



OFFICIAL

A guide to interpreting M5 match results

Standard Operating Procedure

Document ID (PPN)	IIB-1530
TRIM Record Number	ADD2025/974589
BCS Function	Intelligence, identity, and biometric management
Document Owner	Senior Director Identity & Biometrics Forensic Services Branch
Approval Date	05 March 2025
Document Contact	Biometric Resolution Section, M5 Helpdesk s. 22(1)(a)(ii)@homeaffairs.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Table of Contents

1.	Purpose	3
2.	Scope	3
2.1.	In Scope	3
2.2.	Out of Scope	3
3.	Standard Operating Procedure	3
3.1.	M5 data sharing arrangement	3
3.2.	How to use M5 information	4
3.3.	How a match assists with an identity assessment	4
3.4.	Client Search Portal and the Biometric Interaction Tab	5
3.5.	Biometric Match Indicator	5

s. 47E(d)

3.9.	Partner Specific Information	9
------	------------------------------	---

s. 33(1)(b)

4.	Statement of Expectation	29
5.	Accountabilities and Responsibilities.	30
6.	Version Control	30
	Attachment A - Definitions	31
	Attachment B – Assurance and Control Matrix	32
	Attachment C – Consultation	33
1.1	Internal consultation	33
1.2	External consultation	33

1. Purpose

The Migration Five (M5), formerly known as the Five Country Conference (FCC) is a consortium of the immigration agencies of Australia (AUS), New Zealand (NZ), the United Kingdom (UK), the United States (US) and Canada. The five countries have entered into agreements to exchange biometric information (fingerprints) against their respective immigration databases. The M5 objectives are to *“detect, deter and prevent mala fide (with intent to deceive) travelers, while ensuring bona fide travelers can move without undue delay or cost – where they are already known to an M5 member – to realise the benefits of cost savings, security and the integrity of our immigration systems”*.

This arrangement is in line with the Five Country Conference High Value Data Sharing Protocol and the relevant Memorandum of Understanding between the Department of Home Affairs (the department) and each of the M5 partners.

The purpose of the Standard Operating Procedure is to provide guidance to decision makers and the Biometrics Resolution Section in interpreting the Migration Five match results in the Client Search Portal for the UK, Canada, the US and NZ.

2. Scope

2.1. In Scope

This Standard Operating Procedure (SOP) covers M5 match codes and their interpretation.

2.2. Out of Scope

This SOP does not cover the interpretation of Biometric Match Indicators (BMIs) that are not related to M5 matching.

3. Standard Operating Procedure

3.1. M5 data sharing arrangement

The Biometric Resolution Section (BRS) manages the operational relationship with M5 countries and requests data from them, either automatically from the US, NZ and Canada for visa applicants located in certain countries applying for certain visa subclasses, or manually on a weekly basis from the UK. These requests are known as M5 referrals.

There are three levels of queries, with each successive response providing more information. The initial search to each of the M5 partners is based on a fingerprint match. If the fingerprints are a match, the partner country can be sent additional queries.

- Level 1 includes whether there is a match or not, and if there is a match, it provides basic biographic data for each biometric event and a facial image if available.
- Level 2 includes additional document data and biometric encounters. Note that for referrals to the US, NZ and Canada, Levels 1 and 2 information will be received at the same time due to the automated process, however this is not necessarily the case for information from the UK.

- Level 3 provides the opportunity to ask specific questions about a match.

The information returned in Level 1 and 2 responses is specified in bi-lateral agreements and generally includes the following data elements:

- Date, location and reason fingerprinted
- Last name, first name, any other names
- Date and place of birth, nationality and gender
- Travel document number, visa type and visa outcome
- Facial image, and/or scan of the travel document's bio-data page
- s. 47E(d) or derogatory information (where available)

The information provided under all three levels is dependent on the information held by the M5 partner country, and their ability to lawfully disclose that information. As such, responses may vary between countries.

s. 47E(d)

3.2. How to use M5 information

All biometric match information is potentially valuable and even if not adverse, may be useful in corroborating or establishing the client's story. Adverse match information could relate to immigration infringements, fraud, s. 47E(d). All adverse information should be investigated and should be viewed in the light of applicant declarations and their character.

3.3. How a match assists with an identity assessment

M5 information can support or negate a person's claimed identity. A match can indicate whether a person has made an application to, or visited an M5 country under a particular nationality, residency and/or identity.

Inconsistencies in the person's identity could be minor and/or due to data error. For example, most clients that do not know their DOB will have a default DOB of 01/01/year or 31/12/year depending on the organisation that registered that client. Such differences could be considered acceptable.

Some inconsistencies may be greater and may indicate that a fraudulent identity has been used. You must consider which identity, if any, is likely to be genuine.

An identity may be considered supported where a match indicates that a person has travelled to a partner country whose processes we have assessed as having a high level of trust. In these cases the providing country may hold a travel document and possibly other identity documents to support the identity. However if the person has only applied for a visa but has not been granted and has not travelled, there may be a lower level of assurance with that identity as it may not have been verified. Regardless, an M5 match will confirm that a person has provided biometrics and documentation at a certain place and point in time, to one or more of our M5 partners.

s. 47E(d)

Further information may be requested from partner countries by raising a Biometric Issue Referral in the Client Search Portal. The instructions can be found here: [BIR 1 page for ICH.docx \(bcz.gov.au\)](#).

3.4. Client Search Portal and the Biometric Interaction Tab

The Client Search Portal (CSP) is the Department's preferred client search system, providing officers with a consistent, comprehensive and up-to-date summary view of a client's core details, business interactions and dealings with the Department. The Biometric Interaction Tab of the client's record within CSP holds all biometric information including the results of internal matching and checks to law enforcement records and M5 partners.

The *CSP FCC Advance User* access is required to view match results in the CSP. This role can be requested through easySAP using role code: **SECS-CSP_FCC_ADVANCE_USER**.

s. 47E(d)

3.5. Biometric Match Indicator

A Biometric Match Indicator (BMI) is generated as a result of a number of matching rules that are triggered on biometric collection. The BMI is sent to ICSE or IRIS and is designed to assist decision makers.

It is important to note that BMIs are enrolment specific. A client may have had their biometrics collected during previous interactions with the Department, these are displayed chronologically in the Client Search Portal (CSP).

When biometrics are collected they are compared to fingerprints and facial images within the Department's holdings. s. 47E(d)

When a fingerprint is checked with an M5 partner the BMI for that specific enrolment will be displayed as Amber when checks are pending, and Green when checks are cleared and no derogatory information is received. s. 47E(d)

s. 47E(d)

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 47E(d)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

3.9. Partner Specific Information

The elements that make up an M5 response are different for each partner and have been negotiated based on what is available from the providing country and what is deemed appropriate for sharing. Level 1 information, for example the name, DOB and nationality fields are consistent across M5 partners.

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

s. 33(1)(b)

s. 47E(d)

s. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 33(1)(b)

s. 47E(d)

s. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

S. 47E(d)

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 33(1)(b)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

S. 33(1)(b)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 33(1)(b)

4. Statement of Expectation

The APS Code of Conduct states that an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction under subsection 13(5) of the Public Service Act 1999 (the Public Service Act).

Failure by an APS employee to comply with any direction contained in this SOP may be determined to be a breach of the APS Code of Conduct, which could result in sanctions under subsection 15(1) of the Public Service Act.

The Secretary's Professional Standards Direction, issued under subsection 55(1) of the Australian Border Force Act 2015, (the ABF Act) requires all IBP workers who are not employed under the Public Service Act to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in this SOP may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

All IBP workers who make decisions or exercise powers or functions under legislation have a duty to do so in accordance with the requirements of the legislation and legal principles.

5. Accountabilities and Responsibilities.

Role	Description
BRS Manager	Oversight of entire process.
Department decision makers	Reviews the M5 match results in CSP, submits a request for additional information to BRS and makes informed visa decisions based upon the match information received from the M5 partner.

6. Version Control

Version number	Date of issue	Author(s)	Brief description of change
0.1	April 2018	s. 22(1)(a)(ii)	Drafted SOP
0.2	May 2018		Reviewed SOP
0.3	May 2018		Reviewed SOP
0.4	June 2018		Reviewed SOP and provided feedback
0.5	June 2018		Reviewed SOP
0.6	June 2018		Reviewed SOP and provided feedback
0.7	June 2018		Reviewed SOP and provided feedback
0.8	July 2018		Reviewed SOP and provided feedback
0.9	July 2018		Reviewed SOP and made some changes
0.10	July 2018		Reviewed SOP and made some changes
0.11	August 2018		Reviewed SOP
0.12	August 2018		Reviewed SOP and made final changes
1.0	November 2018		Finalised version for publication on PPCR
2.0	December 2021		Reviewed and made some changes
2.1	December 2021		Reviewed and made some changes
2.2	December 2021		Reviewed SOP and made some changes
3.0	March 2022		Provided content for the Department of Defense watchlist Codes
3.1	March 2022		Reviewed
3.2	March 2022		Reviewed changes
3.3	March 2022		Reviewed SOP and made final changes
3.4	November 2022		Provided content for Citizenship
3.5	February 2024		Addition of disclosure table and other minor changes
3.4	January 2025		Reviewed SOP
3.5	January 2025		Reviewed SOP
3.6	January 2025		Reviewed SOP and made some changes
3.7	March 2025		Reviewed SOP and made final changes

Attachment A - Definitions

Term	Acronym (if applicable)	Definition
Migration 5	M5	The M5 participants are the governments of AUS, NZ, UK, US and Canada. These countries exchange data for immigration, visa and citizenship purposes.
Client Identifier	CID	Unique ICSE Client Identifier number.
Client Search Portal	CSP	The Department of Home Affairs' immigration and citizenship client database which consolidates data from various source systems. Presents a comprehensive summary of the client's business dealings with the Department and provides the only complete view of biometric match information.
Biometric Match Indicator	BMI	Only applicable to offshore fingerprint and Citizenship facial enrolments. Shows the result of various matching rules. A Red BMI should be investigated, they indicate Irregularities found were in the automatic biometric comparisons. Amber indicates automatic biometric comparisons are underway with an M5 partner and Green indicates no irregularities were found in the automatic biometric comparisons.
Biometric Resolution Section	BRS	BRS is responsible for conveying and coordinating data exchanges with M5 partners. It also provides support in regard to interpreting match results and facilitates additional manual requests.

Attachment B – Assurance and Control Matrix

1.1. Powers and Obligations

Implementation of this SOP does not require any powers, delegations or authorisations.

1.2. Control and Assurance

Related Policy	<u>Identity - Policy Statement (IIB-6798)</u>
Procedures / Supporting Materials	s. 47E(d)
Training/Certification or Accreditation	NIL
Other required job role requirements	NIL
Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	Advice and outreach can be provided by the Biometric Resolution Section at s. 22(1)(a)(ii)@homeaffairs.gov.au
Escalation arrangements	Escalation of concerns or issues can be sent to s. 22(1)(a)(ii)@homeaffairs.gov.au
Recordkeeping (e.g. system based facilities to record decisions)	All correspondence and decisions regarding M5 queries are saved in departmental systems and/or the department's record management system, Content Manager.
Program or Framework (i.e. overarching Policy Framework or Business Program)	<u>Identity - Policy Statement (IIB-6798)</u>
Job Vocational Framework Role	Program Implementation - Program Delivery

Attachment C – Consultation

1.1 Internal consultation

- Biometrics and Data Exchange Section
- Caseload Integrity and Logistics Section
- Privacy Information Disclosure Section
- Citizenship Program Delivery
- All staff in accordance with clause 1.7 of the Department of Home Affairs Workplace Determination 2019.

1.2 External consultation

M5 partners – the United Kingdom, Canada, United States and New Zealand



OFFICIAL: Sensitive

Biometric Collection and Exchange

This factsheet provides information about the Department of Home Affairs' biometrics collection and exchange arrangements.

Biometrics Collection

The Department uses biometrics for identity verification and confirmation of an applicant's identity for any visa application requiring biometrics. In most cases, if an applicant has had biometrics collected for the purposes of one visa application, and subsequently makes an application for a different visa, they will be required to provide biometrics for the purposes of that visa application.

The collection program underpins the Department's international data sharing obligations and maintains the integrity and security of the traveller and migration programs. Data sharing with international partners is an essential and mainstream element of global migration and border management processes.

Offshore collection

The Department's Offshore Biometric Collection Program (OBCP) commenced collecting fingerprints and facial images from visa applicants in December 2010 with an initial target of 17 countries managed by 10 offshore posts. s. 47E(d)

Currently, the Department collects biometrics (fingerprints and facial images) from applicants in 53 countries across a range of visa products, as a requirement of their visa application.

Onshore collection

The Department collects biometrics from a broad range of persons seeking access to Australia's borders including illegal Foreign Fishers in immigration detention; citizenship applicants s. 47E(d) unlawful non-citizens in immigration detention onshore; onshore permanent protection visa applicants; onshore visitor visa renewal applicants and travellers using SmartGates s. 47E(d)

Further information: s. 47E(d)

When are biometrics required?

Visa applicants must provide their biometrics (facial image and fingerprints) if they apply from a country, or for a visa, that is part of the Department's Biometric Collection Program. Further information about the participating countries and visas is available on the Department's website.

OFFICIAL: Sensitive

How we collect biometrics?

Biometrics (or personal identifiers) collected under the Program are digital facial images and 10-digit fingerprint scans obtained using a digital fingerprint scanner. The process is quick, discreet and non-intrusive.

The Department has contracted Australian Biometrics Collection Centres (ABCCs) to provide biometric collection services. ABCCs charge a service fee to the visa applicant for the collection of biometrics.

Visa applicants in participating countries, who are required to provide biometrics, are sent a biometrics request letter shortly after lodgement of their visa application. Applicants who receive a letter must attend an ABCC in person and provide their biometrics.

How do we store biometrics?

The Department stores applicant facial images and fingerprints in a Departmental database which can only be accessed by authorised officers.

The Department retains and uses biometrics collected offshore in subsequent visa applications. That is, visa applicants whose initial application was granted offshore but who later apply onshore to renew their visa may be required to provide biometrics.

Exclusions, Exemptions and Waivers

Further information about the policy waivers, exclusions and exemptions is in the S. 47E(d)

Exchange

Who do we share our data with?

S. 47E(d)

What is checked against M5 partners?

The M5 network involves automated exchange of fingerprint data via the Secure Real Time Platform (S RTP) with three of the partners (NZ, CAN, and the US), while the UK operates manually via the Secure File Sharing Service (SFSS) and is S. 47E(d).

Confirmed matches are recorded in Departmental systems S. 47E(d)

S. 47E(d)

M5 information is protected by strict administrative, technical, and physical safeguards appropriate to the sensitivity of the information. Privacy measures are articulated and given effect in bilateral treaties, arrangements and annexes. The S RTP completed a Privacy Impact Assessment prior to commencement.

Legislative and policy framework for biometric collection and exchange

The Department collects, retains, uses and discloses personal identifiers under the following legislative and policy frameworks and procedural instructions with further information at **Attachment A**.

Attachment A

Legislation

Legislation underpinning the biometric collection and exchange program includes:

For collection:

- Migration Act s257A – person may be required to provide personal identifiers
- Privacy Act APP 3 – collection of solicited personal information
- Privacy Act APP5 – notification of the collection of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))

Further information on the historical and current legislative basis is at 3.1 of the IIB-1486.

For exchange:

- Migration Act s336E – disclosing identifying information
- Migration Act s336F – authorising disclosure of identifying information to foreign countries etc.
- Privacy Act APP6 – use and disclosure of personal information
- Privacy Act APP8 – cross-border disclosure of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))
- Bilateral arrangements are realised under either under a Treaty (for all connections with the US) or a Memorandum of Understanding/Arrangement (MOU/MOA) (for all connections to which the US is not a party). These information-sharing arrangements are designed to meet policy, privacy and legal conditions for international data exchange.
 - These data sharing arrangements are future proofed, high-level documents and cover data exchange for all immigration purposes.
 - The Secure Real Time Platform has a Privacy Impact Assessment.

Definitions:

- Migration Act Section 5A – meaning of personal identifier
- Privacy Act Section 6(1) – meaning of sensitive information and personal information

Policies, procedures and standard operating procedures

The Department's approach to identity and biometrics complies with existing policies and frameworks including:

S. 47E(d)

- List of relevant Policy Statements, Procedural Instructions (PIs) and Standard Operating Procedures

s. 47E(d)

Policy
Statement

IIB-6798

Identity

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982



OFFICIAL: Sensitive

Biometric Collection and Exchange

This factsheet provides information about the Department of Home Affairs' biometrics collection and exchange arrangements.

Collecting biometrics (facial images and/or fingerprints) from visa applicants is a critical step in anchoring identity to improve security and safety for travellers and the Australian community. Biometric collection improves the integrity of Australia's visa program, reduces identity fraud, and reduces forum and visa shopping s. 47E(d)

s. 47E(d)

The Biometric Collection and Exchange programs operate under the authority of the *Migration Act 1958* and its *Regulations*, *Citizenship Act 1948* and its *Regulations*, and the *Australian Border Force Act 2015*. The *Privacy Act 1988* governs how personal identifiers and information are managed, and the *Freedom of Information Act 1982* provides clients with right of access to the personal information we collect and exchange.

Biometrics Collection

The Department uses biometrics for identity verification and confirmation of an applicant's identity for any visa application requiring biometrics. In most cases, if an applicant has had biometrics collected for the purposes of one visa application, and subsequently makes an application for a different visa, they may be required to provide biometrics for the purposes of that visa application.

The collection program underpins the Department's international data sharing obligations and maintains the integrity and security of the traveller and migration programs. Data sharing with international partners is an essential and mainstream element of global migration and border management processes.

Offshore collection

The Department's Offshore Biometric Collection Program (OBCP) commenced collecting fingerprints and facial images from visa applicants in December 2010 with an initial target of 17 countries managed by 10 offshore posts. s. 47E(d)

Currently, the Department collects biometrics (fingerprints and facial images) from applicants in 53 countries across a range of visa products, as a requirement for their visa application. Further information about these countries and visas is available on the [Department's website](#).

OFFICIAL: Sensitive

s. 47E(d)

The collection of biometrics offshore enables cost effective risk mitigation of threats well before they reach our shores, s. 47E(d)

Onshore collection

The Department collects biometrics from a broad range of persons seeking access to Australia's borders including:

- illegal Foreign Fishers in immigration detention
- citizenship applicants s. 47E(d)
- unlawful non-citizens in immigration detention onshore
- onshore permanent protection visa applicants – s40 of the *Migration Act 1958* ('the Migration Act') mandates the collection of biometrics from onshore permanent protection visa applicants. Temporary visa applicants are not required to provide biometrics
- onshore visitor visa renewal applicants – clients who initially entered Australia through the visitor visa program and who subsequently apply to renew their visa onshore may be required to provide biometrics.
- travellers using SmartGates s. 47E(d)

Further information: s. 47E(d)

When are biometrics required?

Visa applicants must provide their biometrics (facial image and fingerprints) if they apply from a country, or for a visa, that is part of the Department's Biometric Collection Program.

Further information about the participating countries and visas is available on the [Department's](#) website.

How we collect biometrics?

Biometrics (or personal identifiers) collected under the Program are digital facial images and 10-digit fingerprint scans obtained using a digital fingerprint scanner. The process is quick, discreet and non-intrusive.

The Department has contracted Australian Biometrics Collection Centres (ABCCs) to provide biometric collection services. ABCCs charge a service fee to the visa applicant for the collection of biometrics. The Australian Government manages this fee and it is benchmarked against Australia's other international partners and in line with equitable international standards.

Visa applicants in participating countries, who are required to provide biometrics, are sent a biometrics request letter shortly after lodgement of their visa application. Applicants who receive a letter must attend an ABCC in person and provide their biometrics.

How do we store biometrics?

The Department stores applicant facial images and fingerprints in a Departmental database which can only be accessed by authorised officers.

The Department retains and uses biometrics collected offshore in subsequent visa applications. That is, visa applicants whose initial application was granted offshore but who later apply onshore to renew their visa may be required to provide biometrics.

Under the *Archives Act* 1983, the Department is permitted to retain biometrics and the Department's Record Authority 2018/00083401, specifies retention of fingerprint biometrics for 75 years from the date of collection.

Exclusions and Exemptions

Policy Exclusions

s. 47E(d)

Policy Exemptions

s. 47E(d)

s. 47E(d)

s. 47E(d)

Exchange

Who do we share our data with?

s. 47E(d)

What is checked against M5 partners?

The Department has been verifying identity through exchanging biometric data with Australia's M5 partners since 2009. s. 47E(d)

The M5 network involves automated exchange of fingerprint data via Secure Real Time Platform (SRTP) with three of the partners (NZ, CAN, and the US), while the UK operates manually via the Secure File Sharing Service (SFSS) s. 47E(d)

Confirmed matches are recorded in Departmental systems s. 47E(d)

s. 47E(d)

M5 information is protected by strict administrative, technical, and physical safeguards that is appropriate to the sensitivity of the information. Privacy measures are articulated and given effect in bilateral treaties, arrangements and annexes. The SRTP completed a Privacy Impact Assessment prior to commencement.

Legislative and policy framework for biometric collection and exchange

The Department collects, retains, uses and discloses personal identifiers under the following legislative and policy frameworks and procedural instructions with further information at **Attachment A**.

Attachment A

Legislation

Legislation underpinning the biometric collection and exchange program includes:

For collection:

- Migration Act s257A – person may be required to provide personal identifiers
- Privacy Act APP 3 – collection of solicited personal information
- Privacy Act APP5 – notification of the collection of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))

Further information on the historical and current legislative basis is at 3.1 of the IIB-1486.

For exchange:

- Migration Act s336E – disclosing identifying information
- Migration Act s336F – authorising disclosure of identifying information to foreign countries etc.
- Privacy Act APP6 – use and disclosure of personal information
- Privacy Act APP8 – cross-border disclosure of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))
- Bilateral arrangements are realised under either under a Treaty (for all connections with the US) or a Memorandum of Understanding/Arrangement (MOU/MOA) (for all connections to which the US is not a party). These information-sharing arrangements are designed to meet policy, privacy and legal conditions for international data exchange.
 - These data sharing arrangements are future proofed, high-level documents and cover data exchange for all immigration purposes.
 - The Secure Real Time Platform has a Privacy Impact Assessment.

Definitions:

- Migration Act Section 5A – meaning of personal identifier
- Privacy Act Section 6(1) – meaning of sensitive information and personal information

Policies, procedures and standard operating procedures

The Department's approach to identity and biometrics complies with existing policies and frameworks including:

S. 47E(d)

- List of relevant Policy Statements, Procedural Instructions (PIs) and Standard Operating Procedures (SOPs):

Type	Reference	Title
------	-----------	-------

s. 47E(d)

Policy Statement	IIB-6798	Identity
------------------	----------	----------

s. 47E(d)

FOR OFFICIAL USE ONLY / OFFICIAL

Automated

Annex to the

Memorandum of Arrangement between the Government of New Zealand as represented by the Ministry of Business, Innovation and Employment (Immigration New Zealand) and the Commonwealth of Australia as represented by the Department of Immigration and Border Protection Regarding the Exchange of Information

Concerning the Automated Exchange of Information

Pursuant to the provisions of the Memorandum of Arrangement (the MOA) between the Government of New Zealand as represented by the Ministry of Business, Innovation and Employment (Immigration New Zealand) and the Commonwealth of Australia as represented by the Department of Immigration and Border Protection Regarding the Exchange of Information, signed on 6/09/2016²⁰¹⁶, Immigration New Zealand and the Department of Home Affairs (formerly the Department of Immigration and Border Protection), hereinafter referred to collectively as the "Participants", have mutually come to the following understanding:

1. General

- 11/9/2023
- (a) This Annex is made in accordance with paragraph 3(b) of the MOA.
 - (b) Information exchanged pursuant to this Annex to the MOA is subject to the provisions, including any conditions included therein, of the MOA. Any guidance on the interpretation and application of this Annex is intended to be read in conjunction with the MOA.
 - (c) The Participants intend to resolve any differences regarding the interpretation and application of this Annex through mutual consultation.
 - (d) This Annex is not intended to affect the exchange of information between the Participants under other established information sharing arrangements or Agreements, including other annexes to the MOA.

Automated

2. Purpose

- (a) Pursuant to paragraph 3(b) of the MOA, the purpose of this Annex is to establish conditions under which the Participants intend to automatically exchange Information to assist in the administration and enforcement of their respective immigration and citizenship laws, as described in Paragraph 1(b) of the MOA and consistent with their respective domestic laws.

3. Definitions

- (a) Definitions in the MOA are to be incorporated by reference within this Annex.
- (b) For the purpose of this Annex:
 - i. "Information" means data collected for the purpose of administering or enforcing the Participants' respective domestic immigration and citizenship laws, and includes but is not limited to Personal Information, policy documents and best practices, procedures, trend analysis, and statistical data.
 - ii. "Personal Information" means Information that relates to an individual who can be identified (i) from that Information or (ii) from that Information and other information that is in the possession of, or is likely to come into the possession of, the Participant, including identifying information such as biographic details or personal information/biometrics, any immigration or citizenship decisions made related to the individual, and any indication of the intent on the part of the Participant or any other person that would have the effect of identifying the individual.
 - iii. "Automatic" refers to an electronic sharing process initiated by a Participant who has reason to request Information:
 - A. pertaining to an individual that may generate Information relevant for administering or enforcing its domestic immigration and citizenship laws; or
 - B. that is relevant to the other Participant for the purpose of administering or enforcing its domestic immigration and citizenship laws.
 - iv. "Requesting Participant" means the Participant to this Annex that has initiated the query.
 - v. "Providing Participant" means the Participant to this Annex that receives the query from the Requesting Participant.
 - vi. "Query" means a Participant's request for Information, through an Automatic search process requiring minimal human intervention and is In Writing.

Automated

- vii. "Identifier" means agreed personal information/biometric and/or biographic Information used in a Query.
- viii. "Migration Five Partner Match Indicator(s)" means a data element that indicates another Migration Five Partner may know the individual because that Migration Five Partner has previously shared information with the Providing Participant.

4. Exchange of Information

- (a) If a Participant determines that exchanging Information under this Annex is inconsistent with its domestic laws and policies or international obligations, or may prejudice or cause harm to its national sovereignty, national security, public policy, or other important national interest, or could compromise an ongoing investigation, a Participant may decline to provide all or part of the Information or offer to provide all or part of the Information subject to such terms and conditions as it may specify.

5. Sending Queries:

- (a) The Participants intend to send Queries to each other seeking Information on individuals
 - i. intending to board a craft for the purpose of travelling to a Requesting Participant's territory e.g. those undergoing advance passenger processing;
 - ii. applying for:
 - 1. permission to travel to or remain in a Requesting Participant's territory;
 - 2. recognition in a Requesting Participant's territory under the:
 - a. 1951 Convention relating to the Status of Refugees or its 1967 Protocol relating to the Status of Refugees; or
 - b. 1984 Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment; or
 - c. 1966 International Covenant on Civil or Political Rights (together, "specified international agreements") and its Second Optional Protocol aiming at the abolition of the death penalty; or
 - iii. being investigated by a Requesting Participant in order to:
 - 1. cancel any visa held;

Automated

2. determine whether any person has complied with immigration obligations;
 3. deport or remove any person;
 4. exclude any person; or
 5. cancel any person's recognition, or to cease any person's recognition, consistent with international agreements; or
 - iv. for any other matter consistent with Paragraph 1(b) of the MOA.
- (b) The Participants intend to mutually establish the estimated maximum annual volume of Queries that may be initiated pursuant to this Annex. This estimated maximum may be adjusted at any time by mutual consent.
- (c) The Participants intend that a Query by a Requesting Participant include the following Information:
- i. Relevant Identifier;
 - ii. A unique reference number for each set of Identifiers ;
 - iii. The case type of the Query.
- (d) The Participants intend to initially use fingerprints as the Identifier in a Query. Additional Identifiers may be added with the mutual, written consent of the Participants.

6. Responding to Queries:

- (a) The Providing Participant intends to respond to all Queries, except as noted in paragraph 4(a), as follows:
- i. By indicating when an Identifier match is established and providing associated Information to the Requesting Participant, consistent with the MOA and the Providing Participant's domestic laws; or
 - ii. By indicating that no Identifier match has been established.
- (b) Following a data match, the Providing Participant intends to send the data elements, as described in Appendix A, subject to availability and practicability, in the Providing Participant's applicable database or databases.

7. Reciprocal Queries:

- (a) Following the receipt of a match response with the available data elements, the Providing Participant may request that the Requesting Participant provide the data elements, as described in Appendix B for reciprocal queries, subject to availability and practicability, in relation to the individual who was the subject of the initial Query.

Automated

8. Queries Requesting Additional Information:

- (a) After completing the exchange of information described in paragraph 5 through 7, a Participant may request additional information about the subject of the match pursuant to the terms of the Case-by-Case Annex of the MOA.

9. Managing Datasets

- (a) The datasets identified in Appendix A and Appendix B are expected to be replicated in any technical documentation developed by the Participants to support this Annex.
- (b) The Participants acknowledge that the provisions of this Annex, including the datasets outlined in Appendix A and Appendix B and any future modifications pursuant to paragraph 11(a) of this Annex, are intended to be applied should any discrepancy arise between this Annex and any other operational or technical documents drafted by the Participants to support this Annex.

10. Designations

- (a) The Participants intend to designate officials authorised to exchange Information pursuant to this Annex. The Participants will inform each other in Writing of such designations or any changes. The Participants intend to ensure that all Information exchange, including requests, occurs only between these designated officials.

11. Use and Onward Disclosure of Information

- (a) The Participants intend to collect, use and disclose any Information shared pursuant to this Annex in a manner consistent with the MOA and their respective international obligations, domestic laws, regulations and policies.
- (b) Information, including Personal Information, is to be protected by appropriate administrative, technical and physical safeguards, appropriately classified and may only be disclosed to authorised individuals in circumstances consistent with paragraph 5 of the MOA and only for uses that are consistent with the purpose described in paragraph 1(b) of the MOA and paragraph 2(a) of this Annex.
- (c) For greater certainty, the use or onward disclosure of Information received under this Annex for any other circumstance or purpose is not authorised, except as

Automated

noted in paragraph 5 of the MOA. For the purpose of Paragraph 5(e) and (f) of the MOA, this Annex constitutes prior written approval for the exchange of the Migration Five Partner Match Indicator(s).

- (d) The Participants may disclose Information in the administration and enforcement of their respective immigration and citizenship laws to other institutions, such as the Ombudsmen, Privacy Commissioner, Immigration and Protection Tribunal, and the courts for New Zealand, and review bodies in Australia, to further their adjudication or review of said claims or applications, as this is consistent with the purpose described in paragraph 2(a) of this Annex.

12. Retention and Disposal

- (a) Pursuant to paragraph 8 of the MOA, the Participants do not intend to retain, in any form, the fingerprint submitted as part of the initial Query. The Participants only intend to retain the unique reference number submitted as part of an initial Query, to be used for audit, correction, performance monitoring and quality assurance purposes.
- (b) Information that is retained on an electronic or paper case file relating to the individual to whom the Information pertains, 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.
- (c) The Participants intend to mark Information retained as having been received from the other Participant.
- (d) The Participants intend to dispose of all Information determined not to be of relevance or necessity to the administration and enforcement of their respective immigration and citizenship laws, in a timely manner and in accordance with their respective laws and policies.

13. Right of Access and Rectification

- (a) In accordance with paragraph 7(b) of the MOA, each Participant confirms that it has in place a framework that allows an individual to request access to Information about himself or herself that was exchanged under this Annex, and, where that Information is releasable to that individual, allows the individual to request a correction to, or annotation of, that Information.
- (b) In accordance with paragraph 7(c) of the MOA, each Participant confirms that it has a framework in place allowing individuals to seek a review when a Participant

Automated

refuses a request to release Information to an individual about whom the Information pertains.

- (c) Any release of Information received under this Annex to the individual about whom the Information pertains is subject to the provisions of paragraph 5(d) of the MOA.

14. Secure Transmission

- (a) The Participants intend to protect the technical connection between their relevant systems through appropriate means.

15. Compliance and Review

- (a) Pursuant to paragraph 10 of the MOA, the Participants intend to review on an annual basis the volume of transactions, the outcomes and the timeliness of the response to Queries based on mutual decided performance and management measurements, which may include:
 - i. The number of Queries sent;
 - ii. The number and percentage of matches;
 - iii. The number and severity of any security breaches of the Information sharing system, databases, or Personal Information shared under this Annex, as well as a summary of remedial actions taken; and
 - iv. The number and severity of any privacy breaches of the Information sharing system, databases, or Personal Information shared under this Annex as well as a summary of remedial actions taken.
- (b) The Participants intend, to the extent practicable, to share additional statistics and case studies demonstrating how this exchange of Information has assisted in the effective administration and enforcement of the immigration and citizenship laws of their respective countries.
- (c) Pursuant to paragraph 10(d) of the MOA, the Participants understand that the usefulness of the Information shared, and the limitations thereof, are subject to ongoing review and discussion.
- (d) The participants intend to regularly review that Information exchanged pursuant to this Annex is of continued relevance to the purposes identified in paragraph 1(b) of the MOA. The first review may take place no earlier than one year and no later than five years from the date this Annex comes into effect, and as mutually decided upon thereafter.

Automated

16. Financing

- (a) The Participants will pay their own costs and use their own equipment and personnel resources in performing their activities under this Annex.

17. Final Dispositions

- (a) The Participants may amend this Annex, including the data elements as described in Appendix A and B, by mutual written consent.
- (b) Consistent with the MOA, any Participant may terminate this Annex at any time by giving written notice to the other Participant. Termination will become effective 90 days after receipt of such notice. The Participants may also mutually consent In Writing to terminate this Annex at any time. The Participants understand that paragraphs 5 through 9 of the MOA and Paragraphs 6 through 8 of this Annex will continue to apply to any Information shared pursuant to this Annex, notwithstanding termination of the MOA.
- (c) This Annex to the MOA will take effect upon the date it is signed by all Participants or the date it is signed by the last Participant where the Participants do not sign the Annex on the same day.

FOR OFFICIAL USE ONLY / OFFICIAL

Automated

Signed a s. 22(1)(a)(ii) this 19th day of July, 2023, in duplicate.

FOR THE MINISTRY OF BUSINESS, INNOVATION AND EMPLOYMENT (IMMIGRATION NEW ZEALAND)

Print s. 22(1)(a)(ii) CENTRAL MANAGER
s. 22(1)(a)(ii) IMMIGRATION RISK & BORDER

Sign [Redacted]

FOR THE DEPARTMENT OF HOME AFFAIRS

Print PETER ANDER

Sign s. 22(1)(a)(ii) 28/6/23.

s. 47E(d)

s. 47E(d)



**OPERATIONAL PROTOCOL
for Canada and Australia
Regarding Notifications on Removal
of Own Country Nationals Who May
Pose A Risk to States of Return**

Version 1.06

Document Version Control Table

Version #	Date	Responsible	Description of Changes
0.01	2018-03-12	s. 22(1)(a)(ii)	Initial DRAFT
0.02	2018-04-05		Edits per CBSA internal consultation
0.03	2018-04-09		Initial management review Addition of RCMP and INTERPOL to definitions, HQ recipient for users
0.04	2018-06-11		Australian comments and additions
0.05	2018-06-22		Updated based on AU comments and internal CBSA discussions
0.06	2018-07-18		Edits and updates following CBSA-DHA telecon 2018-07-04
0.07	2018-08-02		Australian comments and additions
0.08	2018-08-07		Updated based on AU comments and prepared for translation
0.09	2018-10-18		Updated to amend title, add AU Ottawa email, and clarify advance notification by CBSA is 7 Canadian working days.
0.10	2018-10-31		Updated text based on CA-AU telecon 2018-10-29/30
1.00	2018-11-02		FINAL Document prepared for signing
1.01	2019-04-25		Updated CA process descriptions to reflect that these are standard procedures already in place.
1.02	2022-01-21		Review from current AU perspective and comment
1.03	2022-02-08		Update and comment
1.04	2022-04-26		Update and comment on v1.03
1.05	2022-05-24		Last updates – contacts and LO function
1.06	2023-07-27		Added contact point and other minor edits for AFP at their request

1. Introduction

1.1 Purpose and Scope

The purpose of this document is to describe the processes by which the Canada Border Services Agency (CBSA), on the Canadian side, and the Department of Home Affairs (Home Affairs), the Australian Border Force (ABF) and Australian Federal Police (AFP), on the Australian side (known individually as the Participant and collectively as the Participants) share information about Canadian or Australian nationals who have been notified that arrangements are being made for their removal or deportation to the Participant's country in advance of removal or deportation, where it is considered those persons may pose a risk to the public in the receiving country.

This document elaborates on how the Participants share information on removal of Participant nationals, under the following information exchange authorities:

- *The Memorandum of Understanding Between the Department of Citizenship and Immigration Canada and the Canada Border Services Agency and the Department of Home Affairs of the Commonwealth of Australia Regarding the Exchange of information*, herein referred to as the **MOU**
- *The Annex to the Memorandum of Understanding between the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency and the Department of Home Affairs of the Commonwealth of Australia Regarding the Exchange of Information Concerning the Exchange of Information on a Case-by-case Basis*, herein referred to as the **Case-by-Case Annex**.

This information sharing supports the administration and enforcement of the Participants' respective immigration, border protection and citizenship laws and collaborative efforts in the interest of public safety and protection.

The CBSA will share relevant information on Australian nationals being removed under the following sections/paragraphs of the Canadian *Immigration and Refugee Protection Act* (IRPA):

- s. 34 – Security
- s. 35 – Human or international rights violations
- s. 36(1) – Serious criminality
- s. 37 – Organized criminality
- s.38(1)(a) or (b) – Health grounds

Home Affairs, ABF and AFP will share relevant information on Canadian nationals subject to removal under section 198 of the Australian *Migration Act 1958* (the Migration Act). The Canadian nationals would be unlawful non-citizens because their visa had been cancelled under the character provisions of the Migration Act, cancelled as a result of being deemed to be a risk to the Australian community under the relevant provisions of

the Migration Act, or expired while they were in custody and are unlawful non-citizens at the time of removal.

This document is not legally binding. Nothing in this document gives rise to rights or obligations under international or applicable domestic laws, common law powers and policies.

1.2 Information to be Shared

Information that may be shared (where available and when in compliance with relevant domestic laws, regulations and policies, and international obligations) includes but is not limited to information listed at:

- paragraph 4 of the *2016 Case-by-Case* annex to the *MOU* and
- parts [2.1](#), [2.2](#) and [3.1](#) of this Operational Protocol.

The Participants should provide, when possible, the following information:

- i. Full names, date of birth, place of birth, and known aliases
- ii. Travel Document information
- iii. Removal details (flight number(s), carrier name(s), departure and arrival time(s), transit information and escort information if available)
- iv. Removal grounds
- v. Conviction and sentence information.

1.3 Audience

This guide describes processes used by the following individuals and groups:

In Canada:

Delegated officers at the CBSA involved in the removal of an Australian national to Australia, whereby the removal is assessed to be relevant to the purpose described in paragraph [1.1](#) of this Operational Protocol, specifically (but not limited to):

- Removals Officers in Removals Operations at National Headquarters
- Regional Removals Officers
- International Liaison Officers (LO)
- Liaison Officer Assistant
- International Network Managers (INM)
- CBSA Liaison Officer at the Royal Canadian Mounted Police (RCMP)
- Intelligence Tactical Operation Centre (ITOC): Manager; Senior Program Advisor, Senior Program Officer
- National Targeting Centre (NTC): Manager; Senior Program Advisor, Shift Supervisor/Superintendent, Senior Program Officer, Canberra Tactical NTC Liaison Officer

- Ports of Entry: Shift Supervisor/Superintendent, Border Services Officer
- Royal Canadian Mounted Police (RCMP) via INTERPOL Ottawa National Central Bureau (CA-NCB).

In Australia:

Officers representing Home Affairs, ABF and the Australian Federal Police (AFP), involved in the removal of a Canadian national to Canada, whereby the removal is assessed to be relevant to the purpose described in paragraph [1.1](#) of this Operational Protocol, specifically (but not limited to) including those from the following areas:

- National Removals (ABF)
- Australian Border Operations Centre (ABF)
- Regional Removal Officers (ABF)
- Character and Cancellation Branch (Home Affairs)
- Australian officers and locally engaged staff at Post (Ottawa and Washington)
- Biometric Collection and Exchange Section, Digital Technology Policy Division (Home Affairs)
- AFP INTERPOL Canberra National Central Bureau (AU-NCB)

1.4 Legal and Policy Guidelines

The exchange of relevant removal information as outlined in paragraph [1.2](#), supports:

- the administration and enforcement of a Participant's respective laws and policies governing the removal of a foreign national from their country; or
- the admission of a Participant's national following removal from the other Participant's country.

Exchanges of information outlined herein are carried out pursuant to, and consistent with, the domestic laws and policies of the Participants and, where possible, with reference to Part 3 of the *MOU*.

1.5 Authority for Canada to Provide Information

The CBSA provides information to Australia about the removal of Australian nationals under authority of the IRPA and the Canadian *Privacy Act* (1985). Specifically, authority is provided under s. 8(2)(a) of the *Privacy Act*, which states that a government institution may disclose information for the purpose under which the institution compiled the information or, for a use consistent with that purpose.

In addition, the CBSA provides information to Home Affairs regarding the identity and citizenship of the Australian national under authority of s. 8(2)(f) of the Canadian *Privacy Act* (1985) and the *MOU* and its Case-by-Case Annex to assist in their determining the admissibility of the person being removed.

1.6 Authority for Australia to Provide Information

Australia provides information to Canada about the removal of Canadian nationals in accordance with the requirements in Australia's *Privacy Act 1988*, *Migration Act 1958*, *Australian Federal Police Act 1979*, and the *Australian Border Force Act 2015*, and in accordance with all applicable domestic laws.

2. Operational Guidelines – CBSA Effecting Removal to Australia

For removals of Australian nationals from Canada consistent with paragraph [1.1](#), the CBSA follows existing standard removal procedures outlined in its Immigration Enforcement Manual, chapter ENF 10 Removals. Under these procedures the Agency's LO or INM in Canberra provides at least seven Canadian working days advance notice prior to the removal to the Australian Border Operations Centre (ABOC) and to Australia's Principal Migration Officer (PMO) Ottawa. The CBSA also provides the removal information to INTERPOL Ottawa to forward to INTERPOL Canberra via a travel advisory email through the INTERPOL secure channel. These notifications include both escorted and non-escorted cases.

2.1 Notification by CBSA LO or INM in Canberra

The seven Canadian working days advance notification via the LO / INM in Canberra stipulates whether the removal is escorted or unescorted and indicates if the notification is being provided for information only, or if assistance is required prior to, or upon arrival. The notification is sent to ^{s. 22(1)(a)(i)} [@abf.gov.au](mailto:abf@dfat.gov.au) for ABOC and to the PMO (Home Affairs) Ottawa at ^{s. 22(1)(a)(ii)} [@dfat.gov.au](mailto:dfat@dfat.gov.au).

Noting CBSA cannot provide criminal information, the LO / INM will take the following steps:

- i. The LO / INM will review and confirm the individual is being removed to Australia and the date of the departure/arrival of the removal/deportation.
- ii. The LO / INM will assist the Inland Enforcement Officer and will liaise with appropriate stakeholders if assistance with approvals from the airline or Australia is required.
- iii. If no assistance is required the LO / INM will only notify partners in Australia and any partners in the areas through which the individual being removed/deported may be transiting.

If all or part of the steps cannot be completed at least seven Canadian working days in advance of the removal date, the LO / INM will notify the ABOC and PMO (Home Affairs) Ottawa as soon as possible to prevent difficult situations from developing and to ensure that any necessary assistance is made available.

s. 47E(d)

3. Operational Guidelines – Australia Effecting Removal to Canada

Australia provides at least seven days advance notice of the removal of a Canadian national by forwarding the information outlined in section 3.1 of this document, subject to availability from and in accordance with law or as authorised or required under law:

- Non-criminal information through Home Affairs Ottawa Post to CBSA INM / LO at Canberra s. 22(1)(a)(ii) with a copy to the CBSA Intelligence Tactical Operation Centre s. 22(1)(a)(ii)
- Criminal information through ABF to CA-NCB via secure channel.

This includes both escorted and non-escorted cases who are being removed consistent with Paragraph 1.1.



The Removals Officer provides this information to PMO (Home Affairs) Ottawa Post s. 22(1)(a)(ii) [@dfat.gov.au](mailto:dfat.gov.au) copied to ABF Removals Operations s. 22(1)(a)(ii) [@abf.gov.au](mailto:abf.gov.au).

In Addition: 48 Hours Prior to Removal

As soon as the removal date is confirmed, and a minimum of 48 hours prior to removal Home Affairs Ottawa Post will forward to CBSA, subject to availability, the following information:

- Any relevant personal or identifying information (from 3.1 above) that has not already been provided;
- Travel document and flight details (if not already provided);
- Health Discharge Assessment summary as provided by the Home Affairs Detention Health Services contractor or where provided by the relevant Correctional authority.

This information will be sent to CBSA INM / LO at Canberra
s. 22(1)(a)(ii) with a copy to the CBSA Intelligence Tactical
Operation Centre s. 22(1)(a)(ii)

4. Onward Disclosure

The Participants expect that there may be circumstances where onward disclosure of information, provided for removal purposes, is exchanged with domestic third parties (for example, to local law enforcement). For the processes described in this Operational Protocol, the Participants will ensure the following circumstances are met for any onward disclosure and is consistent with:

- i. their applicable domestic laws and regulations and consistent with the purpose for which the information was provided;
- ii. Part 6 of the *MOU*;
- iii. Part 7 of the *Case-by-Case Annex*.

The Participants undertake not to use or further disclose the Information provided under this Protocol except in accordance with this Protocol, for the purpose specified in Paragraph 1.1 or otherwise as required or authorised by law.

Participants will notify each other of any onward disclosure of the removal information outside of law enforcement, and will ensure, to the best of their ability that any third party receiving the information must apply a similar level of protection to the information as the Participants.

5. Final Dispositions

This document will take effect on the date it is approved by the last Participant.

In line with the *MOU* and the *Case-by-Case Annex*:

- i. the Participants may amend this document by their mutual consent in writing
- ii. a Participant may terminate its agreement to this document by giving 90 days' notice in writing to the other participant
- iii. the Participants intend to conduct regular quality assurance activities to ensure that the exchanges carried out are consistent with the intent of this document.

The participants further intend to review or revise this document every two years.

6. Points of Contact

The points of contact for reviewing or revising this document, or raising issues around the operations of this document, are the following (or their successors):

6.1 Canada

The CBSA International Network Manager at Canberra will serve as the single point of contact to coordinate input from program areas.

Email: s. 22(1)(a)(ii)

For Migration Five Immigration Information Sharing Operational Protocol Updates:

Traveller Border Programs Division
Travellers Policy and Programs Directorate
Travellers Branch
Canada Border Services Agency

Email: s. 22(1)(a)(ii)

For removals of an Australian national from Canada:

Inland Enforcement Program Management Division
Enforcement and Intelligence Programs Directorate
Intelligence and Enforcement Branch
Canada Border Services Agency

Email: s. 22(1)(a)(ii)

For returns of Canadian nationals for criminality:

Intelligence, Targeting and Criminal Investigations Program Management Division
Enforcement and Intelligence Programs Directorate
Intelligence and Enforcement Branch
Canada Border Services Agency

Email: s. 22(1)(a)(ii)

6.2 Australia

The ABF International Operations and Coordination Branch will serve as the single point of contact to coordinate input from program areas and changes to this operational protocol.

Email: s. 22(1)(a)(ii)@abf.gov.au

For Migration Five Immigration Information Sharing Arrangements:

Biometric Collection and Exchange Section

Identity and Biometrics Policy and Strategy Branch
Digital Technology Policy Division
Australian Department of Home Affairs

Email: **s. 22(1)(a)(ii)**@homeaffairs.gov.au
For removals of a Canadian national from Australia
National Removals
Australian Border Force

Email: **s. 22(1)(a)(ii)**@abf.gov.au

Point of contact for Home Affairs in Canada

PMO (Home Affairs) Ottawa
International Policy Division
Australian Department of Home Affairs

Email: **s. 22(1)(a)(ii)** @dfat.gov.au

For returns of Australian nationals for criminality

INTERPOL Canberra (AU-NCB)

Email: **s. 22(1)(a)(ii)**

7. Definitions

For the purposes of this Operational protocol, the following definitions apply:

- i. **ABF:** Australian Border Force
- ii. **Admissibility Determination (Canada):** The process carried out by a delegated officer to determine whether a foreign national is admissible to remain in Canada under the Canadian *Immigration and Refugee Protection Act* (IRPA).
- iii. **AFP:** Australian Federal Police
- iv. **Australian citizen:** Is an Australian citizen under Division 1 or 2 of Part 2 of the *Australian Citizenship Act 2007* or a person who was an Australian citizen under the *Australian Citizenship Act 1948* immediately before the commencement day and has not ceased to be an Australian citizen under this Act.
- v. **Canadian national:** A person who has been granted citizenship in Canada as defined under section 3 of the *Citizenship Act*, or any person registered as an Indian under the *Indian Act*.
- vi. **CBSA:** Canada Border Services Agency

- vii. **Correctional information (Australia):** Information that has been obtained by Home Affairs from domestic correctional authorities either on request or by receipt.
- viii. **FPS Number:** Fingerprint Section Number, the unique identifier under which criminal data and fingerprints are stored at the RCMP
- ix. **INM:** The CBSA International Network Manager in Canberra, Australia
- x. **INTERPOL Canberra:** The INTERPOL National Central Bureau for Australia hosted by the Australian Federal Police
- xi. **INTERPOL Ottawa:** The INTERPOL National Central Bureau for Canada hosted by the Royal Canadian Mounted Police
- xii. **IRPA:** Canada's *Immigration and Refugee Protection Act* and its associated regulations
- xiii. **LO:** The CBSA Liaison Officer in Canberra, Australia
- xiv. **Migration Act:** Australia's *Migration Act 1958*
- xv. **Participants:** Refers to the Canada Border Services Agency, the Australian Department of Home Affairs (incorporating its operational arm, the Australian Border Force) and the Australian Federal Police
- xvi. **RCMP:** Royal Canadian Mounted Police
- xvii. **Removal Information:** Information that is being shared in support of a removal consistent with paragraph [1.1](#).
- xviii. **Travel Document Information:** As outlined in paragraph 2.1.