the Participants at any time.

## 26. Commencement

1. The Participants intend to begin cooperation under this Memorandum, with the exception of Paragraphs 8, 10 and 11, on the date of signature by both Participants.
2. The Participants intend to begin cooperation under Paragraphs 8 and 10 through 11 of this Memorandum following the completion of the implementing arrangement(s) referred to in Paragraph 11 if the laws of both Participants permit the type of DNA screening contemplated by Paragraphs 8, 10 and 11.

Signed at Canberra, this <sup>16<sup>TH</sup></sup>.....day of November 2011, in duplicate.

(b)(6)



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

(b)(6)



**FOR THE GOVERNMENT OF  
AUSTRALIA:**

**Implementing Arrangement**  
**under the Agreement between the Government of the United States of**  
**America and the Government of the Italian Republic**  
**on Enhancing Cooperation in Preventing and Combating Serious Crime,**  
**signed at Rome on May 28, 2009**

The Department of Homeland Security of the United States of America and the Ministry of Interior of the Italian Republic (herein the "Side" or "Sides" if plural),

HAVING REGARD for the Agreement Between the Government of the United States of America and the Government of the Italian Republic on Enhancing Cooperation in Preventing and Combating Serious Crime done at Rome on May 28, 2009 (herein the "U.S.-Italy PCSC Agreement"), and, in particular, Article 5, which permits implementing arrangements to set forth technical and procedural details for automated queries conducted under Article 4 of the U.S.-Italy PCSC Agreement,

ACKNOWLEDGING the Statement of Intent on Enhancing Bilateral Cooperation to Prevent and Combat Serious Crime and Terrorism in the Context of Migration Flows signed in Rome on October 21, 2016,

NOTING their national laws and policies on data protection, in particular, for Italy, the Legislative Decree 30 June 2003 no. 196 "Code on personal data protection; the "Decree of the President of the Republic 7 April 2016 no. 87 on "Measures for implementing the Law 30 June 2009 no. 85 concerning the establishment of the National DNA Data Bank and the Central Laboratory for the National DNA Data Bank, in accordance with Article 16 of Law no. 85 of 2009"; the Council Framework Decision 2006/960/JHA of 18 December 2006; the Directive of the European Parliament 27 April 2016 no. 2016/680 and the other legal provisions of the European Union which bind Italy in the area of protection and transmission of personal and biometric data; the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offenses signed on 2 June 2016 for both sides and, for the United States, the laws, regulations, and policies regarding the protection and transmission of data and their use, including but not limited to the confidentiality provisions for special protected class information under 8 U.S.C. § 1367 and 8 C.F.R. § 208.6,

CONSIDERING the need to proceed with the conclusion of a technical arrangement for the connection to a secure real-time platform for the exchange of fingerprint data to verify the identity of migrants, asylum seekers or refugees and determine whether they are suspected, investigated, accused or convicted of terrorist offenses, offenses linked to illegal immigration or other serious crimes as specified in the technical annex which is a part of this Understanding as called for in Article 5, paragraph 2 of the U.S.-Italy PCSC Agreement,



AWARE that collaboration between the two Countries is expected to develop in the future through the use of new technologies to increase the ability to identify, prevent and counter serious forms of crime that may require further technical means of implementation between the two Countries, including automated biographic data checks,

HAVE STATED as follows:

### **Section 1 Purpose**

1. For the purposes of this Implementing Arrangement (herein "Understanding"), the Sides intend to utilize the U.S.-Italy PCSC Agreement in order to identify individuals who attempt to exploit the international movement of migrants, refugees and asylum seekers to commit the crimes of terrorism, offenses linked to illegal immigration or other serious crimes, including fraudulent acquisition of or misrepresentation on documents, including those valid for Visa Waiver Program (VWP) travel, as specified in the technical annex to this Understanding that will be updated, where needed, with the mutual consent of the Sides.
2. To this end, the Sides have decided to provide the fingerprint data contained in their national systems for the automated identification of fingerprints under Articles 3 and 4 of the U.S.-Italy PCSC Agreement. This data includes, for the United States, the Federal Bureau of Investigation's criminal history information, in those individual cases when Italy submits a query pursuant to Article 4 of the U.S.-Italy PCSC agreement on a subject suspected, under investigation, charged or convicted of engaging in the crimes of terrorism, offenses linked to illegal immigration or any other serious crime as specified in the technical annex to this Understanding or pursuant to Article 10 of the U.S.-Italy PCSC agreement.

### **Section 2 Definitions**

1. The definitions in Article 1 of the U.S.-Italy PCSC Agreement apply to this Understanding.
2. "Additional Information" means supplemental information related to the fingerprinting of the individual including whether the individual committed crimes of terrorism, offenses linked to illegal immigration or serious crime, as specified in the technical annex to and section 12.2 of this Understanding.
3. "Requesting Side" means the Side to this Understanding that has initiated the query.
4. "Requested Side" means the Side to this Understanding that receives the query from the Requesting Side.

**Section 3**  
**Automated querying of fingerprint data**

1. For the purposes set forth in Section 1, of this Understanding, each Side intends to allow the other Side's national contact points, as referred to in Section 6.1.a.i and 6.1.b of this Understanding, access to the respective automated fingerprint identification systems to conduct automated queries by comparing fingerprint data as provided by Article 4 of the U.S.-Italy PCSC Agreement.
2. Queries may be conducted only in individual cases and in compliance with the Requesting Side's national law, as provided for in Article 4 of the U.S.-Italy PCSC Agreement.
3. An automated query is expected to include the following without human intervention:
  - a. Electronic receipt of a fingerprint and reference (log) data from the Requesting Side;
  - b. Comparison of the fingerprint supplied by the Requesting Side against the automated identification systems of the Requested Side;
  - c. Notification of whether the supplied fingerprint matches a record in the automated identification systems (a positive / hit confirmation):

**Section 4**  
**Supply of further personal and other data**

1. Should the procedure referred to in Section 3 of this Understanding show a match between the queried fingerprint and one held by the Requested Side:
  - a. The Requesting Side intends to supply the Requested Side with personal data and additional information it has collected or generated during the proceeding that motivated its original query.
  - b. The Requested Side intends to supply relevant personal data and additional information to the Requesting Side.
2. Personal data may include, if available and practical, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, current and former nationalities, passport data, numbers from other identity documents and criminal, police and alien records.
3. The Personal data to be supplied may also include, when available, biometric data including but not limited to DNA, photographs or iris scan data.
4. Consistent with Article 6 of the U.S.-Italy PCSC Agreement, Paragraph 1.a of this Section is intended to apply when the individual concerned:
  - a. Is suspected, investigated, charged or convicted of terrorist related crimes as specified in the technical annex to this Understanding;

- b. Is suspected by either Side's competent authorities to belong to a criminal organization that pursues terrorist objectives, including internationally or; is receiving or has received training intended to perpetrate the crime under clause (a).
- c. Is suspected investigated, charged or convicted of immigration related offenses, as specified in the technical annex to this Understanding.
- d. Is suspected, investigated, charged or convicted of any other serious crime, as specified in the technical annex to this Understanding.

## **Section 5**

### **Procedures for the Exchange of Supplementary Information**

- 1. When the Requesting Side encounters an individual who is a potential match, the Sides may exchange personal data and additional information, as described in Section 4, through existing communication channels or through other means of communication, including the connection established through this Understanding, which is expected to be regulated by specific terms mutually decided upon by both Sides.
- 2. The Sides have decided to implement this section through the respective national contact points referred to in Section 6 of this Understanding.

## **Section 6**

### **National contact points**

- 1. For the purpose of the supply of data as referred to in Sections 4, 5, and 7 of this Understanding, the Sides designate the following as national contact points:
  - a. For the United States of America:
    - i. The U.S. Department of Homeland Security is responsible for implementing this Understanding, including the availability of reference data in the applicable U.S. automated fingerprint identification systems through U.S. Customs and Border Protection.
    - ii. For Additional Information from the FBI criminal history data base when the standards for disclosure of that data in Section 1.2 are met, the office of the FBI LEGAT in Rome/FBI Criminal Justice Information Services.
    - iii. For terrorist identity verification, the Terrorist Screening Center, U.S. Federal Bureau of Investigation.
  - b. For Italy: Central Directorate of Criminal Police – International Police Cooperation Service.

**Section 7**  
**Voluntary supply of personal and other data**  
**in order to prevent serious crime and terrorism**

Pursuant to Article 10 of the U.S.-Italy PCSC Agreement and consistent with the purpose in Section 1 of this Understanding, for the prevention of serious crimes, the Sides may, in compliance with their respective laws, even without being requested to do so, supply the other Side's relevant national contact point, personal data specified in Article 10 of the U.S.-Italy PCSC Agreement.

**Section 8**  
**Review**

The Sides intend to consult each other regularly on the implementation of this Understanding. As part of such consultations, the Sides intend to:

- a. review the number of automated queries made and the number and percentage of matches;
- b. share, to the extent practical, additional statistics and case studies demonstrating how the exchange of information under this Understanding has assisted in identifying criminals, including potential terrorists or other threats to national security; and
- c. share any privacy incidents that occur during the implementation of this Understanding, including unauthorized access or disclosure of personal information and the corrective actions taken in response to any such incidents.

**Section 9**  
**Relationship to U.S.-Italy PCSC Agreement**

This Understanding serves as an Implementing Arrangement under the U.S.-Italy PCSC Agreement and the Sides recognize that all of the provisions of the U.S.-Italy PCSC Agreement apply to this Understanding. In the event of a conflict between the provisions of this Understanding and the provisions of the U.S.-Italy PCSC Agreement, the provisions of the U.S.-Italy PCSC Agreement are intended to prevail.

**Section 10**  
**Expenses**

Each Side intends to bear its own expenses for the implementation of this Understanding. In special cases, the Sides may jointly decide otherwise.

**Section 11**  
**Dispute Resolution**

The Sides intend to consult each other in the event of a misunderstanding under this Understanding, or if they wish to modify it.

**Section 12**  
**Final Provisions**

1. This Understanding, which is of unlimited duration, takes effect upon the receipt of notifications between the primary point of contact of the Sides under Section 6.1.a and 6.1.b of this Understanding that the technical aspects for implementing this Understanding have been completed.
2. In carrying out the procedures provided for in this Understanding, the Sides intend to observe their national laws and obligations arising from the U.S.-Italy PCSC Agreement.
3. The Sides intend to inform each other of any changes to their national laws that may materially affect the operation or implementation of this Understanding.
4. This Understanding may be modified with the mutual consent of the Sides expressed in written form.
5. Either Side may discontinue this Understanding at any time, and should provide six months' written notice.

Signed at Ischia, this 20<sup>th</sup> day of October 2017 in duplicate, in the English and Italian languages both texts being equally valid.

(b)(6)

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

(b)(6)

**FOR THE MINISTRY OF  
INTERIOR OF THE ITALIAN  
REPUBLIC:**

**Implementing Arrangement  
under the Agreement between the Government of the United States of  
America and the Government of the Italian Republic  
on Enhancing Cooperation in Preventing and Combating Serious Crime,  
signed at Rome on May 28, 2009**

**TECHNICAL ANNEX (Section 1.2)**

This annex and the types of offenses listed below are intended to apply to this  
Understanding only and do not set any precedent for other bilateral cooperation under the  
U.S.-Italy PCSC Agreement.

- Participation in a criminal organization;
- terrorism offenses (including offenses set forth in UN terrorism conventions, providing material support to terrorists, providing material support to terrorist organizations, receiving or providing military-type training from or to a Foreign Terrorist Organization);
- genocide;
- torture;
- murder/manslaughter;
- serious personal injury;
- trafficking in persons;
- illicit trade in human organs and tissue;
- migrant smuggling;
- facilitation of unauthorized entry and residence;
- involuntary servitude;
- rape and other sex offenses;
- sexual exploitation of minors and child pornography;
- kidnapping, illegal restraint and hostage taking;
- exploitation of prostitution;
- trafficking in biological, chemical, or nuclear materials;
- illicit trafficking in hormonal substances and other growth promoters;
- obstruction of justice;
- perjury and subornation of perjury;
- sabotage;
- corruption;
- illicit trafficking in weapons, munitions and explosives;
- offenses relating to destructive devices or explosive materials;
- use or unlawful possession of biological, nuclear, chemical or other weapons of mass destruction;
- production, transfer, or possession of radiological dispersal devices;
- robbery;
- illicit trafficking in cultural goods, including antiques and works of art;
- trafficking in stolen vehicles;
- racketeering and extortion;
- money laundering;
- embezzlement;
- fraud;
- smuggling of goods;
- theft and trafficking in stolen goods;



- counterfeiting currency;
- counterfeiting and piracy of products;
- forgery or fraudulent use of identity papers and travel documents;
- forgery of means of payment;
- distribution or trafficking in narcotics and psychotropic substances;
- possession of, or possession with intent to sell, narcotics and psychotropic substances, except for small quantities deemed not to be serious crimes under domestic law;
- arson;
- bombings;
- unlawful seizure of aircraft/ships;
- environmental crimes including illicit trafficking in endangered animal species and in endangered plant species and varieties;
- computer crimes.

# **JOINT DECLARATION OF INTENT**

## **BETWEEN**

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

## **AND**

**THE FEDERAL MINISTRY OF THE INTERIOR, BUILDING AND  
COMMUNITY OF THE FEDERAL REPUBLIC OF GERMANY**

### **IN SUPPORT OF THE CONTINUOUS COOPERATION ON PUBLIC SECURITY AND MIGRATION MATTERS**

The Department of Homeland Security of the United States of America and the Federal Ministry of the Interior, Building and Community of the Federal Republic of Germany (hereinafter referred to as "the Participants") acknowledge the long-standing links between the United States of America and the Federal Republic of Germany and their exceptional ongoing cooperation.

The Participants, while sharing the common understanding of the importance of conferring refugee protection on those who need it, recognize the compelling need to tackle identity-related fraud and abuse of immigration laws, including fraud and abuse in resettlement and asylum systems, and understand doing so will further enhance their ability to maintain the integrity and security of both countries.

The Participants are fully aware of the risks deriving from the intensification of terrorist and criminal activities, illegal migration, and transnational challenges having a direct impact on security, and recognize the need for international cooperation to combat transnational crime, particularly those that threaten national security.

The Participants are convinced of the need to further enhance and to reinforce operational cooperation between their respective agencies with a key priority in guaranteeing the availability and effective use of identity and immigration-related information.

The Participants affirm that the protection of individuals in relation to the processing of personal data is of highest importance.

Therefore, the Participants have come to the following understanding:

The Participants intend to give priority to taking a sounding on an arrangement that, with respect to the laws of the two countries, will allow the United States of America and the Federal Republic of Germany to verify the identity of foreigners through the exchange of identity and immigration information regarding nationals of a third country.

As part of this effort, the Participants also intend to identify criminals, including potential terrorists, or other threats to national security attempting to exploit international movement of migrants, refugees and asylum seekers for mala-fide purposes through the exchange as appropriate of threat information regarding nationals of a third country.

The Participants agree on the high importance of privacy protection enshrined in their domestic laws. Therefore, they will thoroughly assess the impact of the information sharing on the protection of personal data and implement necessary measures and safeguards in order to achieve a high level of data protection, including compliance with relevant laws of each country regarding confidentiality of information. To this end, the Participants will closely consult with the competent supervisory authorities on both sides.

Signed in Washington, D.C., on 28 January 2019

For the  
Department of Homeland Security  
of the United States of America

(b)(6)

Claire M. Grady  
Acting Deputy Secretary

For the  
Federal Ministry of the Interior,  
Building and Community of  
the Federal Republic of Germany

(b)(6)

Hans-Georg Engelke  
State Secretary



Government  
of Canada

Gouvernement  
du Canada



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

May 30, 2012

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

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

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

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

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

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

### **1. Purpose Specification**

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

**2. Relevant and Necessary/Proportionate**

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

**3. Integrity/Data Quality**

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

**4. Non-Discrimination**

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

**5. Information Security**

Personal information is to be protected by appropriate technical, security and organizational procedures and measures to guard against such risks as loss; corruption; misuse; unauthorized access, alteration, disclosure or destruction; or any other risks to the security, confidentiality or integrity of the information. Only authorized individuals with an identified purpose are to have access to personal information.

**6. Accountability**

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

**7. Effective Oversight**

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

**8. Individual Access and Rectification**

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

**9. Transparency and Notice**

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

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

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

#### **10. Redress**

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

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

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

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

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

#### **12. Retention**

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

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

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



**Annex Regarding the Sharing of Information on  
Asylum and Refugee Status Claims to the Statement  
of Mutual Understanding on Information Sharing**

***Between***

**The Department of Citizenship and  
Immigration Canada  
(CIC)**

***and***

**The Bureau of Citizenship and Immigration Services (BCIS),  
of the U.S. Department of Homeland Security (DHS)**

This Annex to the Statement of Mutual Understanding of Information Sharing (SMU) sets forth the understanding between the Participants that they are to share information in the manner described herein. The provisions of the SMU apply at all times to all exchanges of information among the Participants, except as provided in this or other Annexes. This Annex addresses additional requirements or provisions applicable to refugee status claims, as described in this Annex, to the extent that the provisions in this Annex are different from, or not described in, the SMU. Notwithstanding any language used herein, however, nothing in this Annex is intended to give rise to rights or obligations under international law or the domestic laws of the Participants; the Annex reflects the firm political commitments of the Participants to operate in accordance with the provisions detailed herein.

In accordance with section 3(2) of the *Immigration and Refugee Protection Act* (IRPA), the objectives for refugees include establishing fair and efficient procedures that will maintain the integrity of the Canadian refugee status determination system, while upholding Canada's respect for the human rights and fundamental freedoms for all human beings; protecting the health and safety of Canadians and maintaining the security of Canadian society; and promoting international justice and security by denying access to Canada to foreign nationals, including refugee status claimants, who are serious criminals; violators of human and international rights; or, security risks. Under IRPA, the refugee protection definition includes the criteria from the 1951 *Convention relating to the Status of Refugees*, the *Convention against Torture* (CAT), and the further criteria of risk to life or risk of cruel and unusual treatment or punishment. In furtherance of these objectives, and as part of the process in order to provide refugee protection to those who need it, as set out in Part 2 of IRPA, CIC records personal data concerning the refugee status claimant, including biographical information, information regarding suspected or actual inadmissibility, suspected or actual ineligibility to have a refugee status claim referred to the Immigration and Refugee Board, the route by which the refugee status claimant came to Canada and other information relevant to the identity of the person or the merits of his or her claim to protection.

In accordance with sections 208 and 241(b)(3) of the *Immigration and Nationality Act* (INA), and section 2242(b) of the *Foreign Affairs Reform and Restructuring Act* (FARRA) (implementing Article 3 of the *United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*) and corresponding regulations, the United States has established fair and efficient procedures to provide protection for refugees and others who qualify for protection under those provisions and to maintain the integrity of the asylum and refugee status determination system by, among other things, denying asylum to or terminating the asylee status of individuals who are criminals, human rights abusers, or security risks. In administering such procedures, the United States records personal data concerning the refugee status claimant, including biographical information, information regarding suspected or actual inadmissibility or removability, suspected or actual ineligibility for protection, and other information relevant to the identity of the person and/or the merits of his or her claim.

In addition to the objectives set out in the preamble to the SMU, this Annex sets out specific objectives related to the sharing of information in the asylum context.

## Article 1

### Purpose

Subject to the domestic laws of the United States and Canada, and consistent with their commitments to uphold international and domestic obligations not to return qualified individuals to countries where they would face persecution or torture, the Participants intend to implement this Annex in order to

- (a) Preserve and protect their respective countries' asylum and refugee status determination systems;
- (b) Enhance their abilities to assist those who qualify for protection from persecution under the *1951 Convention relating to the Status of Refugees* (the 1951 Convention), the *1967 Protocol relating to the Status of Refugees* (the Protocol), or from torture, within the meaning of Article 1 of the *United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (the Convention Against Torture) and other protection criteria set forth in the Participants' respective domestic legislation;
- (c) Support efforts to share responsibility between the Participants in providing protection to qualified refugee status claimants, including the orderly handling of refugee status claims and the movement of refugee status claimants within North America;
- (d) Identify and prevent abuse of the Participants' asylum and refugee status determination systems and citizenship and immigration laws as defined in Article 1 of the SMU; and
- (e) Identify those who are excluded from protection under Article 1E or 1F, or denied protection according to Article 33(2) of the 1951 Convention, as implemented in the Participants' respective domestic legislation or whose refugee status may be subject to termination, cancellation or revocation.

## Article 2

### Definitions

For purposes of this Annex, the following definitions are applicable:

- (a) "Refugee status determination system" means the sum of laws and administrative and judicial practices employed by each Participant's national government for the purpose of adjudicating refugee status claims.
- (b) "Refugee status claim" generally means a request from a refugee status claimant to the government of either Participant for protection against persecution consistent with the 1951 Convention and the Protocol, and against torture, consistent with Article 1 of the Convention Against Torture, or other protection grounds in accordance with the respective laws of each Participant. In the United States, the phrase means a claim for asylum or

withholding of removal, a claim for protection under Article 3 of the Convention Against Torture, or a credible fear or reasonable fear screening for eligibility for such protection, under the Immigration and Nationality Act or FARRA and implementing regulations. In Canada, the phrase means a claim for protection pursuant to section 99 or section 112 of the Immigration and Refugee Protection Act.

- (c) "Refugee status claimant" means any person who makes a refugee status claim in the territory or at a port of entry of one of the Participants.

### Article 3

#### Applicability

This Annex does not apply to refugee status claims made by persons who are citizens of Canada or the United States or who, not having a country of nationality, are habitual residents of Canada or the United States. This Annex applies to sharing, on a systematic or case-by-case basis, of information concerning refugee status claims made in either Participant's territory. This Annex does not preclude sharing of information on a case-by-case pursuant to the SMU or any other annex to the SMU.

### Article 4

#### Authorities

- (a) United States
- (i) Under the *Immigration and Nationality Act* (INA), section 208, and Title 8 of the *Code of Federal Regulations* (CFR), part 208, the Bureau of Citizenship and Immigration Services (BCIS) has authority to establish processes for individuals seeking protection from persecution or torture. Accordingly, the collection and maintenance by BCIS of the information specified in this Annex is permissible under the Privacy Act, 5 U.S.C § 552a(e)(1), which allows agencies to collect and maintain information that is relevant and necessary to accomplish "a purpose of the agency required to be accomplished by statute or by Executive Order."
- (i) The Privacy Act restricts the ability of the BCIS to share information regarding persons who are United States citizens or Lawful Permanent Residents. Where the subject of the information has consented to the disclosure, the Privacy Act does not restrict the ability of the BCIS to disclose the information. Even in the absence of the subject's consent, however, the BCIS may disclose information relating to a United States citizen or a Lawful Permanent Resident under certain conditions described in the Privacy Act at 5 U.S.C. § 552a(b). Such conditions include where the disclosure of information is pursuant to a routine use consistent with the reasons for collecting the information when the BCIS has published notice of the routine use in the *Federal Register*.

- (iii) Sharing information relating to refugee status claims is governed by regulation at 8 CFR 208.6. The regulation prohibits disclosure to third parties of information regarding individual refugee status claimants without the subject's written consent, except as provided under specific regulatory exceptions or as authorized by the Secretary of Homeland Security.

(b) Canada

Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with provisions of the *Privacy Act*. Under IRPA and the Regulations, CIC collects personal information on refugee status claimants related to identity; admissibility; eligibility; exclusion; intervention; the merits of the refugee status claim; and, compliance with any lawful order under IRPA. Section 7 of IRPA gives authority for the Minister to enter into international agreements with foreign states for the purpose of the Act. Article 8(2) of the *Privacy Act* provides that, subject to any Act of Parliament, personal information under the control of a government institution may be disclosed, for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or, under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a foreign state or any institution thereof, for the purpose of administering any law or carrying out a lawful investigation. This Annex to the SMU is consistent with the Article 8(2)(a) of the Privacy Act, and is an arrangement for an administrative purpose as described in Article 8(2)(f) of the Privacy Act.

## Article 5

### Data Elements to be shared

There are four broad categories of information that may be shared:

- information relating to the identity of the refugee status claimant;
- information relating to the processing of the refugee status claim;
- information relevant to a decision to deny a refugee status claimant access to, to exclude such a claimant from the protection of, the refugee determination system, or to terminate, cancel or revoke an individual's existing refugee status in the United States or Canada; and
- information regarding the substance or history of previous refugee status claim(s) that will assist in determining a subsequent refugee status claim.

(1) Information relating to the identity of the refugee status claimant

Information concerning the identity of a refugee status claimant is essential to the determination of a refugee status claim. In order to establish the identity of a refugee status claimant, the officer relies upon biographic, descriptive or biometrics data. Not all of the identifying data characteristics listed below may be available for each refugee status claimant. The identification information that may be shared under this Annex includes, but is not limited to:

- Name and aliases used;
- Client identification number (for respective Participant's reference only);
- Gender (both birth and post-operative, if applicable);
- Physical description;
- Biometrics, including fingerprints, photographs and physical descriptions;
- Date of birth (both claimed and actual);
- Country of birth (both claimed and actual);
- Nationality or nationalities (both claimed and actual);
- Information relating to identity documents (e.g. passport number); and
- Other relevant identification data (e.g., FBI number, driver's license number).

(c) Information relating to the processing of the refugee status claim

Information regarding the status of a previous or ongoing refugee status claim in the country of one Participant is relevant to the determination of a refugee status claim in the country of the other Participant. This information refers to the processing of the person's refugee status claim in Canada or the United States, and consists of, but is not limited to:

- Information regarding whether the refugee status claim was denied access to the refugee determination system, has been decided, remains pending, or has been declared abandoned or voluntarily withdrawn;
  - If the refugee status claim has been decided, information on whether protection was granted or denied, including the disposition of any appeals; and
  - Information regarding the cessation or vacation of a determination on a refugee status claim.
- (c) Information relevant to a decision to deny a refugee status claimant access to, or exclude such a claimant from the protection of, the refugee status determination system or to terminate, cancel or revoke an individual's existing refugee status in the United States or Canada.

This information is relevant to the decision whether or not to allow the refugee status claimant access to the refugee status determination system. This information may also be relevant to the decision as to whether or not a person ought to be excluded from refugee protection pursuant to Article 1E or 1F or denied protection according to Article 33(2) of the 1951 Convention, as implemented in the refugee status determination systems of the Participants. In Canada, this information may also be relevant to the decision as to whether the Minister of Immigration decides to participate in the refugee status determination process pursuant to Canadian law. The information that may be shared includes, but is not limited to:

- Information related to a determination that a refugee status claimant falls or fell within the provisions of Article 1E or 1F of the 1951 *Convention Relating to Status of Refugees*, as implemented by the Participant;
- Information related to a determination that a refugee status claimant falls or fell within the provisions of Article 33(2) of the 1951 *Convention Relating to Status of Refugees*, as implemented by the Participant;

- Information concerning any outstanding criminal warrants or criminal convictions pertaining to a refugee status claimant, or the nature of any criminal offence that either Participant has reasonable grounds to suspect a refugee status claimant has committed;
  - Information concerning security allegations pertaining to a refugee status claimant, or the nature of any security risk that either Participant has reasonable grounds to suspect a refugee status claimant might present;
  - Information related to outstanding immigration warrants pertaining to a refugee status claimant or the nature of any immigration offence(s) that either Participant has reasonable grounds to suspect a refugee status claimant has committed.
- (c) Information regarding the substance or history of any previous refugee status claim(s) that will assist in determining a subsequent refugee status claim.

Information regarding previous refugee status claims is relevant to the assessment of subsequent claims, including the assessment of credibility. Such information includes, but is not limited to:

- Country of last habitual residence;
- Address;
- Marital status and family composition;
- Immigration status;
- Date(s) of arrival;
- Places(s) of entry;
- Manner of entry;
- Information concerning routes of travel;
- Occupational information;
- Education;
- Information submitted in support of a refugee status claim;
- Information related to the substance of the refugee status claim; and
- Records of decisions taken with respect to the refugee status claim, including reasons.

## **Article 6**

### **Mechanism for Sharing Data**

#### **(a) Systematic Information Sharing**

Systematic information sharing is intended to take place in three stages:

1. Comparison of data;
2. Confirmation of a match; and
3. Sharing of additional information.

Systematic information sharing is to be performed on a periodic basis, as determined by the Participants. Following confirmation of a match and subsequent exchange of information



pursuant to Article 6(a)(3), the Participants may take appropriate action pursuant to the Participants' citizenship and immigration laws as defined in the SMU.

#### 1. Comparison of data

1.1 The Participants may compare basic identification information of refugee status claimants in Canada and the United States in order to match the identity of a claimant in the refugee status determination system of one Participant with the same individual in the refugee status determination system of the other Participant. Initial comparison of basic identification information is for the purpose of matching claimants and is to include basic information such as: name, date of birth, client identification (for the Participant's reference only) and country of birth of refugee status claimants. To increase the reliability of the initial match and minimize sharing of information on mismatched claimants, biometrics technology consisting of fingerprints and photographs may be used when available to make the initial match. Upon receipt of this initial information, the receiving Participant is to check the information against its own database containing personal information of the persons who have sought protection.

1.2 When there is a prima facie match on the basis of name, date of birth and country of birth (or fingerprints when that technology becomes available), the receiving Participant is to notify the providing Participant that there is a prima facie match for the refugee status claimant. In addition, in order to assist the providing Participant in prioritizing requests for further information, the receiving Participant is to include in the notification an indication of the case status as specified in Article 5(b) and an indication as to whether the refugee status claim has raised issues of criminality, security or exclusion as specified in Article 5(c), when it can be ascertained from the electronic information. Similarly, for any potential matches, the providing Participant is to inform the receiving Participant with an indication of the case status as specified in Article 5(b) and an indication as to whether the refugee status claim has raised issues of criminality, security or exclusion as specified in Article 5(c), when it can be ascertained from electronic information.

#### 2. Confirmation of a match

Following a prima facie match, the Participants may share additional identification information as described in Article 5(a) for the purpose of confirming the match. This information is intended to enable the Participants to prioritize further requests for information.

#### 3. Sharing of additional information

Upon confirmation of the match, other data as specified in paragraphs (b), (c), and (d) of Article 5, including non-computer-based data may be shared for the purposes of assessing admissibility of the refugee status claimant, and determining the eligibility and the merits of the refugee status claim in the participant country where the claim is being adjudicated.

At each step of the process described above, non-matched data is to be immediately destroyed upon determination that it does not relate to a positive match.

(b) **Case-by-case sharing of information**

In addition to the systematic sharing of information, the Participants may, in accordance with procedures set forth in the SMU, share information described in Article 5 of this Annex concerning refugee status claims on a case-by-case basis pursuant to the request of either Participant.

**Article 7**

**Confidentiality**

- (a) Each Participant is to protect from disclosure to any non-participant, to the fullest extent provided under its country's laws and regulations, any and all information, inquiries and requests for information received from the other Participants under this Annex.
- (b) Protection of a refugee status claimant includes protecting the confidentiality of an individual's identity and of the information provided in the individual's refugee status claim, including the fact that an individual has submitted a refugee status claim. Unauthorized release of such information may place the refugee status claimant or a member of the refugee status claimant's family at risk of serious harm, including persecution and torture. Consequently, each Participant is to treat as confidential and protect from disclosure to any non-participant, to the fullest extent provided under its country's laws and regulations, any and all information, inquiries, and requests for information received from the other Participant under this Annex. The Participants are to seek to ensure that information is not exchanged or disclosed to a Participant or non-Participant in such a way as to place refugee status claimants or their families at risk in their countries of nationality, or if stateless, countries of last habitual residence.
- (c) The Participants acknowledge that written permission is not required, pursuant to Article 6(c)(i) of the SMU, for the disclosure of information related to the refugee status claim to other agencies to further their adjudication or review of refugee status claims. Thus, a Participant may, for example, release confidential information to the Executive Office for Immigration Review, United States federal courts, and the Immigration and Refugee Board and Federal Court of Canada, in connection with or in furtherance of the adjudication of a refugee status claim.
- (d) Disclosure by the receiving Participant of any information received under this Annex to foreign governments or international organizations requires the written consent of the providing Participant.

**Article 8**

**Custodians**

Each Participant is to designate a custodian to implement, monitor and ensure compliance to the terms and conditions of this Annex.

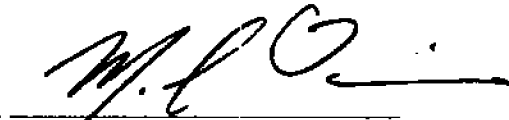
**Article 9****Duration**

Activities under this Annex commence on the date when all Participants have signed. Activities under the Annex cease sixty days after one Participant provides written notice to the others of its intention to no longer participate in the Annex.

**Article 10****Signatures**

In Witness whereof, the Participants have signed this Annex to the Statement of Mutual Understanding:

For Canada  
Department of Citizenship  
and Immigration



Michel Dorais  
Deputy Minister  
Citizenship and Immigration Canada

For the United States  
Department of Homeland Security



Eduardo Aguirre  
Director  
Bureau of Citizenship and Immigration Services

August 22nd, 2003  
Date

Aug 15, 2003  
Date

**Memorandum of Understanding between the U.S. Department of Homeland Security and the Office of the United Nations High Commissioner for Refugees on the Sharing of Personal Data**

The U.S. Department of Homeland Security (DHS), acting through its component agency U.S. Citizenship and Immigration Services (USCIS), and the Office of the United Nations High Commissioner for Refugees (UNHCR), hereinafter referred to as the "Participants,"

*Acknowledging* the commitments of the United States under the Protocol Relating to the Status of Refugees of 1967, and to resettlement under the Refugee Act of 1980 as amended;

*Acknowledging* UNHCR's mission to seek durable solutions for refugees as part of its core mandate, including voluntary repatriation, local integration, and resettlement;

*Recalling*, in this respect, the Memorandum of Understanding between UNHCR and Department of State's Bureau of Population, Refugees, and Migration (PRM) concerning resettlement referrals that involve the electronic transmission of data from UNHCR's ProGres registration database to the Worldwide Refugee Admission Processing System of 2006 and the subsequent Letters of Understanding of 2016 and 2018;

*Willing* to extend and build upon the existing channel of cooperation with PRM through this MoU with DHS particularly regarding the national security interests of the resettlement country;

*Emphasizing* the willingness of DHS and UNHCR to jointly improve the efficiency of the resettlement process through sharing of Personal Data, including Biometric Data, and technological solutions;

*Recognizing*, at the same time, that the systematic sharing of Personal Data of refugees by UNHCR with the United States Government is conditioned upon data protection safeguards as contained in, but not limited to, UNHCR's Policy on the Protection of Personal Data of Persons of Concern, the Privacy Act of 1974, 5 U.S.C. Section 552a, 8 CFR 208.6, "Disclosure to Third Parties," all of which are applied to Refugees as a matter of DHS Policy and the Fair Information Practice Principles as adopted by DHS (See DHS Privacy Policy Guidance Memorandum 2008-1, dated December 29, 2008, entitled *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*);

Have come to the following mutual understanding:

**1. PURPOSE AND SCOPE**

- 1.1 The purpose of this MoU is to regulate the sharing of Personal Data from UNHCR to DHS, including and in particular biometric data.
- 1.2 This MoU does not derogate from or supersede other agreements or arrangements between the United States of America and UNHCR, notably the 2006 *Memorandum of Understanding between UNHCR and Bureau of Population, Refugees, and Migration at the United States Department of State (PRM) concerning the resettlement of referrals that involve the electronic transmission of data from UNHCR's ProGres registration database to the Worldwide Refugee Admissions Processing System (WRAPS) signed on March 22, 2006, as modified and renewed*. It is also not a legally binding agreement and does not give rise to any rights or obligations under international law or the domestic laws of any country.

## 2. DEFINITIONS

- 2.1 Personal Data references any data that could potentially identify a specific individual; including biometric images (face, fingerprints and photograph) and biographic data (e.g. name and date of birth), similar to personally identifiable information (PII).
- 2.2 A biometric is a measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual.
- 2.3 Encounter data includes biographic Personal Data and information stored by DHS relating to the individual who has been biometrically identified using UNHCR Biometric Data, and may also include some or all of the Biographic Data transferred by UNHCR to DHS as defined in Section 3 of this MoU. Encounter data does not include biometric data, with the exception of facial images.
- 2.4 IDENT notifications are outbound messages from IDENT that inform permitted third party IDENT subscribers to the same identity that a biometric match event has occurred. The message has three primary elements: notification date, subscriber organization, and activity category text. No biometric images or biometric data is sent with a notification.
- 2.5 Third party IDENT subscribers permitted for IDENT notification services under this agreement are from DHS, or organizations listed in Section 9.3.

## 3. PERSONAL DATA TO BE TRANSFERRED

- 3.1 Once UNHCR refers an individual to the United States for resettlement, UNHCR intends , provided availability, to share the following Personal Data elements with DHS:
  - 3.1.1 Biographic Personal Data elements would include:
    - (i) Name, including family name and all given names
    - (ii) Date of birth
    - (iii) Country of origin (to be mapped to DHS's Person Nationality Text field)
    - (iv) Gender
    - (v) Unique identification number (IID) for each individual referred
    - (vi) Unique group identification number (UNHCR Group Number RRF Case ID)
    - (vii) Unique biometric ID number for each individual
    - (viii) Date and location of biometric collection by UNHCR
  - 3.1.2 Biometric Personal Data elements would include:
    - (i) Fingerprint images
    - (ii) Facial Images
    - (iii) Iris Scan images
- 3.2 The transfer of any other Biographic or Biometric Data is to be determined by the Participants through a subsequent written exchange of notes.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

## **6. MEANS OF PERSONAL DATA TRANSFER**

- 6.1 Personal Data is to be transferred by means agreed between the Participants in a separate exchange of notes, referring to this MoU.

## **7. FEEDBACK FROM THE UNITED STATES GOVERNMENT**

- 7.1 DHS intends to provide UNHCR with regular reports on the number and/or percentage of cases in which the United States finds a mismatch in identity based on the biometric comparison of data. DHS and UNHCR plan to work together to develop reporting that helps inform the success of this data sharing.
- 7.2 To the extent permitted by U.S. law and policy, DHS intends to provide UNHCR with feedback on specific cases, including those involving suspected identity fraud discovered by comparing

UNHCR data to data held by DHS, as well as any other case-specific information that may impact further processing for resettlement by UNHCR or other resettlement countries.

#### **8. RETENTION OF PERSONAL DATA**

- 8.1 The retention of Personal Data is expected to be limited to that which is necessary for the purposes as set forth in Section 4 of this MoU.
- 8.2 When the information is no longer used and destruction is permitted by law, DHS is to destroy all electronic data from its systems, as well as all paper records that it has in its possession as a result of this MoU in such a manner as to render it unreadable and unrecoverable.
  - 8.2.1 Records retention schedules are outlined in the Automated Biometric Identification System (IDENT) System of Records Notice (SORN), located in the Federal Register.

#### **9. ONWARD DISCLOSURE**

- 9.1 DHS will not share the Personal Data collected by UNHCR with any party outside of DHS except for Encounter Data which may be shared with the third parties listed in Section 9.3 under the circumstances defined in Section 9.2.
- 9.2 Under US law and policy, and in accordance with the purposes set out in Section 4, DHS will share Encounter Data with the third parties listed in 9.3 when biometrics provided by UNHCR match data held on individuals known to DHS for whom there is derogatory information.
- 9.3 Disclosure of Encounter Data is exclusively permissible under the circumstances defined in Section 9.2 above to the following third parties within the US Government:
  - 9.3.1 Department of Justice
  - 9.3.2 Department of Defense
  - 9.3.3 Department of State
  - 9.3.4 Other agencies tasked with national security and counterterrorism responsibilities
- 9.4 Notwithstanding 9.1, 9.2, and 9.3, Encounter Data generated and Personal Data shared under this MoU may be disclosed to third parties only upon prior notification and written authorization of both Parties. In advance of disclosure, the third party must provide appropriate written undertaking to the Parties that the data will not be used or further disclosed for any purpose inconsistent with the aims and objectives for which it was disclosed.

(b)(7)(E)



## **11. REVIEW AND CONSULTATION**

- 11.1 The Participants intend to regularly assess their cooperation under this MoU through a process to be developed through subsequent mutual understanding. The Participants intend to conduct such reviews at least annually.
- 11.2 The Participants intend to advise each other regarding the enactment of any legislation or policy that fundamentally affects their ability to implement this MoU.
- 11.3 The Participants intend to consult over any misunderstanding regarding the interpretation, application or implementation of this MoU.

## **12. MODIFICATION AND DISCONTINUANCE**

- 12.1 The Participants may modify this MoU by mutual decision, in writing.
- 12.2 A Participant may discontinue this MoU at any time, but is expected to give six weeks' notice in writing to the other Participant.
- 12.3 Any data transferred to DHS pursuant to this MoU prior to the effective date of a notice of discontinuance may be retained by DHS and is expected to be protected pursuant to this MoU.

## **13. COSTS**

- 13.1 The Participants understand that performance of this MoU is subject to the respective availability of funds. Each Participant intends to pay its own costs for the use of its own equipment and personnel in performing its activities under this MoU. No provision in this MoU is intended to be interpreted to require the obligation or payment of any funds, including the obligation or payment of funds in the violation of U.S. law or the UN Charter.

## **14. FINAL PROVISIONS**

- 14.1 This MoU is intended to become operative on the date of signature and is expected to remain operative unless discontinued as provided in Section 12.2.
- 14.2 Nothing in or relating to this MoU is intended to operate as a waiver, express or implied, of any privileges or immunities of the United Nations or of UNHCR, as a subsidiary organ of the United Nations.

## **15. POINTS OF CONTACT**

- 15.1 For DHS
  - 15.1.1 USCIS, Immigration Records and Identity Services
  - 15.1.2 USCIS Refugee Affairs Division
- 15.2 For the Office of the United Nations High Commissioner for Refugees (UNHCR)
  - 15.2.1 Identity Management and Registration Section, Division of Programme Support and Management
  - 15.2.2 Resettlement Service, Division of International Protection
  - 15.2.3 Legal Affairs Service

Signed in duplicate in the English language.

For the U.S. Department of Homeland Security:

**TAMMY M  
MECKLEY**

Digitally signed by TAMMY M MECKLEY  
DN: c=US, o=U.S. Government, ou=Department  
of Homeland Security, ou=USCIS, ou=People,  
cn=TAMMY M MECKLEY,  
0.9.2342.1.9200300.100.1.1=0378602930.USCIS  
Date: 2019.01.08 13:58:48 -05'00'

Tammy Meckley  
Associate Director, Immigration Records and  
Identity Services, USCIS

Date: \_\_\_\_\_

For the United Nations High Commissioner for  
Refugees:

(b)(6)

Preeta Law  
Deputy Director, Head of Resettlement Service,  
Division of International Protection, UNHCR

Date: January 9, 2019

## **APPENDIX A**

### **1. Disclosure to other organizations or persons**

- 1.1. Pursuant to 8 CFR 208.6 (and extended to refugees by policy) information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determinations is generally not disclosed to other organizations or persons, except under certain limited circumstances.
  - 1.2. Confidentiality is breached when an unauthorized disclosure allows the other organization or person to link the identity of the applicant to:
    - 1.2.1. The fact that the applicant applied for asylum;
    - 1.2.2. Specific facts or allegations pertaining to the individual asylum claim contained in the asylum application, or
    - 1.2.3. Facts or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum/refugee.
  - 1.3. The protection is indefinite, including where the asylum application has been denied.
2. Disclosure is permissible to DHS and other organizations as specified in Section 9 for the purposes listed in Section 4 of this agreement.

[END OF AGREEMENT]

MEMORANDUM OF UNDERSTANDING  
BETWEEN  
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE  
DEPARTMENT OF HOMELAND SECURITY, GOVERNMENT OF THE UNITED STATES  
OF AMERICA  
AND  
CYBER SECURITY AGENCY,  
GOVERNMENT OF THE REPUBLIC OF SINGAPORE  
ON  
COOPERATION IN THE AREA OF CYBERSECURITY

The National Protection and Programs Directorate, Department of Homeland Security of the Government of the United States of America and the Cyber Security Agency of the Government of the Republic of Singapore (hereinafter referred to collectively as the "Participants"),

Noting our shared vision to achieve global prosperity through an open and secure cyberspace;

Recognizing our interdependence in cyberspace and, as leading online economies, our shared interest in protecting critical infrastructure and ensuring a safe and reliable Internet that supports innovation and economic and social development;

Recognizing the benefits of close cooperation between our governments in sharing expertise and working together to secure cyberspace in the future;

Considering that governments, businesses and consumers are increasingly faced with a variety of cyber threats and there is a need to further improve cybersecurity readiness and raise awareness around the importance of keeping systems secure; and

Recognizing the importance of cooperation by the two organizations in the area of cybersecurity,

Have reached the following understanding:

SECTION 1  
Basic Principles

The Participants hereby confirm their intention to promote closer cooperation and the exchange of information pertaining to cybersecurity in accordance with the laws and regulations of their respective countries and on the basis of equality, reciprocity and mutual benefit.

## SECTION 2

### Scope of Bilateral Cooperation

The scope of cooperation between the Participants may include the following areas relating to cybersecurity: information sharing, incident response, critical infrastructure protection, risk management, awareness raising, capacity building and workforce development. Additional topics may be added as mutually determined by the Participants.

## SECTION 3

### Implementation

Each Participant may identify and facilitate cooperation on a range of activities, including but not limited to the following:

- a) Establishment of regular information exchange through secure communication mechanisms on cybersecurity issues, including indicators of compromise and mitigation measures, in order to prevent incidents and their recurrence;
- b) Coordination of response to cybersecurity events that may occur;
- c) Exchange of assessments of the prevailing cybersecurity trends and best practices, including with respect to the cybersecurity of critical infrastructure;
- d) Conduct cybersecurity exercises;
- e) Raising of awareness regarding cybersecurity with respective constituents; and
- f) Cooperation in capacity building activities.

## SECTION 4

### Funding

Each Participant is expected to be responsible for its own costs incurred in furtherance of this Memorandum of Understanding. The cost of joint cooperative activities is intended to be shared by the Participants in a manner to be mutually determined.

## SECTION 5

### Intellectual Property Rights

1. The Participants do not expect to transfer ownership in any intellectual property provided under this Memorandum of Understanding.
2. The Participants intend to follow the principles of existing U.S.-Singapore bilateral agreements for the case-by-case basis allocation of any intellectual property rights arising out of any activity under this Memorandum of Understanding.
3. In the event intellectual property is created, developed or generated out of any activity under this Memorandum of Understanding and the principles of existing U.S.-Singapore bilateral

agreements do not adequately address the allocation of rights, the Participants intend to reserve the option of entering into a separate and appropriate arrangement to govern the allocation of ownership of such intellectual property rights.

## SECTION 6

### Release of Information

It is intended that a Participant may disclose or distribute any information transmitted by the other Participant in the process of cooperative activities under this Memorandum of Understanding, but the Participants do not intend to disclose or distribute transmitted information that is specific to the cyber incidents of either country. The participants intend to disclose and distribute any transmitted information in accordance with the Traffic Light Protocol.

In the event of unauthorized use or disclosure, the Participants should exercise best efforts to notify each other without delay. Both Participants should jointly decide on appropriate measures to address such unauthorized use or disclosure of information.

## SECTION 7

### Modifications

This Memorandum of Understanding may be modified in writing by mutual consent of the Participants.

## SECTION 8

### Resolution of Differences

In the event of differences concerning the interpretation or implementation of this Memorandum of Understanding, the Participants should promptly undertake consultations with each other with the aim of amicably resolving the issue, without reference to any international court, tribunal or other forum.

## SECTION 9

### Validity

1. This Memorandum of Understanding is not legally binding.
2. This Memorandum of Understanding is intended to become operative on the date of its signature and remain in effect for a period of five (5) years.
3. This Memorandum of Understanding may be extended at any time, before its expiration, by mutual written consent of the Participants and for such period as may be mutually understood in writing.

4. This Memorandum of Understanding may be discontinued at any time, by either Participant giving at least one (1) month's prior notice in writing to the other Participant.
5. The expiration of this Memorandum of Understanding is not expected to affect any cooperative activities carried out under Sections 2 and 3 that had commenced prior to the expiration of the Memorandum of Understanding.

Signed in duplicate at Washington, on 2 August 2016, in the English language,

FOR THE GOVERNMENT  
OF THE UNITED STATES OF AMERICA:

(b)(6)



Suzanne Spaulding  
Under Secretary  
National Protection and Programs Directorate,  
Department of Homeland Security of  
the Government of the United States of America

FOR THE GOVERNMENT OF  
THE REPUBLIC OF SINGAPORE:

(b)(6)



David Koh  
Chief Executive  
Cyber Security Agency of  
the Government of the Republic of Singapore