



OFFICIAL: Sensitive

# Central Movement Alert List (CMAL)

## Procedural Instruction

Document ID (PPN)	VM-4816
TRIM record number	ADD2021/4462189
BCS Function	Visa and Migration Management
Document owner	Commander, Border Systems and Program Management
Approval date	19 June 2020
Document Contact	ABF Operations Systems Management s. 47E(d)

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

OFFICIAL: Sensitive

# Table of Contents

<b>1. Purpose</b>	<b>8</b>
<b>2. Scope</b>	<b>8</b>
2.1. In Scope	8
2.2. Out of Scope	8
<b>3. Procedural Instruction</b>	<b>9</b>
3.1. CMAL Access	9
s. 47E(d)	
s. 47E(d)	
3.1.3. Launching CMAL and viewing MAL statuses	10
3.1.4. Viewing narratives	10
s. 47E(d)	
3.1.6. Onshore CMAL access	11
3.1.7. Offshore CMAL access	11
3.1.8. Applying for CMAL access (Offshore and Onshore for non CITRIX users)	11
3.1.9. HMAL Access	12
3.2. Considering Identities or documents for MAL	12
3.3. Alert Reason Codes	13
3.3.1. Alert Reasons	13
3.3.2. Risk categories	16
3.3.3. Group Codes	16
s. 47E(d)	
3.3.5. Classification Flag	17
3.3.6. ARC Roles and responsibilities	17
3.3.7. Creating new ARCs	18
3.3.8. Reviewing the relevance of an ARC category or ownership	18
3.3.9. Deletion of an ARC	19
s. 47E(d)	
3.6. ARC 03 War crimes or human rights abuse	22
3.6.1. ARC 03 policy	22
3.6.2. ARC 03 CMAL system constraints	23
3.7. ARC 04 Controversial visitors	24
3.7.1. ARC 04 policy	24
3.7.2. ARC 04 CMAL system constraints	26
3.8. ARC 05 Serious or high profile crime	27
3.8.1. ARC 05 policy	27
3.8.2. ARC 05 CMAL system constraints	28
3.9. ARC 06 Health concerns	30
3.9.1. ARC 06 policy	30
3.9.2. ARC 06 CMAL system constraints	31
3.10. ARC 07 Organised immigration malpractice	33

3.10.1.	ARC 07 policy	33
3.10.2.	ARC 07 CMAL system constraints	34
3.11.	ARC 08 Child custody concerns	35
3.11.1.	ARC 08 policy	35
3.11.2.	ARC 08 CMAL system constraints	37
3.12.	ARC 09 Other criminals	37
3.12.1.	ARC 09 policy	37
3.12.2.	ARC 09 CMAL system constraints	40
3.13.	ARC 10 Overstayers	40
3.13.1.	ARC 10 policy	40
3.13.2.	ARC 10 CMAL system constraints	42
3.14.	ARC 11 Breach of visa conditions	43
3.14.1.	ARC 11 policy	43
3.14.2.	ARC 11 CMAL system constraints	44
3.15.	ARC 12 Debts to the Commonwealth	45
3.15.1.	ARC 12 policy	45
3.15.2.	ARC 12 CMAL system constraints	46
3.16.	ARC 13 Immigration malpractice	47
3.16.1.	ARC 13 policy	47
3.16.2.	ARC 13 CMAL system constraints	48
3.17.	ARC 14 Bypassed/refused immigration clearance	49
3.17.1.	ARC 14 policy	49
3.17.2.	ARC 14 CMAL system constraints	51
3.18.	ARC 16 Suspect genuineness	52
3.18.1.	ARC 16 policy	52
3.18.2.	ARC 16 CMAL system constraints	53
3.19.	ARC 17 Surrender Australian travel document	54
3.19.1.	ARC 17 policy	54
3.19.2.	ARC 17 CMAL system constraints	55
3.20.	ARC 18 Travel sanctions	56
3.20.1.	ARC 18 policy	56
3.20.2.	ARC 18 CMAL system constraints	57
3.21.	ARC 19 Illegal fishers	58
3.21.1.	ARC 19 policy	58
3.21.2.	ARC 19 CMAL system constraints	59
3.22.	ARC 20 Visa Fraud	60
3.22.1.	ARC 20 policy	60
3.22.2.	ARC 20 CMAL system constraints	61
3.23.	ARC 22 INTERPOL (Australian Federal Police)	63
3.23.1.	ARC 22 policy	63
3.23.2.	ARC 22 CMAL system constraints	64
3.24.	ARC 23 Identity	65
3.24.1.	ARC 23 policy	65
3.24.2.	ARC 23 CMAL system constraints	67
3.25.	ARC 25 Serious criminal (poor bio-data)	68
3.25.1.	ARC 25 policy	68
3.25.2.	ARC 25 CMAL system constraints	69
3.26.	ARC 26 INTERPOL (Missing Children)	70

3.26.1.	ARC 26 policy	70
3.26.2.	ARC 26 CMAL system constraints	71
3.27.	Credible Sources	72
3.28.	Considering Australians for MAL	73
3.28.1.	Listing Australian Aliases	74
3.28.2.	Applicable ARCs and approvals	74
3.28.3.	MAL for new Australian citizens	74
3.29.	Considering New Zealand Identities for MAL	75
3.30.	Considering Foreign National Identities for MAL	75
3.31.	Deceased persons	75
3.32.	Considering minors for inclusion on MAL	76
3.33.	Considering Australian Documents for MAL	76
3.33.1.	Approval for listing Australian Travel Documents	77
3.34.	Considering New Zealand Travel Documents for MAL	77
3.35.	Considering Foreign Travel Documents for MAL	78
3.35.1.	Policy and operational owners	79
3.35.2.	Listing lost or stolen passports	80
3.35.3.	Counterfeit or suspect documents	80
3.35.4.	Fraudulently used or fraudulently altered documents	80
3.35.5.	Confiscated by people smugglers and other third parties	80
3.35.6.	Restricting travel	80
3.35.7.	Public Interest Criteria (PIC)	80
3.36.	Listing identities or documents on MAL- narrative requirements	81
3.36.1.	Catering to the audience	81
3.36.2.	Using minimal acronyms	81
3.36.3.	Required data	81
3.36.4.	Narratives for Australian citizens	82
s. 47E(d)		
3.36.6.	A good example of a narrative text	83
3.37.	Proposing identities for MAL inclusion	83
3.37.1.	Minimum data required	84
3.37.2.	Supporting documentation	84
3.37.3.	Listing aliases on MAL	84
3.38.	Listing Documents on MAL	85
3.38.1.	Automatic document listing on MAL	85
3.38.2.	Required data	85
s. 47E(d)		
s. 47E(d)		
3.38.5.	Supporting documentation	87
3.39.	Reviewing and Updating MAL Identities and Documents	88
s. 47E(d)		
3.39.2.	Automatic review dates for identities (PALs)	88
s. 47E(d)		
3.39.4.	Visa/citizenship grant or refusal	89
s. 47E(d)		
3.39.6.	Reviewing Australian identities on MAL	89
3.39.7.	Reviewing Australian documents on MAL	90
s. 47E(d)		
s. 47E(d)		

3.40.2.	Automatic identity and document expiry	90
3.40.3.	When to manually expire a MAL identity or document	92
3.40.4.	Void Australian and New Zealand travel documents	92
3.40.5	Invalid records	92
3.40.6.	Re-listing a found passport on MAL	92
3.40.7.	What happens to expired records?	92
3.41.	ARC Owner Change Form	93
3.41.1.	ARC Owner Transfer	93
3.41.2.	ARC Creation/Change to Business rules	93
3.41.3.	Deletion of an ARC	96
<b>4.</b>	<b>Accountabilities and Responsibilities</b>	<b>97</b>
4.1	Policy owner responsibilities	97
4.2.	User and stakeholder responsibilities	97
4.3.	Records Management responsibilities	97
<b>5.</b>	<b>Version Control</b>	<b>97</b>
	<b>Attachment A – Definitions</b>	<b>99</b>
	<b>Attachment B – Assurance and Control Matrix</b>	<b>102</b>
	Powers and Obligations	102
	Controls and Assurance	104
s. 47E(d)		
	<b>Appendix – CMAL Supporting Material</b>	<b>106</b>
s. 47E(d)		
s. 47E(d)		
3.	CMAL Remote Input Function (RIF) Guidelines – s. 47E(d) - 26	114
s. 47E(d)		

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


3.2.	Processing s. 47E(d) - 26	114
4.	CMAL Remote Input Function (RIF) Guidelines – Documents	115
4.1.	Documents for inclusion on MAL	115
4.2.	DAL bulk loads	116
5.	CMAL - checking MAL and assessing potential matches	117
5.1.	Performing MAL Checks	117
	s. 47E(d)	
5.3.	Variable thresholds	118
5.4.	Documents	118
5.5.	Identities	119
5.6.	Initial MAL status allocation and action	119
	s. 47E(d)	
5.8.	CMALs name matching software	120
5.9	Biometrics matching capability	120
	s. 47E(d)	
6.2.	Assessing duplicate records	121
6.3.	Assessment priorities	121
	s. 47E(d)	
	s. 47E(d)	
6.6	Resolving a potential match	121
	s. 47E(d)	
8.	CMAL Guidelines - actioning and overriding MAL alerts	125
8.1.	MAL is not a legislative instrument	125
	s. 47E(d)	
8.3.	Granting citizenship to a MAL-listed identity	126
	s. 47E(d)	
	s. 47E(d)	
	s. 47E(d)	
	s. 47E(d)	
	s. 47E(d)	
9.	Process: manually expiring an identity or document record	128
10.	Disclosure and Classification of MAL Records	129
10.1.	Security classification of MAL records	129
10.2.	Privacy and Freedom of Information	129
10.3.	Further information	130
10.4.	Disclosing MAL business operations and stakeholders	130
10.5.	Disclosing personal information contained in MAL	130
10.6.	Disclosing adverse information to government agencies	130
11.	Policy Implications for Public Interest Criteria	131
11.1.	Relationship between PIC and ARC	131
11.2.	Section 501 of the Migration Act	131
11.3.	PIC 4001 - Character Concerns ARC 03, 05, 09, 25	132
11.4.	PIC 4002 - Security of the Australian Community s. 47E(d)	132
11.5.	PIC 4003(a) - National Security or Foreign Policy interest ARC 18	132

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



11.6.	PIC 4003A/4003(b) - Weapons of Mass Destruction ARC 04	132
11.7.	PIC 4004 - Debts to the Commonwealth ARC 12	132
11.8.	PIC 4005/4007 - Health/Health Burden ARC 06	132
11.9.	PIC 4012 - Unaccompanied Minors	132
11.10.	PIC 4013 - Cancellation ARC 07, 11, 13	133
11.11.	PIC 4014 - Overstayers ARC 10	133
11.12.	PIC 4015/4017 - Child Custody (parental responsibility) concerns ARC 08	133
11.13.	PIC 4020 - The Integrity PIC ARC 20	133
11.14.	Illegal Foreign Fishers Legislation ARC 19	134
11.15.	Damaged passports and the <i>Australian Passports Act</i> ARC 17	134
11.16.	Sanctions Regimes ARC 18	134
11.17.	Geneva Conventions Act 1957 ARC 03	135
11.18.	S166 Travel Document Requirement - DAL records	135

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



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

# 1. Purpose

The Central Movement Alert List (CMAL) is the system used to store, maintain and access a central repository of Movement Alert List (MAL) identities and documents of concern.

CMAL is programmed to determine the MAL Status for a client so that CMAL concerns are brought to the attention of decision makers in both the pre and post visa contexts. The MAL status should also be considered when assessing sponsors for visa applicants and those entering Australia.

In line with the purpose of MAL, CMAL facilitates a centralised high-quality check of all visa and citizenship applicants against MAL to:

- streamline visa application processing
- support the management of border and compliance risks
- enhance border security.

This CMAL Procedural Instruction and (Support material) applies to:

1. Visa Processing/Case Officers (on and off-shore)
2. Citizenship Officers
3. Compliance Officers
4. Detention Officers
5. Alert Reason Code (ARC) owners and;
6. Border Operation Centre (BOC) staff.

## 2. Scope

### 2.1. In Scope

This document outlines the structure of CMAL policy, including the document hierarchy and key accountabilities and responsibilities. The CMAL Procedural Instruction suite of documents provides an overview of the MAL/CMAL policy and procedural direction on the following aspects:

- listing and maintaining identities and documents of concern on MAL
- data quality
- maintaining Alert Reason Codes (ARCs)
- performing MAL checks
- assessing and actioning potential MAL matches
- granting visas or approving applications for citizenship to clients listed on MAL
- implications for Public Interest Criteria (PIC)
- security requirements for accessing and storing MAL records.

### 2.2. Out of Scope

As the CMAL Procedural Instruction is concerned with broad policy direction and instruction, as well as some support material, it does not contain detailed operational procedures or training material. It also does not contain information relating to systems issues.

The following areas will respond to these enquiries, as needed:

Subject of enquiry	Email	Phone
MAL operational procedures or Remote Input Function (RIF)	s. 47E(c)	s. 22(1)(a)(ii)
Policy advice and Systems Issues	s. 47E(c)	

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



## 3. Procedural Instruction

### 3.1. CMAL Access

Many roles in the Department require access to CMAL to perform their duties. The access level required depends on:


- role and responsibilities
- security clearance
- position number
- employment conditions.

It is essential that managers determine the correct level of access required to perform the role.

CMAL access is provided to staff who:

- are responsible for maintaining the MAL database, including proposing additions or amendments to Person and Document Alert List (PAL and DAL) records
- need to check the MAL status of a client
- need access to perform their role.

s. 47E(d)



#### 3.1.1. Role-based access

CMAL access is based on roles and is linked to a staff member's position number, not their departmental user ID. Consideration must be given as to whether a staff member's role matches the CMAL access level required.

Further, if a staff member's position number changes, the position may be linked to:

- a different CMAL access level, or
- no CMAL access.

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

Staff with appropriate approval or delegation powers must ensure they fully understand the details of a MAL document or identity alert. Therefore, it is imperative that the decision maker has the appropriate level of access to make fully informed decisions.

For further information, email: s. 47E(d)

s. 47E(d)

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

### 3.1.3. Launching CMAL and viewing MAL statuses

CMAL can be launched from:

- various visa processing systems
- intranet homepage.

In general, decision-makers can view a client's MAL status in the visa processing system, and then launch CMAL directly from the visa processing system. The visa processing system being used dictates the way that CMAL is launched.

### 3.1.4. Viewing narratives

The ability to view narratives on PAL and DAL records depends on the:

- security classification of the record
- staff member's role, and related level of CMAL access. This includes Locally Engaged Employees (LEEs) at overseas posts.

Only BOC staff are able to read the narratives on:

s. 47E(d)


If a user is not able to view a narrative, CMAL displays a message referring them to one of the following for further information:

- The BOC

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


- Principal Migration Officer (PMO) if they are a LEE.

s. 47E(d)




### **3.1.6. Onshore CMAL access**

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



### **3.1.8. Applying for CMAL access (Offshore and Onshore for non CITRIX users)**

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



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

### 3.1.9. HMAL Access

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



## 3.2. Considering Identities or documents for MAL

CMAL is programmed to determine the MAL Status for a client so that any CMAL concerns are brought to the attention of decision makers in both the pre and post visa contexts.

CMAL interfaces with a number of internal (departmental) and external (other agency) systems. These are listed in the table below.

**Note:** The CMAL system is not connected to any births, deaths or marriages databases so will not update automatically in the event of an identity's death.

**Contact:** The Border Operations Centre (BOC) for further information.

System	Host
<p>The following internal systems:</p> <ul style="list-style-type: none"> <li>• Client Data Hub (CDH)</li> <li>• Integrated Client Services Environment (ICSE)</li> <li>• Immigration Records Information System (IRIS)</li> <li>• Travel and Immigration Processing System (TRIPS)</li> <li>• Advanced Passenger Processing (APP)</li> <li>• Security Referral Service (SRS)</li> <li>• Border Security Portal (BSP)</li> </ul>	Department of Home Affairs

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

System	Host
<ul style="list-style-type: none"> <li>Client Search Portal (CSP)</li> <li>Passenger Analysis Clearance and Evaluation (EPAC/PACE)</li> <li>SmartGate</li> </ul>	
Electronic Travel Authority System (ETAS)	SITAs (airline and maritime communication organisation)

s. 47E(d)

Records listed on MAL are separated into two categories:

- identities of concern, which are recorded in the PAL. s. 47E(d)
- documents of concern, which are recorded in the DAL. These are records about lost, stolen, cancelled, counterfeit, fraudulently altered or otherwise suspect foreign government passports and other travel documents. s. 47E(d)

To ensure that departmental dealings with clients remain fair, open and reasonable, careful consideration must be given to:

- whether an identity or document warrants listing on MAL
- whether the data source is credible
- the quality of the data for each record.

Most Home Affairs staff will source information on clients or Persons of Interest that is applicable for the MAL during their daily processes. When determining that an alert is to be listed, the Home Affairs officer must assign an appropriate Alert Reason Code to the listing.

### 3.3. Alert Reason Codes

Alert Reason Codes (ARCs) are codes assigned to identities listed on MAL that:

- state the reasons under which each identity is listed
- provide applicable business rules for the listing
- list the minimum data required when listing an identity under a specific ARC
- list sources that are considered credible as a basis for the listing.

ARCs only apply to identities listed in the PAL component of MAL. ARCs do not apply to documents listed in the DAL.

#### 3.3.1. Alert Reasons

The table below summarises the ARCs and the reasons for considering an identity for inclusion on MAL.



ARC	Risk	Reasons
s. 47E(d)		s. 47E(d)
s. 47E(d)		
03 War crimes or human rights abuse	High	
04 Controversial visitors	High	
05 Serious or high profile crime	High	
06 Health concerns	Medium	
07 Organised immigration malpractice	High	
08 Child custody concerns	Medium	
09 Other criminals	Medium	
10 Overstayers	Low	
11 Breach of visa conditions	Low	
12 Debts to the Commonwealth	Low	

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

ARC	Risk	Reasons	
		s. 47E(d)	
13 Immigration malpractice	Low		
14 Bypassed/refused immigration clearance	Low		
16 Suspect genuineness	Low		
17 Surrender Australian Travel Document	Low		
18 Travel sanctions	High		
19 Illegal fishers	Low		
20 Visa Fraud	High		
22 INTERPOL	High		
23 Identity	Medium		

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

ARC	Risk	Reasons
		s. 47E(d)
25 Serious criminal (poor bio-data)	High	
26 INTERPOL (missing children)	Medium	

### 3.3.2. Risk categories

Each ARC belongs to a risk category. There are categories - high, medium and low. The categories reflect the potential risk to the Australian public should a person travel to Australia without coming to the notice of the relevant authorities.

The table below describes the categories and lists the ARC codes that belong to each category.

Category	ARC codes	Description
High risk	s. 47E(d) 03, 04, 05, 07, 18, 20, 22, 25	s. 47E(d)
Medium risk	06, 08, 09, 23, 26	
Low risk	10, 11, 12, 13, 14, 16, 17, 19	

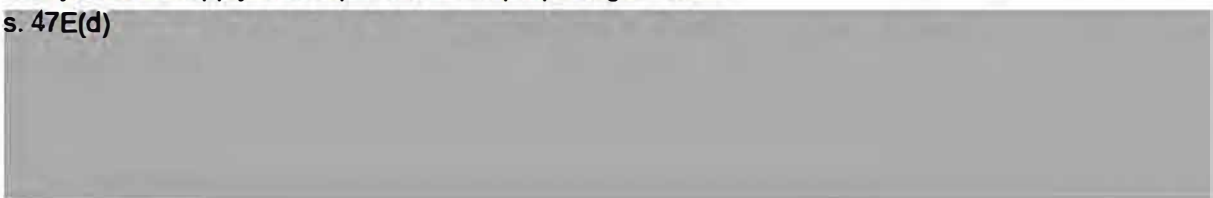
### 3.3.3. Group Codes

Group Codes are key words that can be used to create sub-categories of alert types under the same ARC. The use of Group Codes delivers ARC owners many benefits because they can identify a specific cohort of alerts listed under their ARC. This means it is easier to update review periods for a specific group of alerts while allowing for accurate reporting of alerts against a Group Code.

Group Codes are set by the ARC owner and are listed in the relevant policy and business rules applying to the specific ARC, as detailed within this Procedural Instruction. The proposer when proposing an alert in the Remote Input Function (RIF) can apply a Group Code.

Group Codes should be used wherever possible to categorise an alert reason. It will be mandatory under many ARCs to apply a Group Code when proposing an alert.

s. 47E(d)



ARC owners can create Group Codes in CMAL by selecting the key word/s to identify the cohort (a maximum of three words per Group Code) and emailing a request for the Group Codes to be created in CMAL to s. 47E(d).

There is no limit on the number of Group Codes that can be created under an ARC.

When proposing an alert you can select the appropriate Group Code from a drop down menu in CMAL. If you require clarification on the appropriate Group Code to use, refer to the business rules for the ARCs listed in this Procedural Instruction. A maximum of four group codes may be applied to a single alert.

s. 47E(d)

### 3.3.5. Classification Flag

The Classification Flag must be set as 'OFFICIAL: Sensitive'.

s. 47E(d) CMAL records listed as 'Protected' are only visible to staff working in the BOC. Match cases with the 'Protected' record can only be overridden using an override key provided by the BOC following authorisation from the Alert Reason Code (ARC) operational owner.

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

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

Information is available for disclosure and classification of MAL records regarding PROTECTED records.

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

### 3.3.6. ARC Roles and responsibilities

The Policy Owner, in conjunction with the BOC, defines:

- the policy and rules for the record set
- credible data sources
- the legislative basis for the alert (if applicable)
- how the match is confirmed
- referral procedures
- where evidence supporting the record can be located
- processes for a Red status
- the match case threshold score
- minimum data standards for the ARC.

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

They identify the Operational Owner who has responsibility for managing the MAL records for an ARC or ARC group.

The Operational Owner:

- manages a set of records within an ARC or ARC group
- holds the evidence for each record listing
- deals with requests to clarify match case referrals
- liaises with the information source(s)
- maintains the accuracy and currency of the MAL records.

### **3.3.7. Creating new ARCs**

Creating new ARCs can be done in consultation with the BOC.

If a business reason exists for creating a new ARC, the Superintendents (EL2) of the ABF Operations Systems Support must be consulted and approve the new ARC. If the proposal is not being submitted from the intended new policy and operational owners, endorsement from the intended new policy and operational owners of the proposed new ARC will be required.

When submitting an initial proposal for the creation of a new ARC, it must include:

- the expected source of the information for the alerts (i.e. client records, other agencies)
- the minimum data standards/business rules for listing the alert
- the referral process
- the measures you want in place before an alert can be overridden.

Where there are records existing under other ARCs intended for the new ARC, a business plan for the transfer of these records needs to be provided. Where there is to be an expansion to the type of alerts to be listed under an existing ARC, the associated ARC policy within this Procedural Instruction must be updated, including agreement of any alternative ARC owner who may be affected.

When a request for a new ARC is approved, it is the responsibility of the ARC owner to communicate details of the associated policy and business rules.

### **3.3.8. Reviewing the relevance of an ARC category or ownership**

Following a restructure of responsibilities, ARC owners could find they have a cohort of record holdings under their ARC that no longer fit within their area of responsibility. In this circumstance, they retain responsibility for the ARC, but may redefine the policy and business rules for future listings under the ARC to close off any further listings for this cohort. However, ARC owners will need to submit details of arrangements they have in place for managing the cohort of alerts with the new owner.

The new owner may request a new ARC be created, or identify an existing ARC where they can direct future alerts. Where this is required, please refer to: 3.3.7 Creating new ARCs.

Where there are any alerts under an ARC that may belong elsewhere due to a change in reporting lines and to ensure these will be managed during any interim period, the existing ARC owner will retain responsibility for them. The existing alerts still need to be managed, until they are expired, deleted, or amended to place them under a different ARC (this update has to be done manually to each individual alert as arranged by the ARC owner).

Group Codes can be of assistance where ARC owners are looking to split the operational responsibility for managing alerts. Instead of deleting or creating a new ARC, the creation of a new Group Code under an existing ARC will allow for future alerts to be differentiated from others under the ARC category. Refer to the section 3.3.3 on Group Codes for more information.

When an ARC is moved to a new policy owner, the Superintendent (EL2) of ABF Operations Systems Management must be notified in writing. This includes advising of any changes in policy parameters, system constraints, business ownership and contact details for responsible ARCs.



### 3.3.9. Deletion of an ARC

An ARC owner may consider deleting an ARC. However, the need to delete an ARC is considered a rare event, given that the reasons why an ARC was initially created are unlikely to change. However, a need may arise to close down an ARC, such as if the reason for the ARC no longer exists due to a legislative change.

With current system functionality, an ARC category can only be deleted if no alerts remain under the ARC (i.e. they are all expired, deleted, or transferred to another ARC). It may take time to manage any residual alerts until the ARC is empty and can be deleted. Therefore, if a decision to close down an ARC category is made, there may be an option to close the ARC off to receiving any new alerts. The existing alerts can then be managed by the ARC owner without any new alerts being added. This option may become available following a system upgrade request.

If an ARC category is to be closed down, the responsibility for any residual alerts will remain with the ARC owner until there are no remaining alerts. This governance framework is required to ensure the operational effectiveness of CMAL is maintained.

If the closure of an ARC category is sought, send a request to the Central MAL mailbox with detail of how the residual alerts will continue to be managed.

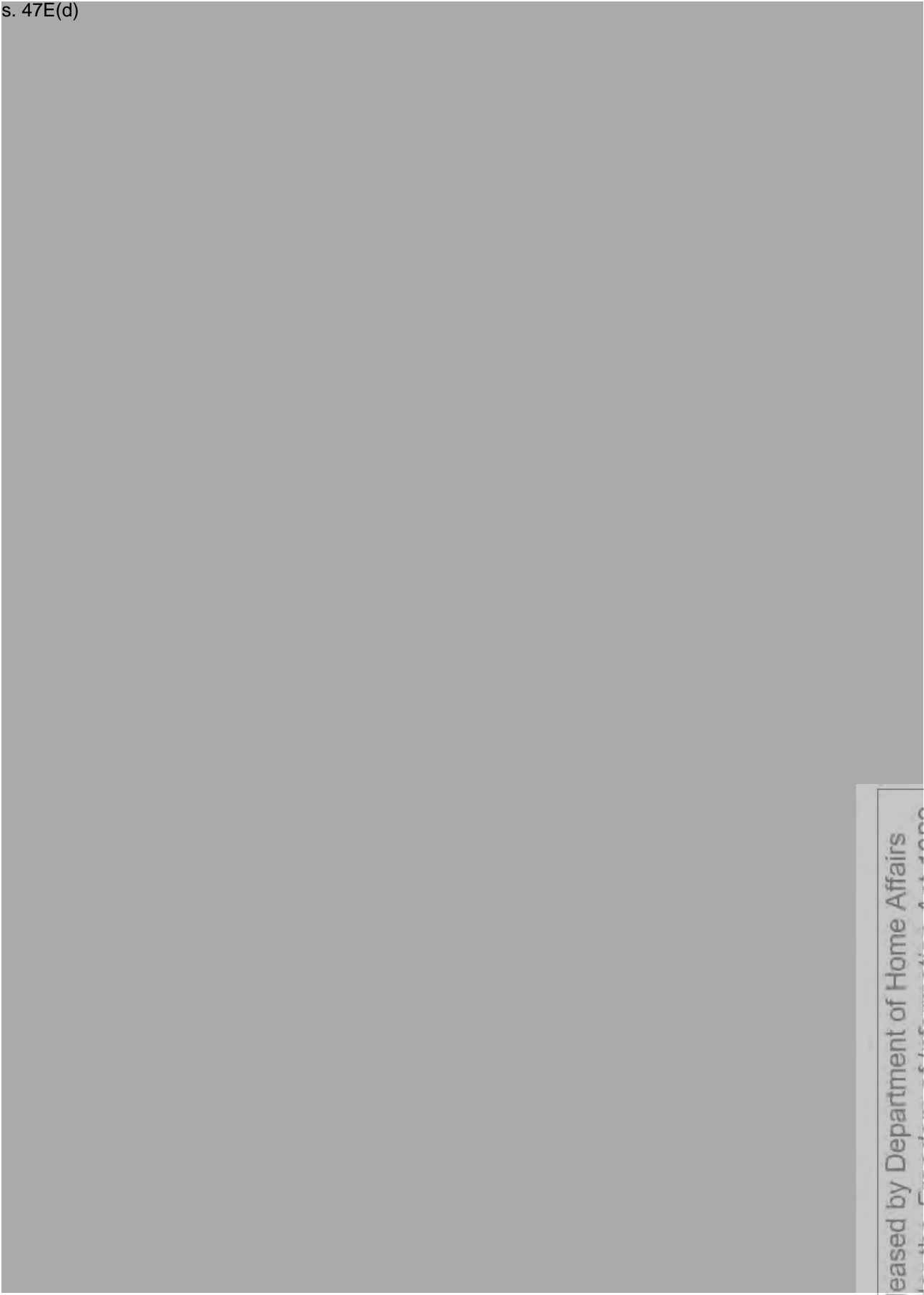
**Email:** s. 47E(d)

s. 47E(d)

s. 47E(d)

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

s. 47E(d)

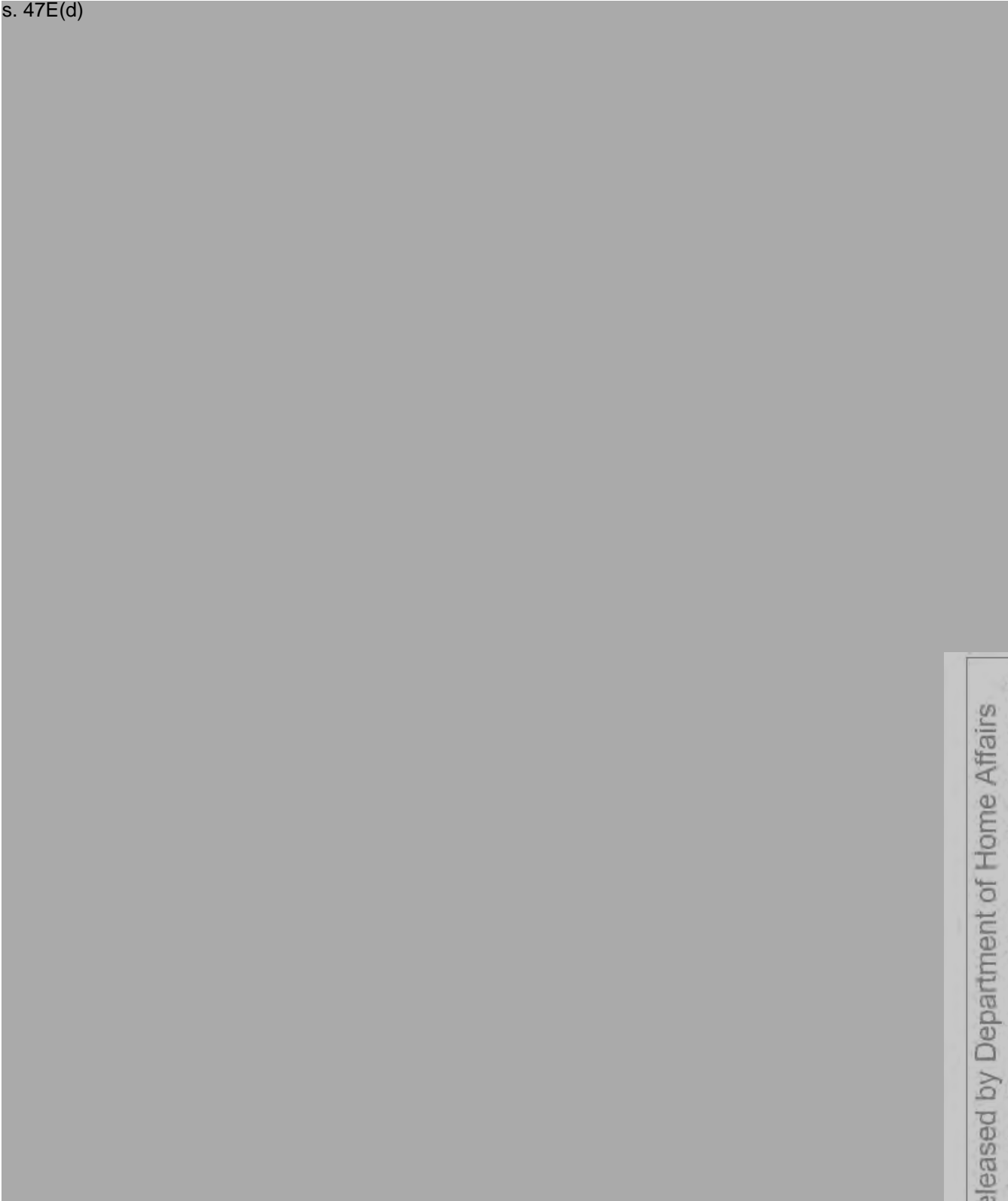


Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

s. 47E(d)



s. 47E(d)



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

s. 47E(d)

### 3.6. ARC 03 War crimes or human rights abuse

#### 3.6.1. ARC 03 policy

Attribute	Description
Risk category	High
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	
Groups	
Policy owner	
Role and responsibility of policy owner	
Operational owner	
Role and responsibility of operational owner	s. 47E(d) is responsible for sourcing, evaluating and qualifying the listing of all ARC 03 records.
Legislation	s501, <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	The Character Test: PIC 4001; PIC 4003 – National Security or Foreign Policy interest as advised by the Foreign Minister. See: Policy Implication for Public Interest Criteria
Policy for reviewing these records	Review in 10 years. The review period starts from the date the MAL record was created.

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

Attribute	Description
Variable threshold	Amber match at a score of 85 or above. Green at a score of 84 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to the BOC. <b>Email:</b> s. 47E(d) <b>Phone:</b> s. 22(1)(a)(ii)

### 3.6.2. ARC 03 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	Desirable
Date of birth	Year of birth is desirable; day and month are optional. No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	Optional
Country of Birth (COB) and Citizenship	Optional <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age; by default review 10 years from creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 120 years of age, or 100 years from creation date, whichever comes first. <b>Note:</b> The default expiry date can be changed.
Business rules	Refer true or potential matches.
Narrative	s. 47E(d)
Information status on Red match	'MAL status is Red.s. 47E(d)
Information status on Amber match	'MAL status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	Written advice from s. 47E(d)

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



### 3.7. ARC 04 Controversial visitors

#### 3.7.1. ARC 04 policy

Attribute	Description
Risk category	High
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)

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

Attribute	Description
Groups	s. 47E(d)
Policy owners	s. 47E(d)
Role and responsibility of policy owners	<p>The role of the [REDACTED] is to:</p> <ul style="list-style-type: none"> <li>• Provide advice to visa processing areas, the controversial visitor Concept of Operations and external stakeholders on the controversial visitor framework</li> <li>• Update/maintain the Controversial Visitor Procedures Advice Manual</li> <li>• Set minimum data standards that creators of ARC04 alerts must follow.</li> <li>• [REDACTED] also has responsibility for ARC18 – Travel Sanctions.</li> </ul>
Operational owners	The CVU within s. 47E(d) [REDACTED] deals with all operational aspects of controversial visitor alerts.
Role and responsibility of operational owners	The [REDACTED] within s. 47E(d) [REDACTED] receive referrals from visa processing areas and coordinates assessments for controversial visitors against the <i>Migration Act 1958</i> (character test and general cancellation provisions) and <i>Migration Regulations 1994</i> (PIC4003(a)) requirements. [REDACTED] s. 47E(d) provides advice on ARC04 matches.
Legislation	s501(6)(d)(iii)-(v) <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	<p><b>PIC 4001 provides that:</b></p> <p>Either:</p> <ul style="list-style-type: none"> <li>• the person satisfies the Minister that the person passes the character test; or</li> <li>• the Minister is satisfied, after appropriate inquiries, that there is nothing to indicate that the person would fail to satisfy the Minister that the person passes the character test; or</li> <li>• the Minister has decided not to refuse to grant a visa to the person despite reasonably suspecting that the person does not pass the character test; or</li> <li>• the Minister has decided not to refuse to grant a visa to the person despite not being satisfied that the person passes the character test.</li> </ul> <p>Note that the character provisions under section 501 of the <i>Migration Act 1958</i> apply to all visa applicants, even where PIC4001 is not a criterion for grant. Controversial Visitors are considered against these provisions, primarily but not exclusively, section 501(6)(d)(iii)-(v) of the <i>Migration Act</i>.</p> <p><b>PIC 4003(a) provides that:</b></p> <p>The applicant is not determined by the Foreign Minister, or a person authorised by the Foreign Minister, to be a person whose presence in Australia is, or would be, contrary to Australia's foreign policy interests. PIC4003 (a) assessments are conducted s. 47E(d) and may be decided by the Foreign Minister personally or by his/her [REDACTED] s. 47E(d) delegate.</p>

Attribute	Description
Policy for reviewing these records	Review in 10 years from the date the MAL record was created.
Variable threshold	Amber status at a score of 85 or above. Green status at a score of 84 or below.
Contact for further information	Initial enquiries should be directed to Border Operations Centre: Email: s. 47E(d) Phone s. 22(1)(a)(ii)

### 3.7.2. ARC 04 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory (unless business case provided to operational owner)</b>
Date of birth	Year of birth is mandatory; day and month are optional, yet desirable. No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	<b>Desirable</b>
Country of Birth (COB) and Citizenship	COB is desirable. Citizenship is mandatory. <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age; by default review 10 years from create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 120 years of age, or 100 years from creation date, whichever comes first. <b>Note:</b> The default expiry date can be changed.
Business rules	Refer true or potential matches (based on group code).
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d)
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)

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

Field	Description
Grounds or authority for expiry of the alert	Written advice from s. 47E(d) [REDACTED] is a team within this section.

### 3.8. ARC 05 Serious or high profile crime

#### 3.8.1. ARC 05 policy

Attribute	Description
Risk category	High
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d) [REDACTED]
Source of information	s. 47E(d) [REDACTED]
Groups	s. 47E(d) [REDACTED]

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



Attribute	Description
Policy owner	s. 47E(d) Email: s. 47E(d) Telephone: 02 s. 22(1)(a)(ii)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC, how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identifies the operational owner who is responsible for managing the MAL records for an ARC or ARC Group.</li> </ul>
Operational owner	s. 47E(d)
Role and responsibility of operational owner	The operational owner manages the alert record set for an ARC or ARC Group. They are responsible for: <ul style="list-style-type: none"> <li>dealing with requests for clarification of match case referrals</li> <li>liaising with the information source or sources</li> <li>maintaining the accuracy and currency of the MAL records (in conjunction with CMAL users, who must update alerts they have created as required)</li> <li>approving alert override requests, alert expiry requests and proposed changes to alert reason code</li> <li>making decisions on minimum data standards and information sources</li> <li>approval of new alerts where Minimum Data Standards are not strictly met.</li> </ul>
Legislation	s501, <i>Migration Act 1958</i>
Relevant Public Interest Criteria (PIC)	PIC 4001 <b>Note:</b> Section 501 still applies even if PIC 4001 is not a criterion.
Policy for reviewing these records	Review as updates arise, or in 10 years from the date the record was created.
Variable threshold	Amber status at a score of 85 or above Green status at a score of 84 or below.
Contact for further information	Policy enquiries should be directed to: s. 47E(d) Email: s. 47E(d) Telephone: 02 s. 22(1)(a)(ii) Additional contact: BOC Email: s. 47E(d) Telephone: s. 22(1)(a)(ii) See: CMAL contact list for additional contact details.

### 3.8.2. ARC 05 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> if no date of birth, <b>desirable</b> otherwise



Field	Description
Date of birth	Date of birth is <b>mandatory</b> , or if unknown, year of birth is <b>mandatory</b> . No minimum age. Maximum age is 120 years.
Other ARCs	Must not be listed with 09 or 25, and cannot be listed with s. 47E(d)
Gender/sex	Optional
Country of Birth (COB) and Citizenship	One <b>must</b> be entered. <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Desirable
Informer	<b>Mandatory</b>
Creation	Via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age. Default review 10 years from creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 100 years of age. No default expiry based on creation date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information on Red MAL status (true match)	'MAL Status is Red. s. 47E(d)
Information on Amber MAL status (potential match)	'MAL Status is Amber. Awaiting case assessment. If this case is urgent or the SLA has expired, contact the BOC for more information'. <b>Telephone:</b> s. 22(1)(a)(ii)
Grounds or authority for expiry of an alert	If granted Australian Citizenship, reaches the age of 100 or on written advice from the Assistant Director (EL1), s. 47E(d)

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

### 3.9. ARC 06 Health concerns

#### 3.9.1. ARC 06 policy

Attribute	Description
Risk category	Medium
Classification	OFFICIAL: Sensitive
Who s hould be listed	s. 47E(d)
Source of information	s. 47E(d)
Groups	s. 47E(d)

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

Attribute	Description
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	<ul style="list-style-type: none"> <li>s. 47E(d) defines the policy which underpins the ARC, makes decisions in consultation with the BOC on the match threshold score, minimum data standards and information sources</li> <li>reviews and monitors listings on a risk management basis.</li> </ul>
Operational owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of operational owner	The s. 47E(d) will initiate alerts for applicants who are non-compliant with their health undertaking in accordance with the Health Requirement Procedural Instruction. The s. 47E(d) will also update these records if they receive subsequent advice from the state or territory health authority that the applicant has complied.
Legislation	s60, s65 and s496 of the <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	PIC 4005 PIC 4007 See: <u>Sch4/4005-4007 – The Health Requirement</u>
Policy for reviewing these records	Periodically CMAL data management reviews will assess the narrative against group code.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	<p>Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre. Email: s. 47E(d) Phone s. 22(1)(a)</p> <p>In the first instance, VPOs should refer to the table above for information on specific codes and how to action CMAL alerts. In sensitive or complex cases, VPOs should contact s. 47E(d) for further advice and assistance. Email: s. 47E(d)</p> <p>See: <u>Sch4/4005-4007 – The Health Requirement</u></p>

### 3.9.2. ARC 06 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	Desirable (if known)
Date of birth	Date of birth is <b>mandatory</b> , or, if unknown, year of birth is <b>mandatory</b> (along with country of birth and/or citizenship). No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	Required
Country of Birth (COB) and Citizenship	One must be entered, but request both be entered wherever possible. <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia
Travel document	Optional

Field	Description	
Informer	<b>Mandatory</b>	
Creation	Interface from Health systems via CMAL Remote Input Function (CMAL RIF).	
CMAL default review date	No default review date based on age or creation date. <b>Note:</b> The default review date can be changed.	
CMAL default expiry date	Default expiry at 120 years of age. No default expiry based on creation date. <b>Note:</b> The default expiry date can be changed.	
Business rules	s. 47E(d)	
Narrative	s. 47E(d)	
Information status on Red match	'MAL Status is Red. s. 47E(d)	
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)	
Grounds or authority for expiry of the alert	s. 47E(d)	

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



Field	Description
	s. 47E(d)

### 3.10. ARC 07 Organised immigration malpractice

#### 3.10.1. ARC 07 policy

Attribute	Description
Risk category	High
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	s. 47E(d) as the policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status.</li> </ul>
Operational owner	s. 47E(d) Other informers are identified in the <u>narrative</u> or informer fields – for alerts listed prior to September 2018. For all alerts listed after 01 September 2018, the listing section is the operational owner of the alert.
Role and responsibility of operational owner	The listing section as the operational owner manages the alert record. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with information sources and maintaining the accuracy of the MAL record.
Legislation	s501 <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	The Character Test: PIC 4013. See: <u>Policy Implication for Public Interest Criteria</u> .
Policy for reviewing these records	Review in 10 years from the date the record was created. Expire at 100 years of age if convicted of people smuggling.

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

Attribute	Description
Variable threshold	Amber match at a score of 85 or above. Green at a score of 84 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: <b>Email:</b> s. 47E(d) <b>Telephone:</b> s. 22(1)(a)(ii)

### 3.10.2. ARC 07 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	Desirable (if known)
Date of birth	Date of birth is <b>mandatory</b> , or, if unknown, year of birth is <b>mandatory</b> (along with country of birth and/or citizenship). No minimum age: maximum age is 120 years.
Other ARCs	Must not be listed with 13.
Gender/sex	Mandatory
Country of Birth (COB) and Citizenship	At least one is mandatory – Both are desirable. Note: Australian citizens are permitted after EL2 approval of the listing section. <b>See:</b> <u>Considering Australian Identities for MAL</u>
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age. Default review 10 years from create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 100 years of age. No default expiry based on create date. <b>Note:</b> The default expiry date can be changed.
Business rules	Refer true or potential matches for requirements relating to listing Australian Citizens. <b>See:</b> <u>Considering Australian Identities for MAL</u>
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d)

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



Field	Description
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information. Telephone: s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	Written advice from s. 47E(d)

### 3.11. ARC 08 Child custody concerns

#### 3.11.1. ARC 08 policy

Attribute	Description
Risk category	Medium
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status

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

Attribute	Description
	<p>identifies the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</p> <p>makes decisions on the match threshold score, minimum data standards and information sources.</p> <p>Australia has obligations regarding the custody of children under the <i>Hague Convention on the Civil Aspects of Child Abduction</i> and the <i>Hague Convention on Intercountry Adoption</i>. Public Interest Criteria 4015 and 4017 are designed to uphold these obligations by ensuring that children can only be granted a visa when these criteria are met. This means that either each person who is legally able to determine where a child lives consents to the grant of the visa, or that the grant of the visa would be consistent with an order made by a court of Australia or the child's own country. Additional criteria must also be met for children undergoing adoption proceedings.</p> <p>Information may be brought to the Department's attention through court proceedings in either Australia or the child's home country, referrals from child welfare authorities and through correspondence with the child's parent.</p> <p>Where officers become aware of children that may be at risk of being brought to Australia under such circumstances, they should contact s. 47E(d) for advice.</p>
Operational owner	<p>s. 47E(d) manage the listing of Child Custody concerns for foreign citizens.</p> <p><b>Note:</b> The policy owner and operational owner are the same section.</p>
Role and responsibility of operational owner	<p>The operational owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.</p> <p><b>Note:</b> Individual records are not kept with s. 47E(d). Case officers must maintain records in this regard.</p>
Legislation	<p>State and territory child protection legislation (applicable in each state and territory, various dates)</p> <p>Reg.1.04 – <i>Migration Regulations 1994</i> (Migration Regulations)</p> <p>Schedule 2 criteria – Migration Regulations following visa subclasses: 802, 837, 101, 102, 117, 445</p>
Relevant Public Interest Criteria (PIC)	<ul style="list-style-type: none"> <li>PIC 4015</li> <li>PIC 4017</li> </ul> <p>See: <u>Policy Implication for Public Interest Criteria</u></p>
Policy for reviewing these records	<p>Alert may be reviewed, prior to the child turning 18 years of age, if parental responsibility issues are resolved through:</p> <p>a court order from Australia or the child's home country being presented or permission for the visa to be granted is provided by the representative/s with legal/formal parental responsibility (custody) for the child.</p> <p>If allegation only received, review in one month from the date the record was created.</p>
Variable threshold	<p>Amber match at a score of 95 or above.</p> <p>Green at a score of 94 or below.</p>
Contact for further information	<p>Initial enquiries should be directed to the nominated ARC policy owner.</p> <p>Further enquiries can be directed to Border Operations Centre:</p> <p><b>Email:</b> s. 47E(d)</p> <p><b>Telephone:</b> s. 22(1)(a)(ii)</p>

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

## 3.11.2. ARC 08 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	Date of birth is <b>mandatory</b> , or, if unknown, year of birth is <b>mandatory</b> (along with country of birth and/or citizenship). No minimum age: maximum age is 18 years.
Other ARCs	Cannot be listed with <b>s. 47E(d)</b>
Gender/sex	Required
Country of Birth (COB) and Citizenship	One <b>must</b> be entered. <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age or creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 18 years of age. No default expiry based on create date. <b>Note:</b> The default expiry date can be changed.
Business rules	<b>s. 47E(d)</b>
Narrative	<b>s. 47E(d)</b>
Information status on Red match	'MAL Status is Red. <b>s. 47E(d)</b>
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on <b>s. 22(1)(a)(ii)</b>
Grounds or authority for expiry of the alert	If the child has reached 18 years of age or on written advice from the requesting parents/guardians that parental responsibility (custody) issues have been satisfactorily resolved.

## 3.12. ARC 09 Other criminals

## 3.12.1. ARC 09 policy

Attribute	Description
Risk category	Medium
Classification	OFFICIAL: Sensitive



Attribute	Description
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Groups	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The Policy Owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	s. 47E(d)
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	S501 <i>Migration Act 1958</i> and <i>Foreign Acquisitions and Takeovers Act 1975</i> .
Relevant Public Interest Criteria (PIC)	The Character Test: PIC 4001 See: <u><a href="#">Policy Implications for Public Interest Criteria</a></u>
Policy for reviewing these records	If allegation only received, review in 60 days. Contact BOC if more time is needed. Persons alleged to be in breach of FATA, expire in 10 years. Expire at 100 years of age or if granted Australian Citizenship.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.

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

Attribute	Description
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: Email: [REDACTED] Phone: s. 22(1)(a)(ii) [REDACTED]

### 3.12.2. ARC 09 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	Date of birth is <b>mandatory</b> , or, if unknown, year of birth is <b>mandatory</b> (along with country of birth and/or citizenship). No minimum age: maximum age is 120 years.
Other ARCs	Must not be listed with 05, 25. Cannot be listed with s. 47E(d)
Gender/sex	Optional
Country of Birth (COB) and Citizenship	Optional <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date- based on age or create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 100 years of age. No default expiry based on create date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red s. 47E(d)
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	If granted Australian Citizenship or on written advice from the Assistant Director (EL1) s. 47E(d)

### 3.13. ARC 10 Overstayers

#### 3.13.1. ARC 10 policy

Attribute	Description
Risk category	Low
Classification	OFFICIAL: Sensitive



Attribute	Description
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	<p>The policy owner:</p> <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a person has a Red MAL status</li> <li>identifies the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>makes decisions on the match threshold score, minimum data standards and information sources</li> <li>works with the CMAL training area to ensure training courses include material about Minimum Data Standards (MDS) obligations</li> </ul>
Operational owner	The informer of the alert record.
Role and responsibility of operational owner	<p>The Operational Owner:</p> <ul style="list-style-type: none"> <li>manages a set of records within an ARC or ARC group</li> <li>holds the evidence for each record listing</li> <li>deals with requests to clarify match case referrals</li> <li>liaises with the information source(s)</li> <li>maintains the accuracy and currency of the MAL records.</li> </ul>
Legislation	Schedule 4 of the <i>Migration Regulations 1994</i>
Relevant Public Interest Criteria (PIC)	PIC 4014

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

Attribute	Description
Policy for reviewing these records	Expire in three years from the date the person left Australia (Refer PIC subclause 4014(1) of the <i>Migration Regulations 1994</i> ).
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: Email: s. 47E(d) Telephone: s. 22(1)(a)(ii)

### 3.13.2. ARC 10 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> – Dash “-” can be used if no given name exists
Date of birth	<b>Mandatory</b> - No minimum age; maximum age is 120 years
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	<b>Mandatory</b>
Country of Birth (COB) and Citizenship	<b>Mandatory</b> <b>Note:</b> Australian citizens not permitted. Can include non-citizens whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age or creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	By default, expire three years from create date (being the date the person left Australia). <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)

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

Field	Description
Information status on Red match	'MAL Status is Red. s. 47E(d)
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	If PIC 4014 no longer applies.

### 3.14. ARC 11 Breach of visa conditions

#### 3.14.1. ARC 11 policy

Attribute	Description
Risk category	Low
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	Compliance Officers in the applicable state and territory office.
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	Schedule 4 of the Migration Regulations. S116 of the <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	PIC 4013. <b>See:</b> <u>Policy Implications for Public Interest Criteria</u>

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



Attribute	Description
Policy for reviewing these records	Expire in three years from the date of cancellation <b>Note:</b> Clients whose visa have been cancelled due to breach of visa conditions are subject to a three-year exclusion period from being granted another visa.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre. <b>Email:</b> s. 47E(d) <b>Telephone:</b> s. 22(1)(a)(ii)

### 3.14.2. ARC 11 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	<b>Mandatory.</b> No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	Required
Country of Birth (COB) and Citizenship	Optional <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF) or CMAL RIF by system interface.
CMAL default review date	No default review date based on age or creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	No default expiry age. By default, expire three years from create date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d)

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

Field	Description
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	If any risk factors for PIC4013 no longer apply.

### 3.15. ARC 12 Debts to the Commonwealth

#### 3.15.1. ARC 12 policy

Attribute	Description
Risk category	Low
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of operational owner	s. 47E(d) will deal with enquiries about the status of a client debt and ensure that records are updated as debt is cleared as appropriate. The operational owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	s501, Migration Act 1958

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

Attribute	Description
Relevant Public Interest Criteria (PIC)	PIC 4004. <b>See:</b> <u>Policy Implications for Public Interest Criteria</u>
Policy for reviewing these records	Debts expire at age 100 years. When debt is repaid, record may be updated with receipt number, and then expired.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: <b>Email:</b> S. 47E(d) <b>Phone:</b> S. 22(1)(a)(ii)

### 3.15.2. ARC 12 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	<b>Mandatory</b> . No minimum age. Maximum age is 120 years.
Other ARCs	Cannot be listed with S. 47E(d)
Gender/sex	<b>Mandatory</b>
Country of Birth (COB) and Citizenship	<b>Mandatory</b> <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b> RRT-DBT, LEG-DBT, REM-DBT, OTH-DBT, ACS, etc. indicates source.
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age or create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 100 years of age. No default expiry based on creation date. <b>Note:</b> The default expiry date can be changed.
Business rules	S. 47E(d)
Narrative	S. 47E(d)
Information status on Red match	'MAL Status is Red. S. 47E(d)

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



Field	Description
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii).
Grounds or authority for expiry of the alert	<ul style="list-style-type: none"> <li>If the debt has been waived or paid in full.</li> <li>If arrangements have been made to repay the debt by non-citizens, the record must remain.</li> <li>When the debt is paid, then the receipt number should be recorded and the record should be expired.</li> </ul> <p>Note: Must be removed if granted Australian citizenship.</p>

### 3.16. ARC 13 Immigration malpractice

#### 3.16.1. ARC 13 policy

Attribute	Description
Risk category	Low
Classification	For-Official-Use-Only
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Groups	s. 47E(d)
Policy owner	s. 47E(d) Email s. 47E(d)
Role and responsibility of policy owner	<p>The policy owner:</p> <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identifies the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>makes decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	The Informer of the alert record.
Role and responsibility of	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with

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

Attribute	Description
operational owner	requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	s501 <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	The Character Test: PIC 4013. See: <u>Policy Implications for Public Interest Criteria</u>
Policy for reviewing these records	If: <ul style="list-style-type: none"> <li>departed, expire in three years from the departure date, or</li> <li>not departed, review in the three years from the date the record was created.</li> </ul>
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre. Email: S. 47E(d) Phone: S. 22(1)(a)(ii)

### 3.16.2. ARC 13 CMAL system constraints

Field	Description
Family name	Mandatory.
Given name	Mandatory.
Date of birth	Mandatory. No minimum age: maximum age is 120 years.
Other ARCs	Must not be listed with 07. Cannot be listed with 6.4724
Gender/sex	Mandatory.
Country of Birth (COB) and Citizenship	Mandatory. Note: Australian citizens are not permitted. Can include people whose COB is Australia.
Travel document	Mandatory.
Informer	Mandatory.
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age or create date. Note: The default review date can be changed.
CMAL default expiry date	No default expiry by age. By default expire three years from create date. Note: The default expiry date can be changed.
Business rules	S. 47E(d)

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

Field	Description
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d)
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	The alert must remain active for the duration of the exclusion period—three years in accordance with PIC 4013. Early expiration can occur with written advice from Assistant Director, or Director, s. 47E(d)

### 3.17. ARC 14 Bypassed/refused immigration clearance

#### 3.17.1. ARC 14 policy

Attribute	Description
Risk category	Low
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)



Attribute	Description
Source of information	s. 47E(d)
Groups	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d) s. 47E(d) s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	<p>The policy owner:</p> <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul> <p><b>Border Clearance:</b> Consideration of the processing of identities referred at Airports and Sea Ports.</p> <p><b>Irregular Maritime Arrivals (IMA):</b> Consideration of the circumstances and timing of listing of detainees.</p>
Operational owner	s. 47E(d)
Role and responsibility of operational owner	<p>The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records, Border Clearance Procedures for listing identities referred at Airports and Sea Ports</p> <p>Irregular Maritime Arrivals (IMA): Procedures for processing Irregular Maritime Arrivals such that the correct outcome is achieved for the MAL record.</p>
Legislation	Division 5 of the <i>Migration Act 1958</i>
Relevant Public Interest Criteria (PIC)	N/A. Refer to border policy.
Policy for reviewing these records	Expire in three years from the date of departure. If not departed, then from the date the record was created.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	<p>Initial enquiries should be directed to the nominated ARC policy owner.</p> <p>Further enquiries can be directed to Border Operations Centre: Email: s. 47E(d) Phone: s. 22(1)(a)(ii)</p>

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

### 3.17.2. ARC 14 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	<b>Mandatory</b> (at least year). No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with <b>s. 47E(d)</b>
Gender/sex	<b>Mandatory</b>
Country of Birth (COB) and Citizenship	<b>Mandatory</b> (one must be entered) <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF). <b>Note:</b> IMA clients should not be entered into MAL until their case has been fully evaluated otherwise the MAL Check becomes a self-fulfilling outcome.
CMAL default review date	No default review date based on age or creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	No default expiry by age. By default expire three years from creation date. <b>Note:</b> The default expiry date can be changed.
Business rules	<b>s. 47E(d)</b>
Narrative	<b>s. 47E(d)</b>
Information status on Red match	'MAL Status is Red. <b>s. 47E(d)</b>
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on <b>s. 22(1)(a)(ii)</b>

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



Field	Description
Grounds or authority for expiry of the alert	If PIC 4013 or 4014 is found to be met or if any existing risk factor no longer applies (see section 501, 501A & 501B as cancellation on character grounds may apply).

### 3.18. ARC 16 Suspect genuineness

#### 3.18.1. ARC 16 policy

Attribute	Description
Risk category	Low
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	The following group category applies to this ARC: BONAFIDES
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC, how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status. identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	s. 47E(d)
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	Sections 91W, 91WA and 116 of the <i>Migration Act 1958</i> relate to identity concerns detected during the application process.
Relevant Public Interest Criteria (PIC)	Identity concerns during the visa or citizenship application process or border processing. PIC 4020. See: Policy Implications for Public Interest Criteria (Support Material) 2.13 PIC 4020 The Integrity PIC ARC 20

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

Attribute	Description
Policy for reviewing these records	If: <ul style="list-style-type: none"> <li>departed - expire in three years from the departure date, or</li> <li>not departed - review in the three years from the date the record was created.</li> </ul>
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre. Email: s. 47E(d) Phone: s. 22(1)(a)(ii)

### 3.18.2. ARC 16 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	<b>Mandatory</b> . No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	<b>Mandatory</b>
Country of Birth (COB) and Citizenship	<b>Mandatory</b> (one must be entered) <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional
Informer	<b>Mandatory</b>
Creation	Informer via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age or creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	No default expiry by age. By default expire three years from creation date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d)
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	If PIC 4013 or 4014 is found to be met or if any existing risk factor no longer applies (see section 501, 501a & 501b as cancellation on character grounds may apply).

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

### 3.19. ARC 17 Surrender Australian travel document

#### 3.19.1. ARC 17 policy


Attribute	Description
Risk category	Low
Classification	OFFICIAL: Sensitive
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	No Groups apply to this ARC.
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	s. 47E(d) is responsible for updating the status of the passport in the Australian Passport Database. s. 47E(d) is represented by s. 47E(d). The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of operational owner	s. 47E(d) will liaise with s. 47E(d) on the cancellation of damaged documents in the Australian Passport Database. The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	Australian Passport Act 2005.
Relevant Public Interest Criteria (PIC)	N/A. Integrity of identity.
Policy for reviewing these records	Review one month after listing. Expire 12 months from the date the record was created.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.

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



Attribute	Description
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre. Email: s. 47E(d) Telephone: s. 22(1)(a)(ii)

### 3.19.2. ARC 17 CMAL system constraints

Field	Description
Family name	<b>Mandatory</b>
Given name	<b>Mandatory</b> (if known)
Date of birth	<b>Mandatory</b> (at least year). No minimum age: maximum age is 120 years.
Other ARCs	Cannot be listed with 
Gender/sex	<b>Mandatory</b>
Country of Birth (COB) and Citizenship	<b>Mandatory</b> (one must be entered) <b>Note:</b> Australian citizens are permitted at the discretion of ABF officers and Airport Liaison Officers. <b>See:</b> <u>Considering Australian Identities for MAL</u>
Travel document	Required
Informer	Mandatory
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age. Default review date one month from creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	No default expiry by age. By default expire one year from creation date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d) s.'
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	If PIC 4013 or 4014 is found to be met or if any existing risk factor no longer applies (see section 501, 501a & 501b as cancellation on character grounds may apply).

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



### 3.20. ARC 18 Travel sanctions

#### 3.20.1. ARC 18 policy

Attribute	Description
Risk category	High.
Classification	OFFICIAL: Sensitive.
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	<p>The s. 47E(d) has procedural responsibility for PIC 4003(a) relating to Foreign Minister 'foreign interests' determinations and PIC 4003(c) relating to autonomous travel sanctions declarations respectively.</p> <p>s. 47E(d) also has procedural responsibility for the UNSC Resolutions Regulations Procedures Advice Manual s. 47E(d) ensures that UNSC Resolutions are implemented through Legislative Instruments under these regulations. s. 47E(d) has delegation to refuse under s.65 persons' subject to travel sanctions, as do A-based at Posts. s. 47E(d) will liaise with s. 47E(d) on whether travel sanctions or foreign policy determinations are in effect/can be waived/ out of effect s. 47E(d) also has responsibility for ARC 04.</p> <p>The policy owner is responsible for identifying the sources and defining the applicable group codes.</p> <p>The policy owner:</p> <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status.</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group.</li> </ul>
Operational owner	s. 47E(d)
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the

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

Attribute	Description
	MAL records. Creators of alerts are responsible for storing/filing evidence for the listing of a record.
UNSC	s. 47E(d) is responsible for and maintains the list of people designated under UNSC resolutions s. 47E(d) should seek clarification of MAL matches directly from s. 47E(d) and s. 47E(d)
Autonomous Foreign	Australia's Autonomous Sanctions are implemented under the Foreign Minister's powers and the <i>Autonomous Sanctions Act</i> . Australia's Foreign Policy travel sanctions are implemented under the Foreign Minister's powers and the <i>Migration Regulations 1994</i> .
Legislation	s501 <i>Migration Act 1958</i> . <i>UN Security Council resolutions</i> . Australia meets its obligations to enforce UNSC Travel Sanctions through the UNSC Resolutions Regulations. The Minister for Home Affairs has the power to prescribe a ground for cancelling a visa under section 116(1)(g) of the Migration Act. The legislative instrument is revised each time a resolution imposing new travel sanctions is passed, or if existing travel sanctions are removed or amended. <i>Autonomous Sanctions Act 2011</i> Autonomous policy travel restrictions are implemented under the Foreign Minister's powers specified by Public Interest Criterion 4003(c) at Schedule 4 of the <i>Migration Regulations 1994</i> (Migration Regulations) for visa refusal matters, and section 116(1)(g) with reference to regulation 2.43(1)(a)(i)(A) for visa cancellation matters. <i>Foreign Policy Sanctions</i> Foreign policy travel restrictions are implemented under the Foreign Minister's powers specified by Public Interest Criterion 4003(a) at Schedule 4 of the Migration Regulations for visa refusal matters, and section 116(1)(g) with reference to regulation 2.43(1)(a)(i)(A) for possible visa cancellation matters.
Relevant Public Interest Criteria (PIC)	PIC 4003(a) – not in Australia's foreign policy interests. PIC 4003(c) – Autonomous travel sanctions, as declared under Autonomous Sanctions Regulations 2011. <b>See: <u>Policy Implications for Public Interest Criteria</u></b>
Policy for reviewing these records	Review in five years from the date the record was created.
Variable threshold	Amber match at a score of 85 or above. Green at a score of 84 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: <b>Email:</b> s. 47E(d) <b>Telephone:</b> s. 22(1)(a)(ii)

### 3.20.2. ARC 18 CMAL system constraints

Field	Description
Family name	<b>Mandatory.</b>
Given name	Desirable (if known).
Date of birth	Year of birth is mandatory (along with citizenship), day and month are desirable. No minimum age: maximum age is 120 years.



Field	Description
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	Optional.
Country of Birth (COB) and Citizenship	COB is desirable. Citizenship is mandatory (with year of birth). <b>Note:</b> Australian citizens are not permitted. Can include people whose COB is Australia.
Travel document	Desirable.
Informer	<b>Mandatory.</b>
Creation	Owner via s. 47E(d) Remote Input Function s. 47E(d) RIF).
CMAL default review date	No default review date based on age. Default review date five years from create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	Default expiry at 120 years of age, or 100 years from create date, whichever comes first. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d) There is no need to contact the BOC.'
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii) s. 47E(d)'
Grounds or authority for expiry of the alert	Expired on advice from s. 47E(d)

### 3.21. ARC 19 Illegal fishers

#### 3.21.1. ARC 19 policy



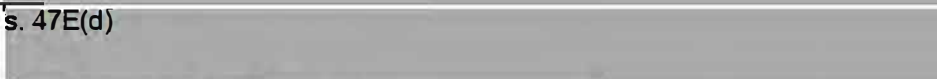



Attribute	Description
Risk category	Low.
Classification	OFFICIAL: Sensitive.
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)

Attribute	Description
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the sources, group codes and operational ownership</li> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	s. 47E(d)
Role and responsibility of operational owner	The operational owner will liaise with the Australian Fisheries Management Authority (AFMA) and the Department as applicable to ensure that the correct detention procedure is followed and that compliance with the appropriate legislation is observed.  The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	<i>Fisheries Management Act 1991</i> <i>Torres Strait Fisheries Act 1984</i> Section 164B of the <i>Migration Act 1958</i>
Relevant Public Interest Criteria (PIC)	The Character Test: PIC 4014. <b>See:</b> <u>Policy Implications for Public Interest Criteria</u>
Policy for reviewing these records	Expire in five years from the date the record was created.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: Email: s. 47E(d) Phone: s. 22(1)(a)(ii)

## 3.21.2. ARC 19 CMAL system constraints


Field	Description
Family name	<b>Mandatory.</b>
Given name	<b>Mandatory</b> (dash '-' the minimum for given name)
Date of birth	<b>Mandatory</b> (at least year). No minimum age: maximum age is 120 years.



Field	Description
Other ARCs	Cannot be listed with 
Gender/sex	<b>Mandatory.</b>
Country of Birth (COB) and Citizenship	<b>Mandatory</b> (one must be entered) <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	<b>Optional.</b>
Informer	<b>Mandatory.</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age or create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	No default expiry by age. By default expire five years from create date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d) 
Narrative	s. 47E(d) 
Information status on Red match	'MAL Status is Red. s. 47E(d) 
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii) 
Grounds or authority for expiry of the alert	If granted Australian Citizenship or on written advice from the Superintendent, s. 47E(d) 

### 3.22. ARC 20 Visa Fraud

#### 3.22.1. ARC 20 policy

Attribute	Description
Risk category	High.
Classification	OFFICIAL: Sensitive.
Who should be listed	s. 47E(d) 

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

Attribute	Description
	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identifies the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>makes decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	The informer of the alert record.
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	Sections 91W, 91WA and 116 of the <i>Migration Act 1958</i> relate to identity concerns detected during the application process. Schedule 4 to the Migration Regulations.
Relevant Public Interest Criteria (PIC)	PIC 4020 - Integrity PIC. Contact: s. 47E(d)
Policy for reviewing these records	Records expire three or 10 years after the date of the visa refusal and when AAT or the courts remit our decision.
Variable threshold	Amber match at a score of 95 or above. Green at a score of 94 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner. Further enquiries can be directed to Border Operations Centre: Email: s. 47E(d) Telephone: s. 22(1)(a)(ii)

### 3.22.2. ARC 20 CMAL system constraints

Field	Description
Family name	Mandatory.
Given name	Mandatory.
Date of birth	Mandatory. No minimum age: maximum age is 120 years.

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

Field	Description
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	<b>Mandatory.</b>
Group	<b>Mandatory.</b> <b>Note:</b> There are three group codes: <ul style="list-style-type: none"> <li>PIC4020 - IDENTITY - 10 year exclusion</li> <li>PIC4020 - OTHER - 3 year exclusion</li> <li>PIC4020 - MINOR - No exclusion applies</li> </ul>
Country of Birth (COB) and Citizenship	<b>Mandatory.</b> <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	<b>Mandatory.</b> <b>Note:</b> If you have travel document please include this information, as it will assist in linking client's identities.
Informer	<b>Mandatory.</b>
Creation	Informer via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date- based on age or creation date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	<b>Mandatory.</b> <b>Note:</b> The expiry date must be entered manually and should be either three or ten years from the date of refusal.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d)'
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)'
Grounds or authority for expiry of the alert	If PIC 4020 is found to be met or if any existing risk factor no longer applies.

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



### 3.23. ARC 22 INTERPOL (Australian Federal Police)

#### 3.23.1. ARC 22 policy

Attribute	Description
Risk category	High.
Classification	OFFICIAL: Sensitive.
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Group	s. 47E(d)
Policy owner	s. 47E(d) Email s. 47E(d) Telephone: s. 22(1)(a)(ii) s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the policy which backs up the ARC, how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>Managing all aspects of the True Match Notification caseload, including consideration of visa cancellation where appropriate.</li> </ul>
Operational owner	s. 47E(d) s. 47E(d) s. 47E(d) Email: s. 47E(d)
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	Section 501 of the Migration Act 1958
Relevant Public Interest Criteria (PIC)	PIC 4001 Note: Section 501 still applies even if PIC 4001 is not a criterion associated to the visa.
Policy for reviewing these records	Review as updates arise, or in 10 years from the date the record was created.
Variable threshold	Amber status at a score of 85 or above Green status at a score of 84 or below.
Contact for further information	Initial enquiries should be directed to the nominated ARC policy owner.

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



Attribute	Description
	Further enquiries can be directed to Border Operations Centre: Email: s. 47E(d) Phone: s. 22(1)(a)(ii)

### 3.23.2. ARC 22 CMAL system constraints

Field	Description
Family name	<b>Mandatory.</b>
Given name	<b>Mandatory</b> if no date of birth, <b>desirable</b> otherwise.
Date of birth	Date of birth is <b>mandatory</b> , or if unknown, year of birth is <b>mandatory</b> . No minimum age. Maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	Required.
Country of Birth (COB) and Citizenship	One <b>must</b> be entered. <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Desirable.
Informer	<b>Mandatory.</b>
Creation	The Border Operations Centre (BOC) loads INTERPOL notices into CMAL and actions INTERPOL addendum emails on behalf of the ARC owner.
CMAL default review date	No default review date.
CMAL default expiry date	Default expiry at 100 years of age. No default expiry based on create date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d) . If after consulting the narrative please use the following override key <xxxx>. There is no need to contact the BOC.'
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment. If this case is urgent or the SLA has expired, contact the BOC for more information'. Telephone: s. 22(1)(a)(ii) Email: s. 47E(d)

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

Field	Description
Grounds or authority for expiry of the alert	If granted Australian Citizenship, reaches the age of 100 or on written advice from the Assistant Director (EL1), s. 47E(d)

### 3.24. ARC 23 Identity

#### 3.24.1. ARC 23 policy

Attribute	Description
Risk category	Medium.
Classification	OFFICIAL: Sensitive.
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Groups	s. 47E(d)
Policy owner	s. 47E(d) Email: s. 47E(d)

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

Attribute	Description
Role and responsibility of policy owner	<p>s. 47E(d) is responsible for:</p> <ul style="list-style-type: none"> <li>Coordinating the update of policy and procedures including: <ul style="list-style-type: none"> <li>Enterprise Identity Procedural Instruction (EIPI) and Enterprise Identity Standard Operating Procedures (EISOPS)</li> <li>CMAL Procedural Instructions relating to <ul style="list-style-type: none"> <li>The reason for the ARC 23 listing</li> </ul> </li> </ul> </li> <li>Identifying the operational owner responsible for managing the MAL records for the ARC Group/s.</li> <li>Deciding the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	<p>s. 47E(d) Email: s. 47E(d) s. 47E(d)</p>
Role and responsibility of operational owner	<p>The s. 47E(d) is responsible for:</p> <ul style="list-style-type: none"> <li>Updating and management of all records</li> <li>Management of the complete alert record list</li> <li>Reference to the evidence required for listing of a record</li> <li>Responding to requests for clarification of match case referrals</li> <li>Liaising with the alert proposers</li> <li>Maintaining the accuracy and currency of the MAL records.</li> </ul>
Alert creator	Identity Integrity Officers.
Role and responsibility of alert creator	<p>Alert creators are responsible for:</p> <ul style="list-style-type: none"> <li>Investigating an identity match</li> <li>Referral/escalation process</li> <li>Advising where evidence supporting an alert record can be found</li> <li>How a decision is made when a client has a red MAL status</li> <li>Responding to requests for further information or additional action made by the BOC</li> <li>All required updates to alerts (such as narrative updates to include new information, visa grant/refusal).</li> </ul>
Legislation	<p>Character: s501, s116, s109, s128 <i>Migration Act 1958</i>. Division 1 of Part 3 of the <i>Australian Citizenship Act 2007</i>.</p>
Relevant Public Interest Criteria (PIC)	<p>False or misleading information: PIC 4020 (ARC20). See: <u>Policy Implications for Public Interest Criteria</u></p>
Policy for reviewing these records	Review in 5 years. The review period starts from the date the MAL record was created.
Variable threshold	Amber match at a score of 95 or above.
Contact for further information	<p>Initial enquiries during business hours should be directed to the s. 47E(d) Email: s. 47E(d) After-hours contact the Border Operations Center (BOC): Email: s. 47E(d) Phone: s. 22(1)(a)(ii)</p>

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



### 3.24.2. ARC 23 CMAL system constraints

Field	Description
Group code	Mandatory.
Family name	Mandatory.
Given name	Mandatory (where there is one).
Date of birth	Year of birth is Mandatory; day and month are desirable. No minimum age; maximum age is 120 years.
Other ARCs	Cannot be listed with s. 47E(d)
Gender/sex	Mandatory.
Country of Birth (COB) and Citizenship	At least one is Mandatory – both are desirable Note: Australian citizens are permitted. Can include people whose COB is Australia. This requires Director level approval from alert sponsor program area. Written approval should be trimmed and reference # included in creation.
Travel document	Mandatory (where travel documents are available).
Client ID	Mandatory.
Informer	Mandatory.
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	All listings to undergo review 5 years from creation date. Note: The default review date can be changed.
CMAL default expiry date	Default expiry at age 120. Note: The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	"MAL status is Red. s. 47E(d) Please consider the information contained in the narrative. Prior to making any visa or citizenship decisions you must contact the nominated contact person/business area.

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



Field	Description
Information status on Amber match	"MAL status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)
Grounds or authority for expiry of the alert	Advice from relevant Director or Assistant Director from the alert owner's business area must be obtained in writing and recorded in TRIM.

### 3.25. ARC 25 Serious criminal (poor bio-data)

#### 3.25.1. ARC 25 policy

Attribute	Description
Risk category	High.
Classification	OFFICIAL: Sensitive.
Who should be listed	s. 47E(d)
Source of information	s. 47E(d)
Groups	s. 47E(d)
Policy owner	s. 47E(d) s. 47E(d) Email: s. 47E(d) s. 47E(d) Email: s. 47E(d)
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>defines the sources, group codes and operational ownership</li> <li>defines the policy which backs up the ARC; how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>identify the operational owner who is responsible for managing the MAL records for an ARC or ARC Group</li> <li>make decisions on the match threshold score, minimum data standards and information sources.</li> </ul>
Operational owner	s. 47E(d) Also BOC s. 47E(d) ) for s. 47E(d) notices and diffusions.
Role and responsibility of operational owner	The Operational Owner manages the alert record set for an ARC or ARC/Group. They are responsible for holding the evidence for the listing of a record, dealing

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

Attribute	Description
	with requests for clarification of match case referrals, liaising with the information source or sources and maintaining the accuracy and currency of the MAL records.
Legislation	s501 <i>Migration Act 1958</i> .
Relevant Public Interest Criteria (PIC)	The Character Test: PIC 4001. <b>See:</b> <u>Policy Implications for Public Interest Criteria</u>
Policy for reviewing these records	Review in two years from the date the record was created, or update to Alert Reason Code 05 if more bio-data can be identified.
Variable threshold	Amber match at a score of 85 or above. Green at a score of 84 or below.
Contact for further information	Initial enquiries should be directed to Border Operations Centre: <b>Email:</b> s. 47E(d) <b>Telephone:</b> s. 22(1)(a)(ii)

## 3.25.2. ARC 25 CMAL system constraints

Field	Description
Family name	<b>Mandatory.</b>
Given name	Desirable.
Date of birth	Year desirable. Day and month optional. No minimum or maximum age.
Other ARCs	Must not be listed with 05 or 09 s. 47E(d)
Gender/sex	Optional.
Country of Birth (COB) and Citizenship	Optional. <b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.
Travel document	Optional.
Informer	<b>Mandatory.</b>
Creation	Owner via CMAL Remote Input Function (CMAL RIF).
CMAL default review date	No default review date based on age. Default review two years from create date. <b>Note:</b> The default review date can be changed.
CMAL default expiry date	No default expiry by age. By default expire 100 years from create date. <b>Note:</b> The default expiry date can be changed.
Business rules	s. 47E(d)
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d) If after consulting the narrative and you wish to override, please use the following override key <xxxx>. There is no need to contact the BOC.'

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

Field	Description
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii) [REDACTED]
Grounds or authority for expiry of the alert	If granted Australian Citizenship, or on written advice from the Assistant Director or Director, s. 47E(d) [REDACTED]

### 3.26. ARC 26 INTERPOL (Missing Children)

#### 3.26.1. ARC 26 policy

Attribute	Description
Risk category	Medium.
Classification	Official: Sensitive.
Who should be listed	s. 47E(d) [REDACTED]
Source of information	s. 47E(d) [REDACTED]
Group	s. 47E(d) [REDACTED]
Policy owner	s. 47E(d) [REDACTED] Email: s. 47E(d) [REDACTED] s. 47E(d) [REDACTED] Email: s. 47E(d) [REDACTED]
Role and responsibility of policy owner	The policy owner: <ul style="list-style-type: none"> <li>Defines the policy which backs up the ARC, how data is sourced, what the basis is for listing, how the match is confirmed, referral procedures, where evidence supporting the alert record can be found and how decisions are made when a client has a Red status</li> <li>Managing all aspects of the True Match Notification caseload, including consideration of visa cancellation where appropriate.</li> </ul>
Operational owner	s. 47E(d) [REDACTED] manage the listing of Child Custody concerns for foreign citizens.
Role and responsibility of operational owner	The operational owner manages the alert record set for an ARC or ARC/Group. They are responsible for: <ul style="list-style-type: none"> <li>Dealing with requests for clarification of match case referrals</li> <li>Liaising with the information source or sources</li> <li>Providing advice as required regarding alert overrides requests, reviewing alert expiry requests and proposed changes to alert reason code</li> <li>making decisions on minimum data standards and information sources</li> <li>Approval of new alerts where Minimum Data Standards are not strictly met.</li> </ul>
Legislation	Child Protection Acts (applicable in each state, various dates) Div 1.2, Adoption Reg 1.04 – <i>Migration Regulations 1994</i> Schedule 2 criteria – <i>Migration Regulations 1994</i> following visa subclasses: 802, 837, 101, 102, 117, 445

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



Attribute	Description
Relevant Public Interest Criteria (PIC)	<ul style="list-style-type: none"> <li>PIC 4015</li> <li>PIC 4017.</li> </ul>
Policy for reviewing these records	<p>Alert may be reviewed, prior to the child turning 18 years of age, if parental responsibility issues are resolved through:</p> <ul style="list-style-type: none"> <li>a court order from Australia or the child's home country being presented or</li> <li>permission for the visa to be granted is provided by the representative/s with legal/formal parental responsibility (custody) for the child.</li> </ul>
Variable threshold	<p>Amber match at a score of 95 or above.</p> <p>Green at a score of 94 or below.</p>
Contact for further information	<p>Initial enquiries should be directed to the nominated ARC policy owner.</p> <p>Further enquiries can be directed to Border Operations Centre:</p> <p>Email: s. 47E(d)</p> <p>Telephone: s. 22(1)(a)(ii)</p> <p>Fax: s. 22(1)(a)(ii)</p>

### 3.26.2. ARC 26 CMAL system constraints

Field	Description
Family name	<b>Mandatory.</b>
Given name	<b>Mandatory</b> (if known).
Date of birth	Date of birth is <b>mandatory</b> , or, if unknown, year of birth is <b>mandatory</b> (along with country of birth and/or citizenship). No minimum age: maximum age is 18 years.
Other ARCs	s. 47E(d)
Gender/sex	Required.
Country of Birth (COB) and Citizenship	<p>One <b>must</b> be entered.</p> <p><b>Note:</b> Australian citizens not permitted. Can include people whose COB is Australia.</p>
Travel document	Optional.
Informer	<b>Mandatory.</b>
Creation	<p>The Border Operations Centre (BOC) loads INTERPOL notices into CMAL and actions INTERPOL addendum emails on behalf of the ARC owners.</p> <p>This alert will be hidden to CRIF users so that only ARC owners and BOC staff will have the ability to <b>add</b> an ARC 26.</p>
CMAL default review date	<p>No default review date based on age or creation date.</p> <p><b>Note:</b> The default review date can be changed.</p>
CMAL default expiry date	<p>Default expiry at 18 years of age. No default expiry based on create date.</p> <p><b>Note:</b> The default expiry date can be changed.</p>
Business rules	s. 47E(d)

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



Field	Description
Narrative	s. 47E(d)
Information status on Red match	'MAL Status is Red. s. 47E(d) .'
Information status on Amber match	'MAL Status is Amber. Awaiting case assessment, if this case is urgent or the SLA has expired please contact the BOC for more information on s. 22(1)(a)(ii)'
Grounds or authority for expiry of the alert	<ul style="list-style-type: none"> <li>Where the child has reached 18 years of age</li> <li>Removed from INTERPOL holdings.</li> </ul>

### 3.27. Credible Sources

In the majority of cases, Home Affairs staff will source information applicable for the MAL during their normal duties.

**Example:** A visa processing/case officer could become aware of a fraudulently altered document as a part of an application process, while a compliance officer may become aware of a breach of visa condition or an overstayer through performing their normal duties.

If Home Affairs staff become aware of an identity or document of concern from another source outside their normal duties, the staff member must take steps to ensure that the information/evidence has come from a credible source before the identity/document can be considered for inclusion on MAL. Officers should not include records on MAL from unapproved sources.

s. 47E(d)

Alert Reason Code (ARC) policy owners have identified sources that are considered credible for listing identities on MAL under a particular reason code.

**See:** The following for specific sources considered credible:

- Identities:** Alert Reason Codes
- Documents:** Considering Foreign Travel Documents for MAL.

**Contact:** The ARC policy owner for advice if you are unsure whether the source is reputable or the information relevant.

When considering other potential sources, the ARC policy owner must approve a MAL listing (BEFORE it is listed) or source based on information from any of the following:

- newspapers
- non-government websites
- other sources outside normal Home Affairs processes.

Home Affairs is reluctant to source information from any of the above sources, as it is difficult to determine the accuracy, motives and possible bias of the information.

If the ARC policy owner approves the source, this must be stated in the narrative when proposing the alert.

If the informer is credible but the evidence is not available, a proposal for a MAL inclusion can be made on the basis that the informer will follow up with evidence. Identities must **not** be listed on the basis of allegations unless the allegation:

- is from a credible informer
- can be reasonably justified.

### 3.28. Considering Australians for MAL

As a general principle, Australian citizens are not listed on MAL. However, there are circumstances where it is in the national interest to do so and strict policies exist for these situations, only a limited range of ARCs allow Australians to be listed. Australians listed on MAL will alert decision-makers to:

- identify non-citizens suspected of illegally using an Australian identity to travel to and enter Australia
- detect and deal with non-bona fide travellers accompanying the Australian citizen
- assess whether the Australian Citizen's involvement in visa applications for a non-citizen are for genuine reasons.

Australian identities must only be considered for listing on MAL if credible information exists to suggest that they intend to commit or facilitate breaches of the *Migration Act 1958* (Migration Act), or have already been convicted of doing so. Migration Act breaches include:

- immigration fraud
- immigration malpractice
- sponsoring a visa applicant under irregular circumstances
- presenting a badly damaged document that will be impounded on arrival under the *Australian Passport Act 2005*.

**See:**

Credible Sources

Narrative requirements

Checklist – Australian Identity

**See also:**

Considering Australian Documents for MAL

Considering New Zealand Identities for MAL

Considering Foreign National Identities for MAL

Examples of Migration Act breaches, which could cause an Australian citizen to be placed on MAL, include the client:

- acting as an escort or people smuggler
- involvement in fraudulent travel documentation
- being a person who under the *Australian Passports Act 2005*, has been identified as a person potentially being refused a passport if they have lost two in the last five years.

### 3.28.1. Listing Australian Aliases

Aliases are other identities that a person of concern uses. If a person is found to have an Australian alias then it should be determined whether the identity is that of an Australian citizen. When a person becomes an Australian citizen they will generally no longer have a MAL concern.

### 3.28.2. Applicable ARCs and approvals

The table below lists the only ARCs that can be used for listing Australian identities on MAL, along with applicable approvals. The narrative must identify the approval process used by the operational owner of the ARC.

If a Home Affairs decision-maker considers that an Australian identity, including a child, needs to be placed on MAL under an ARC, they must seek approval from the delegate listed in the table below.

ARC approval is an important step in the decision to place an Australian citizen on MAL, as it may be unlawful to detain Australian citizens at the border who were wrongfully placed on MAL. The consequence of this could be very serious, including:

- complaints and claims against the Department
- investigation by oversight bodies
- public loss of confidence in border controls as they apply to our own citizens.

The issues and risks to the citizen and Home Affairs must be balanced against the possible consequences of allowing a person to travel. Appropriate approvals result in some loss of operational flexibility in favour of greater risk control.

See: Alert Reason Codes

ARC	Approval
s. 47E(d)	s. 47E(d)
07 Organised Immigration Malpractice	Director (EL2) of the: <ul style="list-style-type: none"> <li>• s. 47E(d) – for records concerning PSIAT initiatives.</li> </ul>
17 Surrender Australian Travel Document	ABF Officers and Airline Liaison Officers may identify documents of concern while the client is in transit and can propose the identity for MAL inclusion.
22 INTERPOL	s. 47E(d)
23 Identity	EL2 (Director) s. 47E(d), approval is required in writing (to be added to client TRIM file) prior to listing. This is relevant to both the Core Business and Project Chameleon.

### 3.28.3. MAL for new Australian citizens

A MAL alert can trigger for a person who is now recorded as an Australian citizen. If this occurs, the concern must be referred to the policy/operational owner of the Alert Reason Code (ARC) on which the record is based for investigation.

Revocation of Australian citizenship is rare but citizenship can be cancelled under certain circumstances prescribed by law.

See also: Performing MAL checks.

Home Affairs officers have no authority to delay or question Australian citizens in immigration clearance without their consent once the person has satisfied the Home Affairs officer that they are an Australian citizen.

### 3.29. Considering New Zealand Identities for MAL

New Zealand passport holders meeting health and character requirements will be granted a Special Category Visa on arrival in Australia. Any New Zealand citizen with criminal convictions or health concerns will be:

- directed to their nearest Immigration Office if they have not yet departed their country of origin, or
- assessed by the airport officer if they have landed in Australia and indicated on their passenger card that they have a health or character concern.

New Zealand citizens are subject to the same MAL listing criteria as other foreign nationals.

**See:** Considering Foreign National Identities for MAL.

However, in addition, a New Zealand passport holder should be placed on MAL under ARC 09 if:

- They have a criminal conviction
- their BCNC status has been assessed.

The MAL listing can occur regardless of whether or not the person is found to be a BCNC. Listing a passport holder who has been assessed as not BCNC facilitates faster passenger processing at the border.

New Zealand passport holders **must also be listed under ARC 06 if they have health concerns identified or declared on an incoming passenger card.**

**See:**

Alert Reason Code 06

Alert Reason Code 09

Checklist – New Zealand Identity

Section 501: The character test, visa refusal & visa cancellation, Migration Act on LEGEND.

**See also:**

Considering New Zealand documents for MAL

Considering Australian Identities for MAL.

### 3.30. Considering Foreign National Identities for MAL

MAL is intended for listing foreign national identities and documents of concern. The circumstances under which it might be necessary to include a foreign national identity on MAL are defined by the Alert Reason Codes (ARCs) which exist to clearly state the:

- circumstances under which an identity can be listed
- sources that are considered credible for considering information/evidence of a suspect identity.

**See:**

Checklist – Foreign National Identity

Considering Australian Identities for MAL

Considering New Zealand Identities for MAL.

### 3.31. Deceased persons

If a foreign national dies while in Australia and a friend or family member reports the incident to Home Affairs, the identity may be a candidate for inclusion on MAL, if there is a reasonable belief that the identity may be

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



used for fraudulent purposes. In this case, Home Affairs must be provided with a death certificate or other evidence, and the Home Affairs officer should do the following:

- If the client is listed as a MAL identity, propose that the record be expired through the CMAL Remote Input Function (CMAL RIF).
- Propose the relevant travel document(s) for inclusion on MAL.
- Update other Home Affairs systems, such as TRIPS and ICSE, if necessary.

**See:**

MAL identities

Listing documents on MAL.

Deceased people may also be listed on MAL due to MAL not being connected to any Births, Deaths and Marriages databases, and officers failing to update CMAL records. An identity will remain on CMAL where there is a genuine risk of identity theft or fraud.

### 3.32. Considering minors for inclusion on MAL

Minors can be included on MAL if:

- debts to the Commonwealth have been accumulated for minors, irrespective of their responsibility for them
- their legal guardians are listed as overstayer
- there are character concerns related to the minor (either ARC05 or 09) as s501 of the *Migration Act 1958* applies to minors.

Rules regarding the minimum and maximum ages are defined for each ARC as well as rules for review and expiry.

**See:** Alert Reason Codes.


### 3.33. Considering Australian Documents for MAL

As a rule, Australian documents are not listed on MAL. However, there are circumstances where it is in the national interest to do so and strict policies exist for these situations. Australian Document Alert List (DAL) records assist the Department to ensure that foreign nationals of concern are not given access to, or able to use, fraudulently gained travel documents for travel to Australia.

Australian travel documents, including passport numbers, must only be listed on MAL if there is a view or a concern that a particular document may be used improperly.

The following are examples of situations for which placing an Australian document on MAL is appropriate:

s. 47E(d)



There is a checklist of requirements that must be met to consider and subsequently propose an Australian travel document for MAL.

**See:**

Checklist – Australian Travel Documents

Considering New Zealand documents for MAL

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

Considering Foreign Travel Documents for MAL.

**3.33.1. Approval for listing Australian Travel Documents**

Departmental Officers who are considering proposing an Australian travel document on MAL must seek approval from the requesting areas First Assistant Secretary (FAS)/ABF Assistant Commissioner (AC). The FAS/AC should understand the implications of listing the MAL record.

An Australian citizen's travel document placed on MAL can result in the citizen being denied travel from a foreign country back to Australia. The consequence of this could be very serious, including:

- complaints and claims against the Department
- investigation by oversight bodies
- public loss of confidence in border controls as they apply to our own citizens.

A specific DAL Request must be prepared for submission to the FAS/AC, which provides the background information that the FAS/AC will need to decide whether the document should be listed on MAL.

**See:** Example of a DAL Request for FAS/AC Approval

List an Australian document only where necessary. A document listed on MAL triggers check-in systems to prevent a passenger holding that document from boarding a flight or vessel. Australians can only be delayed in immigration processing while their identity is being confirmed. Rather than using DAL, direct reference is made to the Australian Passport database to determine the status of an Australian passport. Australian travel documents lost or stolen in transit should only be listed on MAL as an interim border security measure, pending the update of the passport status in the database.

The Department's systems update the person's entry directive on databases shared with other internal clearance systems.

**See also:** Narrative Requirements

**Important:** Once the person has satisfied the Department officer that they are an Australian citizen, departmental officers have no authority to delay or question Australian citizens in immigration clearance without their consent.

**3.34. Considering New Zealand Travel Documents for MAL**

As a general principle, New Zealand documents should not be listed on the Document Alert List (DAL). However, there are circumstances where it is appropriate to do so.

New Zealand travel documents, must only be listed on DAL with approval from First Assistant Secretary (FAS) and approvals must be obtained on a case-by case basis. No bulk approvals. NZ Travel Documents can be listed if:

- there is a view or a concern that a particular document may be used improperly, or fraudulently to gain travel to Australia
- the New Zealand citizen has significant character concerns. This is to provide the traveller the opportunity to rethink their travel arrangements by giving them advance warning that they may not obtain a visa on arrival to Australia.

While travel cannot be prevented this aims to reduce the number of travellers who will not obtain a visa on arrival and need to be returned to New Zealand. Departmental officers have no authority to prevent travel. Listing a New Zealand travel document on DAL is to ONLY provide the opportunity for the traveller to be advised that:

- they will be assessed on arrival for eligibility for a visa to enter Australia and a visa may or may not be issued.
- it is recommended that the individual consult the Australian embassy to confirm eligibility for a visa prior to travel.

Once this advice has been provided, should the traveller disregard the advice and insist on travelling, BOC should issue an OK TO BOARD.

s. 47E(d)

**See:**

- Checklist – New Zealand Travel Documents
- Considering Australian documents for MAL
- Considering Foreign Travel Documents for MAL

List a New Zealand document only where necessary. A document listed on MAL triggers check-in systems to prevent a passenger holding that document from boarding a flight or vessel. Rather than using DAL, Department systems automatically reference New Zealand Passport data to determine the status of a New Zealand passport. New Zealand travel documents lost or stolen in transit should only be listed on DAL as an interim border security measure, pending the update of the passport status in the database.

Report any lost, stolen or fraudulently altered or obtained New Zealand passports to the New Zealand Department of Internal Affairs (NZIA) via the Border Operations Centre (BOC).

**See also:** Narrative Requirements

### 3.35. Considering Foreign Travel Documents for MAL

A foreign national travel document must be listed on MAL if:

- a reputable source reports it as lost or stolen  
**See:** Credible Sources
- it has been fraudulently obtained or altered (and is still in circulation)
- travel sanction or other travel ban.

ALOs suspect genuineness of travellers. The DAL is temporary and will be deleted once the traveller's intent has been properly assessed and appropriate action taken i.e. traveller assessed as genuine and cleared for travel or traveller assessed as non-genuine and referred to post for visa cancellation consideration. The agreed DAL narrative that must be used for these ALO DALs is:

s. 47E(d)

The DALs should be deleted if ALOs assess as genuine, or remain if ALOs assess as non-genuine. If the ALOs assess as non-genuine and refer to post for cancellation, the DALs should be removed once a decision has been made by the cancellation delegate.

- DAL alert for visa cancellation: If a decision has been made to cancel a visa(s), and the cancellation decision(s) may take some time to record in-system, a DAL record can be created to prevent travel pending the cancellation decision being recorded. The narrative must contain clear advice that cancellation has occurred, and that BOC are authorised to prevent uplift accordingly.
- ETA DAL: An automated DAL alert is uploaded to Central Movement Alert List (CMAL) when a client applies for an ETA online and the client:
  - Ticks 'Yes' for 'Criminal Convictions' and/or;
  - Matches to the RSS (Risk Scoring System);
  - Applies with a travel document that matches a document listed on INTERPOL Stolen/Lost Travel Document (SLTD) database.

There is a checklist of requirements that must be met to consider and subsequently propose a foreign travel document for MAL.

**See:** Checklist – Foreign Travel Documents

The following documents must not be listed:

- Australian or New Zealand issued travel documents, except in specific circumstances
- Documents no longer in circulation
- Driving licences or other non-travel documents
- Visa Labels
- National ID numbers (although they can be listed in the National ID field within the passport listing).

**See also:**

Considering Australian Documents for MAL

Considering New Zealand Documents for MAL

For situations not involved with processing an application, for example, information from other government organisations or agencies, the officer who has read or received this information is responsible for listing the document on MAL. It must not be assumed that someone else in the Department has listed this information.

**See:** Credible Sources

### 3.35.1. Policy and operational owners

Policy and operational owners exist for matters relating to placing foreign travel documents on MAL. The responsible areas and their contact details are listed in the table below.

**Note:** Their specific responsibilities are the same as those of all policy and operational owners.

Further information is available about the roles and responsibilities.

**See:** ARC Roles and Responsibilities.

Role	Who	Email
Policy owner	s. 47E(d)	s. 47E(d)
Operational owner	Border Operations Centre	s. 47E(d)

**Note:** Operational enquiries are directed to the CMAL mailbox while the MAL General mailbox is the established point of contact for external information sources and general enquiries about MAL.

The table below lists sources that are considered credible for the purposes of considering when to place a foreign national document on MAL.

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



Document criteria	Source
Lost or stolen documents	<ul style="list-style-type: none"> <li>• Foreign Government Passport Agencies.</li> <li>• The Department's: <ul style="list-style-type: none"> <li>– post and consular network and contacts</li> <li>– ALO network and contacts</li> </ul> </li> <li>• Police jurisdictions.</li> </ul>
Fraudulently used	s. 47E(d)

### 3.35.2. Listing lost or stolen passports

Visa processing/case officers, relevant Border Security and Airport staff should list a lost or stolen passport on MAL. This is for the benefit of the document holder as well as to prevent the fraudulent use of the document in the future. The client still needs to report their passport as lost or stolen to the issuing authority.

Departmental staff including processing officers should not list a passport on MAL if the:

- caller cannot be identified, or
- the applicant is using the absence of a passport as an excuse for not providing a complete set of documentation for application or identity purposes
- The client does not need a replacement passport in order for the previous passport to be listed on DAL, if the departmental officer is satisfied that the document is lost or stolen.

Staff should consider that some foreign passports are issued with multiple individuals on the same passport and it is possible that the passport maybe in use elsewhere.

### 3.35.3. Counterfeit or suspect documents

Counterfeit documents fall into the category of improperly issued and may include manufactured copies and stolen passport blanks.

### 3.35.4. Fraudulently used or fraudulently altered documents

Fraudulent documents fall into the category of improperly altered or improperly used and may include photo-substitution, and use by a person who is not the original holder.

### 3.35.5. Confiscated by people smugglers and other third parties

It is common for:

- people smugglers to confiscate their clients' travel documents, or
- other third parties to retain a holder's documents against their will.

In these cases, it may not be appropriate to contact the issuing authority but there may be a need to corroborate the information with other international agencies. It is important that these documents are listed on MAL to prevent fraudulent use.

### 3.35.6. Restricting travel

MAL is used to comply with United Nations Travel Sanctions and Autonomous Sanctions. The Migration Act requires that travellers must be properly documented. Advance Passenger Processing (APP) uses MAL to advise airlines of passengers who should not board based on the status of their travel document.

### 3.35.7. Public Interest Criteria (PIC)

There are no links between listing foreign national travel documents on MAL and PIC.

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

### 3.36. Listing identities or documents on MAL- narrative requirements

A narrative must be included in all proposals for listing an identity or document on MAL. Narratives explain important aspects of the listing, s. 47E(d)


s. 47E(d)



See: [Checklists](#)

#### 3.36.1. Catering to the audience

s. 47E(d)




#### 3.36.2. Using minimal acronyms

Unlike HMAL, which restricted narrative text, the CMAL narrative box has a considerably larger capacity. Therefore, officers creating and updating narratives are requested to:


- write narratives in plain language
- use minimal abbreviations and acronyms.

#### 3.36.3. Required data

s. 47E(d)

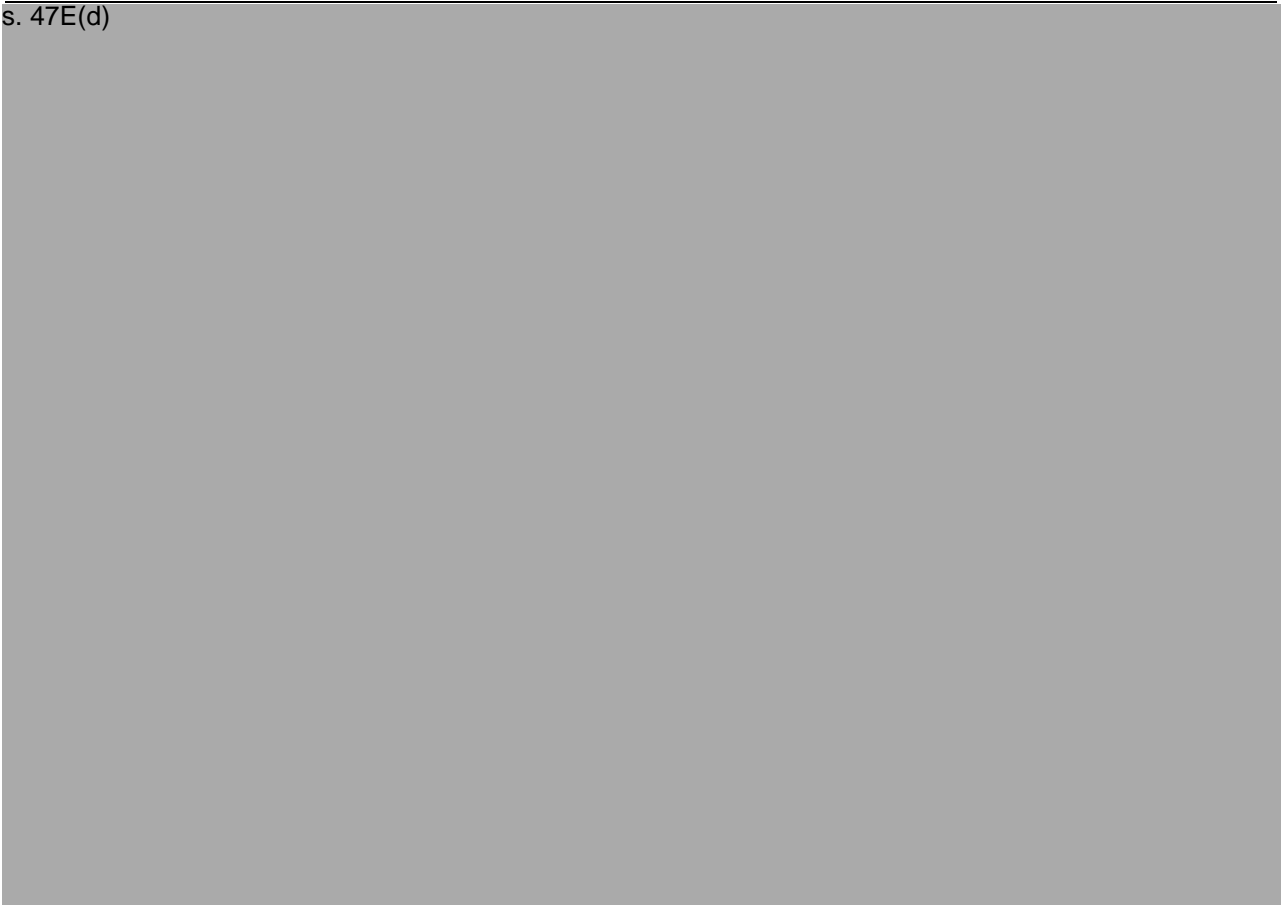


s. 47E(d)



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

s. 47E(d)



### 3.36.4. Narratives for Australian citizens

As well as the above narrative information, specific additional narrative text must be included for Australian citizens placed on MAL.


The following narrative must be included for all Australian citizens who are placed on MAL:

s. 47E(d)



There are no powers under the *Migration Act 1958* that allow Home Affairs officers to detain and question Australian citizens in immigration clearance once a person has satisfied an inspector that they are an Australian citizen. The act of doing so unlawfully places the citizen in 'immigration detention'. Therefore, when placing an Australian citizen on MAL this issue needs to be clearly articulated in the narrative to ensure no Home Affairs officer unlawfully detains an Australian citizen.

s. 47E(d)



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

**3.36.6. A good example of a narrative text**

The text below is an example of a good narrative listed under ARC 07 Organised immigration malpractice. It contains all of the essential narrative elements to help decision-makers determine the appropriate action in the case of an alert. The:

- first component describes the context and background
- second component advises the action to take and who needs to know.

s. 47E(d)

**3.37. Proposing identities for MAL inclusion**

Once it is determined that an identity meets the requirements for inclusion on MAL, a proposal must be created and submitted to the ARC owners for review, before the identity is added to MAL. It is important that the information entered into the proposal:

- is as complete, accurate, timely and up to date as possible
- meets the requirements for the Alert Reason Code (ARC) on which the identity inclusion is based.

**See:**

Considering Australian Identities for MAL

Considering New Zealand Identities for MAL

Considering Foreign National Identities for MAL

Alert Reason Codes (ARCs)

Checklist – Australian Identity

Checklist – New Zealand Identity

Checklist – Foreign National Identity

It is integral for MAL checking that:

- the client's bio-data is accurate, current and complete
- there is a single record for the client only, not duplicate records.

Duplicate records and poor bio-data:

- devalues the integrity of MAL
- places an additional unnecessary workload on the BOC
- impacts Home Affairs client and other internal Service Level Agreements (SLAs)
- reflects negatively in reporting tools.

To ensure quality bio-data and prevent duplicate records, officers should do the following when entering data into the various visa processing systems:

- ensure that the client does not already exist in the system
- use the bio-data exactly as recorded in the client's travel documents.

The relevant ARC owners perform ongoing quality checks and reviews to improve MAL data quality.

If the officer proposing an identity for MAL inclusion genuinely only knows the identity's year of birth, the correct way of loading this information into CMAL is not to enter day and month field.

**Example:** 1977.

**Note:**

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




- Do not guess the date of birth as this will affect how this record is potentially matched with other MAL records. Do not enter the date of birth as 01/01/1977
- The CMAL system is designed to accept blanks if the day and month are unknown
- The minimum data standards still apply for the relevant ARCs. Therefore, if an ARC's minimum data standards require a full date of birth, the CMAL system may not allow the proposed record to be created. Exception management rules apply.

**Contact:** The BOC to discuss further if required.

### 3.37.1. Minimum data required

Each ARC contains business rules and minimum data that must be adhered to when proposing an identity for inclusion on MAL. Officers proposing an identity for MAL should seek and include as many accurate pieces of relevant biographic information about the identity as possible, exceeding the minimum data standards for that particular alert code.

s. 47E(d)



### 3.37.2. Supporting documentation

Depending on the nature and classification of correspondence, all information relating to a document's listing on MAL should be filed:

- in TRIM either electronically or on a paper file, or
- on another database.

**Examples:** INTERPOL notices are held on the INTERPOL network, Australia's autonomous sanctions are held on the s. 47E(d) website, health clearances are recorded in the HATS system, and debts to the Commonwealth are maintained in SAP.

### 3.37.3. Listing aliases on MAL

Aliases are other identities that an identity of concern is also known as having used. An alias record should be created if:

- an officer is aware there is an alternate identity that a person has used or is likely to use, or
- the source material for the record does not clearly differentiate between the family name and the given name.

An alias must not be listed without a birth date. If the alias birth date is unknown, the date of birth of the primary identity must be used with a comment in the narrative advising that the birth date of the alias is unknown.

s. 47E(d)

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

- different dates of birth
- different nationalities
- variations in the spelling of names, names joined, split or hyphenated
- name written in a different word order
- different combinations of parts of their name
- different names and commonly accepted abbreviations.

**Example:** Terry for Terrance, Abdul for Abdullah, Bill for William, Chris for Christine.

**Note:** Although these are linguistically equivalent, visa processing system policy requires that these names be listed as aliases.

Aliases do not include nicknames. Nicknames must not be placed on MAL.

### 3.38. Listing Documents on MAL

Most travel documents on MAL are bulk loaded from passport issuing or law enforcement agency sources. Information from these and other sources is received through the CMAL mailbox.

Once it is determined that a travel document meets the requirements for inclusion on MAL, a proposal must be submitted to the Border Operations Centre (BOC) for review before the document can be added to MAL.

**See:** The following for checklists of requirements that must be met before listing a document on MAL:

[Checklist – Australian Travel Documents](#)

[Checklist – New Zealand Travel Documents](#)

[Checklist – Foreign Travel Documents](#)

**See also:** [Considering Australian documents for MAL](#)

#### 3.38.1. Automatic document listing on MAL

Airport Officers and Airline Liaison Officers may identify clients who are travelling on a document other than that for which the visa was issued. This is most commonly identified because a document has been lost, stolen or expired since the visa was issued.

**Important:** The officer who has identified the old passport must end date it in the visa processing system.

#### 3.38.2. Required data

An alert against a document on MAL will prevent the passenger boarding a flight through Advance Passenger Processing (APP). Therefore, it is important that the document's information on MAL is complete and accurate.

**Note:** Documents listed on the INTERPOL Stolen Lost Travel Documents database will also prevent a passenger boarding a flight. Airline check-in staff will receive a 'Contact BOC' message via the APP system and unless resolved the passenger will not be able to board.

To ensure that document records contain enough information for Home Affairs decision-makers, there is a minimum data set that every document record must contain. However, it is preferable that as much information be completed as possible to ensure efficient matching and to support decision-makers.

Home Affairs officers who handle travel documents should have a broad understanding of the information contained in the passport and should be familiar with the principles of issue for ICAO standard (machine readable) and non-ICAO (often hand written or manual issue). Home Affairs officers must be able to make a distinction between the various document types that can be presented in the application process.

The table below lists mandatory data that must be included, as well as other data that should also be completed if possible.

Data	Mandatory	Description
Document type	Yes	<p>Examples include:</p> <ul style="list-style-type: none"> <li>• Passport</li> <li>• Titre De Voyage</li> <li>• Document of Identity</li> <li>• Certificate of Identity</li> <li>• Document for Travel to Australia/Immcard</li> <li>• Other.</li> </ul> <p>Do not list:</p> <ul style="list-style-type: none"> <li>• Visa labels</li> </ul> <p>Documents that are not used for travel to Australia.  <b>Example:</b> Schengen documents, driving licences and miscellaneous proof of identity, national identity cards (these can be listed in the national ID section within the document section).</p>
Document ID	Yes	<p>The number identifying the travel document. This is the document number that appears in both the machine readable and visible zones of the passport. It is not necessarily the booklet number, which may be punched through the document.</p>
Nationality of holder	Yes	<p>This field is the code for the Nationality in the Visible Zone and is shown in the second line of the passport Machine Readable Zone (MRZ).</p> <p>For documents that do not meet ICAO standards such as documents that are hand written, temporary or emergency travel documents this can be found in the identification page.</p> <p><b>See:</b> The following for policy on listing Australian and New Zealand documents:  <u>Considering Australian Documents for MAL</u>  <u>Considering New Zealand Documents for MAL</u></p>
Country of issue	Desirable	<p>Country of Issue of the document is the Country Code of Issuing State usually at the top of the visible zone and is shown in the First line of the MRZ. It can be used to validate the Document Number Format.</p> <p>This field is not to be confused with the Authority, Issuing Authority or Place of Issue Field.</p> <p>Australian Country of Birth (COB) acceptable; entry of Australian citizens is not approved.</p>
Name of the original holder	Desirable	<p>Knowing the details of the original holder will avoid confusion if the document is detected and will make the distinction between a notification error and a stolen document.</p>
Date of birth of original holder	Desirable	<p>As above.</p>
Gender	Desirable	<p>As above.</p>
Informer	Mandatory (for bulk loads)	<p>This is the source from which the information about the document(s) came.</p> <p><b>Important:</b> A document listing for a passport reported as lost or stolen <b>must</b> contain an informer code to advise the information source. If appropriate a file reference should also be included.</p> <p>Information on <u>credible sources</u> is available.</p> <p><b>See:</b>  <u>Considering foreign national documents for MAL</u></p>

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

Data	Mandatory	Description
Expiry	Yes	Default expiry rules exist for documents placed on MAL. However, if an expiry date is manually entered, this overrides the system defaults. More information is available. s. 47E(d)

s. 47E(d)

s. 47E(d)

### 3.38.5. Supporting documentation

Depending on the nature and classification of correspondence, all information relating to a document's listing on MAL should be filed:

- in TRIM either electronically or on a paper file, or
- on another database.

**Examples:** INTERPOL notices are held on the INTERPOL network, Australia's autonomous sanctions are held on the s. 47E(d) website, health clearances are recorded in the HATS system, and debts to the Commonwealth are maintained in SAP.

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



### 3.39. Reviewing and Updating MAL Identities and Documents

A large number of identities and documents exist on MAL. Each time a MAL check is initiated the client's biodata and travel document is checked against the records contained in the PAL and DAL. Therefore, it is imperative that the alerts are up to date and regularly reviewed, and if necessary expired, otherwise the integrity of MAL is compromised. Out of date or redundant records on MAL can result in invalid potential matches, clients being inconvenienced at the border causing frustration for both clients and Home Affairs decision makers.

s. 47E(d)

s. 47E(d)

s. 47E(d)

#### 3.39.2. Automatic review dates for identities (PALs)

Alert Reason Code (ARC) policy owners specify review dates for each ARC that they own. The CMAL system automatically:

- sets a review date for each MAL-listed identity based on the ARC under which it is listed
- prompts the ARC operational owner to review the identity record when it is due.

**Example:** An identity listed under ARC 19 Illegal fishers will automatically trigger a review five years after the identity was listed on MAL.

s. 47E(d)

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

s. 47E(d)



#### 3.39.4. Visa/citizenship grant or refusal

It is important to update the record in conjunction with a visa grant or refusal if a potential match has been assessed as a true match.

**Note:** The MAL record does need updating if the potential match is determined to be a **true match**, irrespective of whether the application is refused or granted.

If the visa application has been:

- refused, update the record with the refusal, including the reason, or
  - granted, update the record with:
    - the grant details
    - recommendation as to whether the identity should remain on MAL.
- Note:** If the record should not remain, a request to expire the record should be raised.
- See:** How to update or expire a record.

s. 47E(d)



#### 3.39.6. Reviewing Australian identities on MAL

All Australian citizen MAL records must be reviewed at least once every 12 months to ensure the reasons for listing are still current and relevant.

The s. 47E(d) are responsible for reviewing all records listed under:

- ARC 07 Organised Immigration Malpractice.

ARC Owner, in consultation with the operational owner, is responsible for reviewing all other Australian identity records.

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

### 3.39.7. Reviewing Australian documents on MAL

The ARC Owner regularly checks <sup>s. 47E(d)</sup> systems to determine if they reflect Australian documents listed on MAL as void or cancelled. If so, the ARC Owner will remove the listing from MAL if appropriate.

**Note:** Reviews do not apply to foreign national travel documents. Instead, the CMAL system automatically expires these records after a defined time:

s. 47E(d)

s. 47E(d)

A large number of identities and documents exist on MAL. Each time a MAL check is initiated the client's biodata and travel document are checked against the records contained in the PAL and DAL. Therefore, to maintain the operational integrity of MAL, it is imperative that redundant records are removed.

Out of date or redundant records on MAL can result in invalid potential matches and clients being inconvenienced and delayed at the border causing frustration for both clients and Home Affairs decision makers.

**See:** Reviewing and updating MAL identities and documents.

s. 47E(d)

### 3.40.2. Automatic identity and document expiry

#### Identities

If it is possible, ARC policy and operational owners set automatic expiry dates for identities placed on MAL.

s. 47E(d)

s. 47E(d)

#### Documents

All documents placed on MAL automatically expire at different times depending on whether the document expiry date is known. If the document expiry date is:

- known, the document will expire two years from the document expiry date, or
- not known, the document will expire ten years from the date the document was placed on MAL.

**Note:** This is in line with the maximum passport issuance period.

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



### 3.40.3. When to manually expire a MAL identity or document

#### Clients granted citizenship

As a general principle Australian citizens are not listed on MAL. Similarly, if a non-citizen listed on MAL is subsequently approved for Australian citizenship, then as a general rule the MAL record should be considered for deletion.

Before deleting any MAL record, you should ensure that the deletion is consistent with the 'grounds or authority for expiry of the alert'. This information is provided under the 'system constraints' listed against each ARC.

#### Foreign travel documents

A foreign travel document may be expired if compelling evidence is received that the document has been returned to its rightful owner. If the evidence was originally received from a reliable source the decision maker should contact the informer, especially if the narrative stipulates to do so, or if the alert contains a file number.

**Note:** This does not apply to Australian or New Zealand travel documents.

**See also:** Re-listing a found passport on MAL.

### 3.40.4. Void Australian and New Zealand travel documents

In the exception circumstance that an Australian or New Zealand travel document is placed on MAL, the void travel document must be expired as soon as possible to prevent MAL checks against a document that no longer exists.

### 3.40.5 Invalid records

Identities and documents on MAL should be expired when they are no longer valid/required.

**Example:** Risk factors may no longer apply and debts have been repaid in full, and no other section or agency has expressed ongoing interest in the record or identity.

### 3.40.6. Re-listing a found passport on MAL

Occasionally a client who has previously advised they have had their passport lost or stolen later contacts Home Affairs to advise they have found the same passport.

There is very little point reinstating a travel document in these cases as the **Foreign Passports Act considers the document to be void and not to be reinstated** (even if found). It cannot be used again and the document holder is required to apply for a new travel document. The client may hold the found passport but it may not be valid for travel. Staff must be mindful that because a client can prove they 'have the found document in their possession', does not mean the document is valid for travel.

However, if the Home Affairs officer is convinced the document has **only** been reported to Home Affairs, and not the foreign issuing authority, the document can be successfully expired from MAL. However before this is requested, the Home Affairs officer must:

- satisfy themselves that the passport was never reported to the issuing authority as a lost or stolen travel document
- satisfy themselves that the document was only misplaced by the holder and has not in the meantime been used fraudulently
- request the client to provide a scanned copy of the passport in question, or sight the document in question themselves.

### 3.40.7. What happens to expired records?

All expired records, whether automatically or manually expired, are removed from MAL and placed in an archive. Only staff with specific CMAL access are able to view archived records.

### 3.41. ARC Owner Change Form

#### 3.41.1. ARC Owner Transfer

Following a restructure of business lines, ARC owners could find they have a cohort of record holdings under their ARC which no longer fits within their area of responsibility. This may require the transfer of ARC holdings to another owner.

Where there are any alerts under an ARC that may belong elsewhere due to a change in reporting lines and to ensure these will be managed during any interim period, the existing ARC owner will retain responsibility for them. The existing alerts still need to be managed, until they are expired, deleted, or amended to place them under a different ARC (this update has to be done manually to each individual alert as arranged by the ARC owner).

When an ARC is moved to a new policy owner or has significantly changed, the Superintendent (EL2), ABF Operations Systems Management Section must be notified using the form below and **email:**

s. 47E(d)

#### 3.41.2. ARC Creation/Change to Business rules

The new owner may request a new ARC be created, or identify an existing ARC where they can direct future alerts, depending on their specific business needs. The new owner may also choose to redefine the policy and business rules for future listings under the current ARC.

**Note:**

The Policy Owner, in conjunction with the BOC, defines:

- the policy and rules for the record set
- credible data sources
- the legislative basis for the alert (if applicable)
- how the match is confirmed
- referral procedures
- where evidence supporting the record can be located
- processes for a Red status
- the match case threshold score
- minimum data standards for the ARC.

They identify the Operational Owner who has responsibility for managing the MAL records for an ARC or ARC group. They also attend the ARC Owners Consultative Forum (ARCOCF) on a monthly basis. The ARCOCF reinforces ARC owners' responsibility for data quality and end to end alert management. These meetings are held bi-monthly and are aimed at fostering relations and sharing information about CMAL functionality, to improve ARC owners' understanding of their responsibilities and their accountability for data quality of their alert listings.

The Operational Owner:

- manages a set of records within an ARC or ARC group
- holds the evidence for each record listing
- deals with requests to clarify match case referrals
- liaises with the information source(s)
- maintains the accuracy and currency of the MAL records
- reviews the new alerts being created by the CMAL users.

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

Details	Description
ARC Number and Name:	
Current ARC Business Owner (MUST include Division/Branch/Section):	
Contact Officer and Phone Number:	
New ARC Business Owner (MUST include Division/Branch/Section):	
Contact Officer/Representative and Phone Number <i>Note:</i> There is a maximum of two representatives per ARC. Representative/s should be between the EL1 and AS level.):	
Commencement of change date:	
Evidence of agreement to transfer ARC (for example, TRIM location for sign-off document agreeing to new ownership):	

***New ARC Business Owner*** – Please update the below tables on ARC Policy and system parameters (if unchanged, copy the information from the previous ARC listing).

### New Policy Information

Attribute	Description
Risk category	
Classification	
Who should be listed	
Source of information	
Groups	
Policy owner	
Role and responsibility of policy owner	
Operational owner	
Role and responsibility of operational owner	
Legislation	
Relevant Public Interest Criteria (PIC)	

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

Attribute	Description
Policy for reviewing these records	
Variable threshold	
Contact for further information	

### New Systems Constraints

Field	Description
Family name	
Given name	
Date of birth	
Other ARCs	
Gender/sex	
Country of Birth (COB) and Citizenship	
Travel document	
Informer	
Creation	
CMAL default review date	
CMAL default expiry date	
Business rules	
Narrative	
Information status on Red match	
Information status on Amber match	
Grounds or authority for expiry of the alert	

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



### 3.41.3. Deletion of an ARC

An ARC owner may consider deleting an ARC. However, the need to delete an ARC is considered to be a rare event, given that the reasons why an ARC was initially created are unlikely to change. However, a need may arise to close down an ARC, such as if the reason for the ARC no longer exists due to a legislative change.

With current system functionality, an ARC category can only be deleted if no alerts remain under the ARC (i.e. they are all expired, deleted, or transferred to another ARC). It may take time to manage any residual alerts until such time as the ARC is empty and can be deleted. Therefore, if a decision to close down an ARC category is made, there may be an option to close the ARC off to receiving any new alerts. The existing alerts can then be managed by the ARC owner without any new alerts being added. This option may become available following a system upgrade request.

If an ARC category was to be closed down, the responsibility for any residual alerts will remain with the ARC owner until such time as there are no remaining alerts. This governance framework is required to ensure the operational effectiveness of CMAL is maintained.

If the closure of an ARC category is being sought, send the below to the Central MAL mailbox and the Superintendent (EL2) ABF Operations Systems Management Section with detail of how the residual alerts will continue to be managed.

Email: s. 47E(d)

Details	Description
ARC Name and Number:	
Current Owner:	
Contact Name and Phone Number:	
Reason for request for deletion:	
Number of alerts remaining: <u>Note:</u> The responsibility for any residual alerts will remain with the ARC owner, until there are no remaining alerts.	
Details of how the remaining alerts will be managed:	
Requested deletion date: (ABF Operations Systems Management approval pending)	

**For ABF Operations Systems Management use only:**

Action	Date
Procedural Instruction updated:	
ARCOCF notified:	
ABF Operations Systems Management: Noted/Approved	
System changed:	

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

## 4. Accountabilities and Responsibilities

### 4.1 Policy owner responsibilities

The content in this document (and related procedural instructions/support material) will be reviewed by the s. 47E(d) :

- every 12 months, or
- as required to respond to significant changes to the business, policy, legislation or systems environments.

ARC Owners must ensure that:

- the policy parameters, thresholds for matching and business line contacts for internal ARC enquiries are kept up to date for their ARC portfolio
- the sources of data used for matching minimum data standards are consistent and reliable
- representatives from all ARCs are to attend critical forums on CMAL matters, such as the ARC Owners Consultative Forum
- all information regarding individual ARCs and contact procedures in this Procedural Instruction are up to date and correct. ARC owners are to advise ABF Operations Systems Management and the BOC in writing of any changes to their ARC business requirements as soon as it is known. This includes, but is not limited to, advising of any changes in policy parameters, system constraints, business ownership and contact details for responsible ARCs
- PAL updates, additions and expiries are reviewed within required timeframes.

### 4.2. User and stakeholder responsibilities

Users of this Procedural Instruction must ensure that:

- advice in these instructions is followed; and
- any exceptions to these instructions is cleared via relevant policy and support areas (such as the BOC, ABF Operations Systems Management or the ARC owner).

### 4.3. Records Management responsibilities

- All records created as a result of this Procedural Instruction must be managed in accordance with the Records Management Policy Statement.
- Records created as a result of this Procedural Instruction must be saved in TRIM RM8.

## 5. Version Control

Version number	Date of issue	Author(s)	Brief description of change
0.1	01/03/2017	s. 22(1)(a)(ii)	Initial draft
0.2	28/03/2017		Edits and formatting
0.3	30/03/2017		EL2 Approval of initial content
0.4	30/06/2017		Revision of changes from ARC owners and Governance & Evaluation

Version number	Date of issue	Author(s)	Brief description of change
0.5	25/08/2017	s. 22(1)(a)(ii)	Additional format edits
0.6	10/11/2017		Final edits from stakeholder feedback
0.7	02/08/2018		Minor edits on content
0.8	26/11/2018		Revision of entire content from ARC owners and edits
0.9	18/02/2019		Change in template
1.0	31/07/2019		Edits from ARC 20, 22 and Traveller policy
1.1	22/01/2020		Edits on NZ DAL from Traveller Policy and Legal approval
1.2	27/07/2020		Minor edits on formatting and content
1.3	19/08/2020		Minor edits on formatting and content
1.4	25/05/2021		Minor edits for s. 47E(d)
1.5	16/06/2021		Inclusion of Biometrics Capability and minor edits on formatting and content
1.6	28/07/2021		Minor edits to ARC 20 and ARC 08
1.7	10/08/2021		Minor edits to ARC 06

## Attachment A – Definitions

Term	Acronym (if applicable)	Definition
ABF Operations Systems Management	AOSM	Section within Operational Strategies branch that provides support and training for many departmental systems.
Airline Liaison Officer	ALO	An ABF officer who is stationed at major airports to aid in the event of issues with travellers to Australia.
Advance Passenger Processing	APP	A two-way interface between the airline's departure control system and Department of Home Affairs (Home Affairs) databases –checks for authority to travel prior to boarding flight to Australia.
Alert Reason Code	ARC	Codes assigned to identities listed on MAL recording why a person is listed, as well as potential level of risk to the community.
ARC Owner		Business area(s) responsible for the setting of alert matching and policy thresholds for specific individual ARCs, as well as reviewing alerts as they are placed on CMAL.
ARC Owner's Consultative Forum	ARCOCF	A consultative forum consisting of representation from the key business areas responsible for the administration of Alert Reason Codes (ARCs) and management of Centralised Movement Alert List (CMAL) records. ARC owners are required to participate in this forum.
Behaviour Concern Non-Citizen	BCNC	Part of the assessment criteria for determining whether a New Zealand citizen is eligible for a Special Category Visa. Two criteria that would determine a client to be BCNC is if they have been sentenced to more than 12 months cumulative imprisonment, or deported from Australia or another country.
Biometric Person Indicator	BPI	A unique identifier representing a client's biometric identity.
Border Operations Centre	BOC	The BOC provides functions for CMAL, Seaports Referrals as well as facilitating the movements of people across the border by air and sea.
Border Security Portal	BSP	Provides access to consolidated information from another of systems for those staff involved in day-to-day border security work.
Central Movement Alert List	CMAL	The border IT system used to store, maintain and interrogate the central repository of MAL identities and documents of concern.
Client Data Hub	CDH	The Client Data Hub is the Department's consolidated client data repository. It consolidates data from various departmental systems including ICSE, IRIS, ISR and TRIPS.
Client Search Portal	CSP	Department of Home Affairs (Home Affairs) major client search tool. CSP enables users to perform some business activities and client transactions.
Document Alert List	DAL	Records on lost, stolen, cancelled, counterfeit, fraudulently altered or otherwise suspect foreign government passports and other travel documents.

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



Term	Acronym (if applicable)	Definition
Health Alert Tracking System	HATS	Supports Health Services to perform health assessments.
Heritage MAL	HMAL	The Department's legacy system that was used to check MAL before the CMAL system deployment.
International Civil Aviation Organisation	ICAO	A UN specialised agency, which codifies the principles and techniques of international air navigation and fosters the planning and development of international air transport to ensure safe and orderly growth.
Integrated Client Search Environment	ICSE	Records all of the steps involved in visa and citizenship processing. Primarily used for onshore processing. Interacts with TRIPS and ISR to view all relevant client information.
Immigration Records Information System	IRIS	A mainframe system used to record and support the decision making process for visa applications made offshore for entry into Australia.
Identity Services Repository	ISR	Provides a single data store for personal identity information. This includes biographical information, photographs and travel document details
Locally Engaged Employee	LEE	A locally engaged employee usually employed at Department of Home Affairs (Home Affairs) offshore posts involved in client service, visa processing and administrative duties.
Movement Alert List	MAL	A computer database containing electronic records of identities and travel documents of concern.
Medical Officer of the Commonwealth	MOC	A medical practitioner appointed by the Minister in writing to be the Medical Officer of the Commonwealth.
Machine Readable Zone	MRZ	The section of a passport that make it easier for automated checking systems to scan a travel document. It is usually at the bottom of the passport. It enables faster and more accurate processing as well as faster data matching against immigration databases.
Person Alert List	PAL	These are identities of concern to the Australian community for national security, character and health reasons.
Public Interest Criteria	PIC	A legislative tool that is often the basis for granting or refusing visa applications, or refusing entry into Australia.
Security Referral Service	SRS	A secure portal that allows the electronic transfer of security referrals and information requests between Department of Home Affairs (Home Affairs), s. 47E(d)
Travel and Immigration Processing System	TRIPS	A broad group of mainframe systems that form Department of Home Affairs (Home Affairs) main computerised border clearance processing. Includes Movement Records, Visas, Australian and New Zealand passport databases.
Visa Processing Officer	VPO	Department of Home Affairs (Home Affairs) officer responsible for the assessing and granting of visa applications.
Visual Inspection Zone	VIZ	The page of a passport with the personal details that include the passport holder's name, passport number, passport

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

Term	Acronym (if applicable)	Definition
		country and passport issue and expiry dates. A photograph of the passport holder usually accompanies it.

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

## Attachment B – Assurance and Control Matrix

### Powers and Obligations

Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	Reference (for example, section)	Provision		
Migration Act 1958	s36, s60, s65, s109, s116, s128, s200, s496 s501(1),(2)&(3A)	Covers the immigration decision process, including: Protection visas Delegations. Medical examination, Grant or refuse to grant visa Cancellation of visa if information is incorrect Power to cancel Cancellation of visas of people outside Australia Deportation of certain non-citizens Refusal or cancellation of visa on character grounds	Yes	LIN 19/033- Citizenship and Social Cohesion Group and Immigration and Settlement Services Group (Minister) Instrument 2019  DEL 17/088 – Migration (minister) (examination, Search and Detention) Delegation and Authorisation 2017  LIN 19/283 - Australian Border Force (Minister) Delegations and Authorisations 2018 (ABF (M) No. 1 of 2018)
Migration Regulations 1994	r1.04, Schedule 2 ( Visas), Schedule 4 (Public Interest Criteria), Schedule 5 (Special Return Criteria)	Covers the definitions of Visa subclasses, Public Interest Criteria, Special Return Criteria, Adoption and other miscellaneous definitions	Yes	LIN 19/283 Australian Border Force (Minister) Delegations and Authorisations 2018 (ABF (M) No. 1 of 2018)  LIN 19/033- Citizenship and Social Cohesion Group and Immigration and Settlement Services Group

Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	Reference (for example, section)	Provision		(Minister) Instrument 2019
<i>Australian Citizenship Act 2007</i>	Section 4, 13, 20	Covers all aspects of Citizenship including: <ul style="list-style-type: none"> <li>acquiring Australian Citizenship</li> <li>Australian Citizenship rights and responsibilities</li> <li>conferral process</li> <li>application and eligibility of Citizenship.</li> </ul> <b>Important:</b> Home Affairs has very limited legislative basis for placing Australian identities or documents on MAL.	No	NA
	Section 45	Bogus documents and provision to retain them	Yes	MHA No. 2 of 2018- Minister – Delegations and Authorisations Instrument No. 2 of 2018 (Policy Group)
<i>Children and Young People Act 2008 (ACT)</i> <i>Children and Young Persons (Care and Protection) Act 1998 (NSW)</i> <i>Care and Protection of Children Act 2007 (NT)</i> <i>Child Protection Act 1999 (Qld)</i> <i>Children's Protection Act 1993 (SA)</i> <i>Children, Young Persons and their Families Act 1997 (Tas)</i> <i>Children, Youth and Families Act 2005 (Vic)</i>	NA	Every state has its own legislation for the support, care and protection of children and young persons. The Home Affairs responsibility ensures that foreign children at risk are not granted a visa against the will of the person who has legal responsibility for them.	No	NA

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



Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	Reference (for example, section)	Provision		
<i>Children and Community Services Act 2004 (WA)</i>				
<i>Criminal Code Act 1995</i>	s121,s122,s123	Covers the <u>secrecy of information</u> by Commonwealth officer	No	NA
	Chapter 8 – (s268 – s279)	Covers the treatment of individuals under conditions of war. Under the Human Rights Abuses and War Crimes Act, alleged perpetrators are held accountable. Home Affairs is required to exercise universal jurisdictions of recognised subjects. Offences against humanity and related offences	No	NA
<i>Australian Passports Act 2005</i>	Section 23	Covers the powers of officers regarding confiscation of a passport under suspicion of falsification or false pretences, improper use or damage/tampering. Home Affairs facilitates surrender procedures	No	NA
<i>Australian Passports Act 2005</i>	S22A (2) of the passport act	Deals with the suspension of Australian passports and with the retention of Australians on CMAL after citizenship is granted.	No	NA

## Controls and Assurance

Related Policy	Nil
Procedures / Supporting Materials	Nil
Training/Certification or Accreditation	eLearning - Introduction to CMAL RIF Face to face training – CMAL Overview
Other required job role requirements	Nil

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


Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	Any queries regarding the procedures, please email ABF Operations Systems Management team at s. 47E(d)
Escalation arrangements	System related issues can be escalated to s. 47E(d)
Recordkeeping (e.g. system based facilities to record decisions)	TRIM Documents on Migration, Citizenship and Customs Legislation can be viewed via LEGEND.
Program or Framework (i.e. overarching Policy Framework or Business Program)	Nil
Job Vocational Framework Role	<ul style="list-style-type: none"> <li>• Administration</li> <li>• Compliance and Regulation</li> <li>• Compliance and Regulation</li> <li>• Data and Analytics</li> <li>• Development Program</li> <li>• Development Program</li> <li>• Forensics</li> <li>• Information and Communications Technology (ICT)</li> <li>• Intelligence</li> <li>• Program Delivery</li> <li>• Program Delivery Support</li> <li>• Project and Program</li> <li>• Research</li> <li>• Strategic Policy</li> </ul>

s. 47E(d)


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

## Appendix – CMAL Supporting Material


s. 47E(d)

A large rectangular area of the document is redacted with a solid grey fill.

s. 47E(d)

A large rectangular area of the document is redacted with a solid grey fill.

s. 47E(d)

A rectangular area of the document is redacted with a solid grey fill.

s. 47E(d)


A large rectangular area of the document is redacted with a solid grey fill.

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


s. 47E(d)

A large rectangular area of the document is redacted with a solid grey fill.

s. 47E(d)

A large rectangular area of the document is redacted with a solid grey fill.

s. 47E(d)

A horizontal rectangular area of the document is redacted with a solid grey fill.

s. 47E(d)

A large rectangular area of the document is redacted with a solid grey fill.


s. 47E(d)

A rectangular area of the document is redacted with a solid grey fill.


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



s. 47E(d)




s. 47E(d)




s. 47E(d)



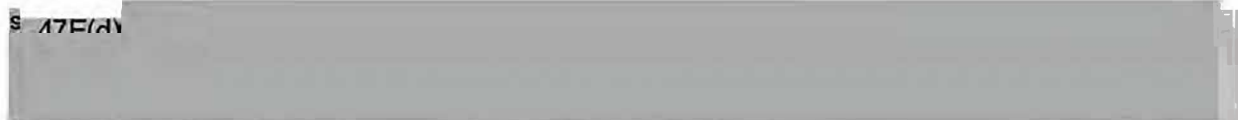
s. 47E(d)



s. 47E(d)




s. 47E(d)



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


s. 47E(d)




s. 47E(d)



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)



s. 47E(d)



s. 47E(d)




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)



s. 47E(d)



s. 47E(d)



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



s. 47E(d)

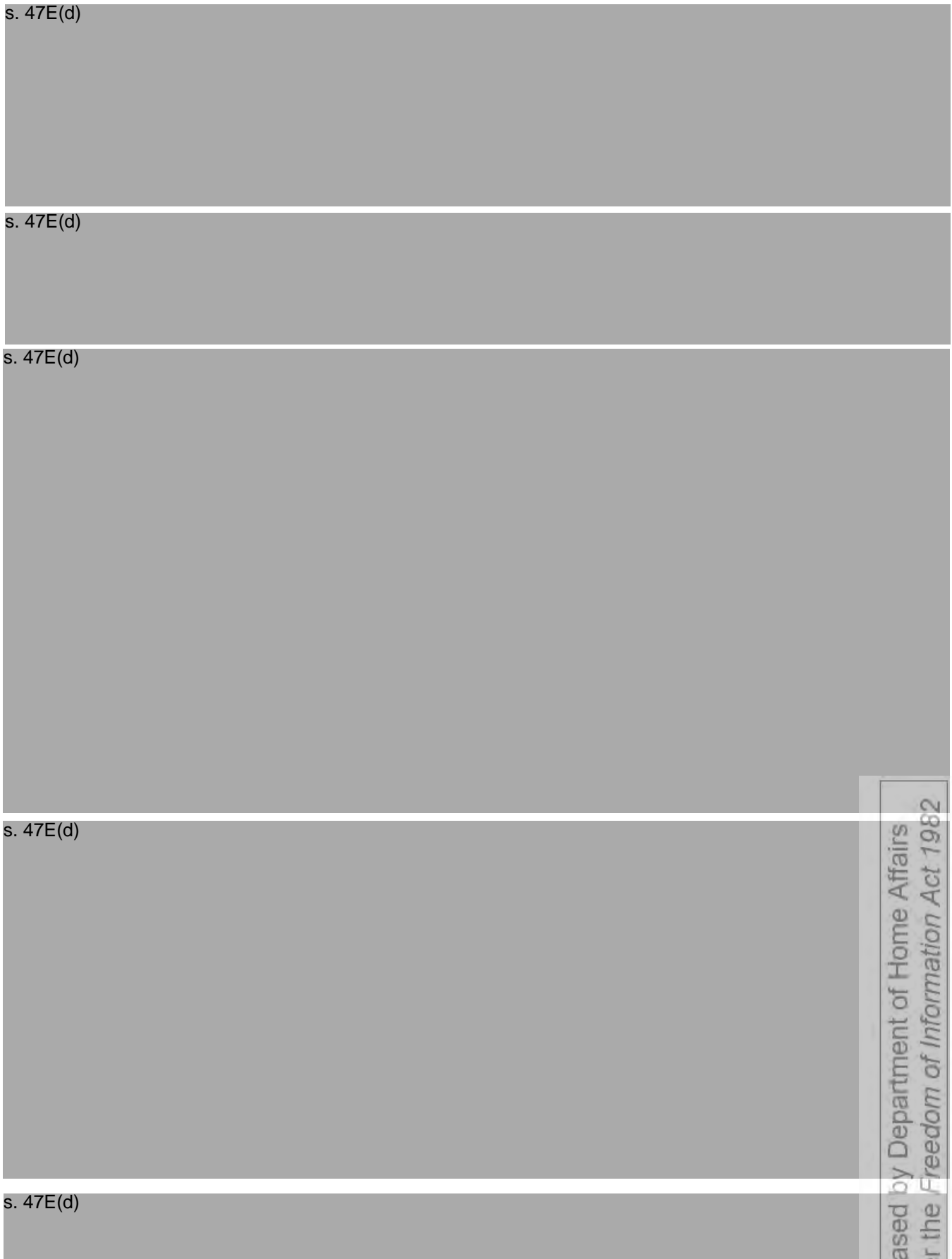


s. 47E(d)



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

s. 47E(d)



s. 47E(d)

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)



### 3. CMAL Remote Input Function (RIF) Guidelines – s. 47E(d) - 26

s. 47E(d)



#### 3.2. s. 47E(d) - 26

The table below lists the process for proposing identities for inclusion on MAL.

**Note:** A similar process is followed for bulk loads as the BOC must review the contents of the batch file before it is loaded into CMAL.

**See:** Bulk loads

Stage	Who	Description
1	Home Affairs staff member	Proposes the identity addition using the CMAL Remote Input Function (CMAL RIF) ensuring that: <ul style="list-style-type: none"> <li>the record contains adequate information</li> <li>data quality standards are met.</li> </ul>

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

Stage	Who	Description
		<p><b>Note:</b> All CMAL RIF proposals are automatically forwarded to the ARC owner for review.</p> <p><b>See:</b> The following for inclusion requirements:</p> <ul style="list-style-type: none"> <li>• <u>Alert Reason Codes</u></li> <li>• <u>Narrative requirements</u></li> </ul>
2	ARC Owner	<p>Reviews the proposed record to ensure that:</p> <ul style="list-style-type: none"> <li>• the reasons for listing are in line with policies for inclusion</li> <li>• data quality standards have been met</li> <li>• the necessary approvals have been sought.</li> </ul> <p>If the record is:</p> <ul style="list-style-type: none"> <li>• valid, go to Stage 3, or</li> <li>• invalid, liaise with the Home Affairs staff member and decide whether or not to proceed with adding the record.</li> </ul> <p><b>Note:</b> If still adding the record, repeat Stages 1 and 2 until the record is valid.</p>
3	System updated	<p>Proposed record added to MAL.</p> <p><b>Note:</b> After a record has been added to MAL:</p> <ul style="list-style-type: none"> <li>• Home Affairs staff members are responsible for updating the record in response to any information they receive concerning the identity</li> <li>• ARC Operational Owners are responsible for reviewing the record to maintain its validity.</li> </ul>

## 4. CMAL Remote Input Function (RIF) Guidelines – Documents

### 4.1. Documents for inclusion on MAL

The table below lists guidelines for proposing documents for inclusion on MAL.

**Prerequisite:** If the document is an Australian travel document, FAS must have approved the document to be listed on MAL before submitting a proposal.

**See:** Considering Australian documents for MAL

**See also:** Bulk loads.

Stage	Who	Description
1	Home Affairs staff member	<p>Proposes the document addition using the CMAL Remote Input Function (CMAL RIF) ensuring that:</p> <ul style="list-style-type: none"> <li>• the record contains adequate information</li> <li>• data quality standards are met.</li> </ul> <p><b>Note:</b> All CMAL RIF proposals are automatically forwarded to the ARC owners for review.</p> <p><b>See:</b> The following for inclusion requirements:</p> <ul style="list-style-type: none"> <li>• <u>Required data</u></li> <li>• <u>Narratives</u></li> </ul> <p><b>See also:</b> The following checklists containing requirements that must be met before listing a document on MAL:</p> <ul style="list-style-type: none"> <li>• <u>Checklist – Australian Travel Documents</u></li> <li>• <u>Checklist – New Zealand Travel Documents</u></li> <li>• <u>Checklist – Foreign Travel Documents</u></li> </ul>

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



Stage	Who	Description
2	ARC owner	<p>Reviews the proposed list to ensure that:</p> <ul style="list-style-type: none"> <li>the reasons for listing are in line with policies for inclusion</li> <li>data quality standards have been met</li> <li>necessary approvals have been sought.</li> </ul> <p>If the record is:</p> <ul style="list-style-type: none"> <li>valid, go to Stage 3, or</li> <li>invalid, liaise with the Home Affairs staff member and decide whether or not to proceed with adding the record.</li> </ul> <p><b>Note:</b> If still adding the record, repeat Stages 1 and 2 until the record is valid.</p>
3	System updated	<p>Proposed record added to MAL.</p> <p><b>Note:</b> After a record has been added to MAL:</p> <ul style="list-style-type: none"> <li>Home Affairs staff members are responsible for updating the record in response to any information they receive concerning the identity</li> <li>ARC Operational Owners are responsible for periodically reviewing the record to maintain its validity.</li> </ul>

#### 4.2. DAL bulk loads

The table below lists the process for proposing bulk loads of documents for inclusion on DAL.

**Prerequisite:** Australian travel documents are not loaded through the bulk load. This process is for foreign travel document lists only.

Stage	Who	Description
1	BOC	<p>Receives bulk load file through mail or email and pre-processes the data into MAL Standard bulk load format.</p> <p><b>See:</b> The following for inclusion requirements:</p> <ul style="list-style-type: none"> <li><u>Required data</u></li> <li><u>Narratives</u></li> </ul>
2	Policy owner	<p>Reviews the proposed records to ensure that:</p> <ul style="list-style-type: none"> <li>the reasons for listing are in line with policies for inclusion</li> <li>data quality standards have been met.</li> </ul> <p>If the records are:</p> <ul style="list-style-type: none"> <li>valid, go to Stage 3, or</li> <li>invalid, liaise with informer and decide whether or not to proceed with adding the list or records within the list.</li> </ul> <p><b>Note:</b> If still adding the record, repeat Stages 1 and 2 until the record is valid.</p>
3	System update	<p>Adds the records to MAL.</p> <p><b>Note:</b> After records have been added to MAL:</p> <ul style="list-style-type: none"> <li>All CMAL users are responsible for updating the record in response to any information they receive concerning the identity</li> <li>ARC Operational Owners are responsible for periodically reviewing the record to maintain its validity.</li> </ul>

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

s. 47E(d)



## **5. CMAL - checking MAL and assessing potential matches**

### **5.1. Performing MAL Checks**

s. 47E(d)




Identity alerts that arise during a MAL check occur when data from the following is matched:

- Person Alert List (PAL) record on MAL, and
- client details from the relevant visa processing system (GVP, ICSE, TRIPS, IRIS).

#### **How do MAL checks work?**

s. 47E(d)



The CMAL system determines a score based on the client's biometric data and the biometric data contained within the PAL. If the score does not meet the variable threshold the system will automatically generate a Green status. If the score meets the threshold score, or above, the system will generate an Amber status and a case will

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

be generated. A Match Case Analyst will resolve the Amber case by assessing it as a true match (assigning a Red MAL status) or assessing the case a non-match (assigning a Green MAL status).

**Note:** It is possible for multiple potential MAL identities to be created within one case. The collective identities are called a Match Case and are all assessed to determine if they match the identity in question.

**See:**

Variable thresholds

Initial MAL status allocation and action

CMALs name matching software

Actioning and overriding MAL alerts.

s. 47E(d)



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

### 5.3. Variable thresholds

ARC policy owners specify threshold scores and minimum data standards for each ARC for which they are responsible. These scores are often linked to the risk level associated with the ARC, which therefore result in varying scores. Currently, the systems variable threshold allows for 85% and 95%, depending on the requirements of the ARC owner.

**Note:** All requests to change an ARCs variable threshold score must be submitted to the Superintendent of the ABF Operations Systems Management.

### 5.4. Documents

By default, all document records have a threshold score of 100. This means that a travel document that a person presents must be an exact match with a document record listed on MAL before an alert is raised.

The Amber status does not apply to documents.

## 5.5. Identities

Due to the nature of identities and the possibility of unknown biographical data, variable thresholds are generally not set at 100. This means that a MAL alert might occur if there is a partial data match.

**Example:** A visa applicant's data might score 86 against a MAL-listed identity. This might be a high enough score for a potential match if the MAL identity is listed under an ARC whose threshold is 85. However, it wouldn't be if the MAL identity is listed under an ARC whose threshold is 90.

## 5.6. Initial MAL status allocation and action

CMAL automatically allocates statuses as follows:

- Green or Red MAL status for document alerts  
**Note:** No potential match cases are created for DALs.
- Green MAL status for identities that score less than the ARC threshold score. This is explained in the table below.

**Note:**

- Approximately 85% of all MAL checks are automatically assigned a Green status, based on the way the name matching software is tuned.  
**See:** CMALs name matching software
- The Border Operations Centre (BOC) assesses all identities that are partially matched (Amber status) and changes the status to Green or Red as required.  
s. 47E(d)
- Home Affairs officers are required to follow specific steps when a document or identity is allocated a Red MAL status.  
**See:** Actioning and overriding MAL alerts.
- On rare occasions where no MAL status is reflected in the visa processing system, the visa processing/case officer should raise the issue with IT Support and contact the BOC for assistance.

	Score	MAL status	Allocation
Document:	<100	Green	System automatically assigns MAL status
	100	Red	System automatically assigns MAL status
Identity:	0-<threshold	Green	System automatically assigns MAL status
	Threshold score or above	Amber	System automatically assigns MAL status – Match Case Analyst must assess the case.

s. 47E(d)



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



### 5.8. CMALs name matching software

The name matching software in CMAL is designed to provide an ordered list of potential matches based on certain tolerance levels and rules. These rules are assembled and weighted to match the data stored in CMAL and are periodically reviewed and tuned to better match search expectations. The key fields that contribute to the threshold score include name, Date of Birth (DOB), Country of Birth (COB), citizenship and gender.

**Contact:** The s. 47E(d) for further information about CMALs name matching software if required.

**Note:** Potential matches at or above the variable threshold are presented to match case analysts in the BOC for evaluation.

s. 47E(d)

### 5.9 Biometrics matching capability

The Biometric Person Identifier (BPI), automatically generated from the Client Data Hub (CDH), allows ABF CMAL users to review and assess the potential biometric match or mismatch on a PAL.

Biometric matching has been made possible by the introduction of the Enterprise Biometric Identification Service (EBIS) system, and more specifically the collection and association of BPIs to client records held within CDH. In essence a BPI can be thought of as a person's biometric identity. If two client records have the same BPI, they are the same person.

There may be instances where there is a biometric match exception, that is:


- PAL and client are the same person but there is a biometric mismatch; or
- PAL and client are not the same person but there is a biometric match

s. 47E(d)

s. 47E(d)

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

s. 47E(d)



## 6.2. Assessing duplicate records

If duplicate records are detected during a MAL check, the officer must examine all the identity and/or document records that are returned as duplicates. This means the narratives for the records must be carefully read and the appropriate action taken to remove the duplication.


## 6.3. Assessment priorities

Any match cases with s. 47E(d) take precedence over the other matches in terms of follow up actions and decision making. If none of the records contain s. 47E(d) potential matches, then the match with the highest risk category takes precedence and must be resolved first.

s. 47E(d)




s. 47E(d)



## 6.6. Resolving a potential match


Once the case is resolved in CMAL, the client's MAL status will be updated in the various processing systems notifying relevant decision-makers, such as border, visa and citizenship officers.

s. 47E(d)



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

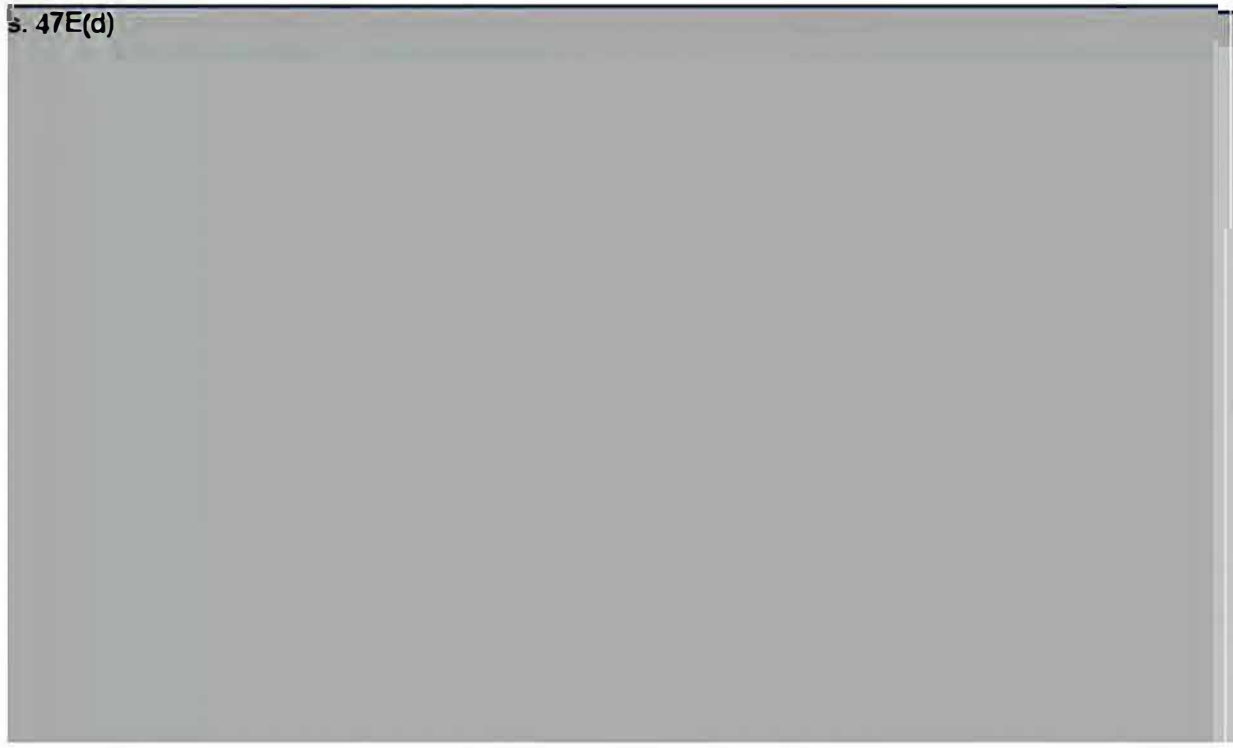
s. 47E(d)



s. 47E(d)

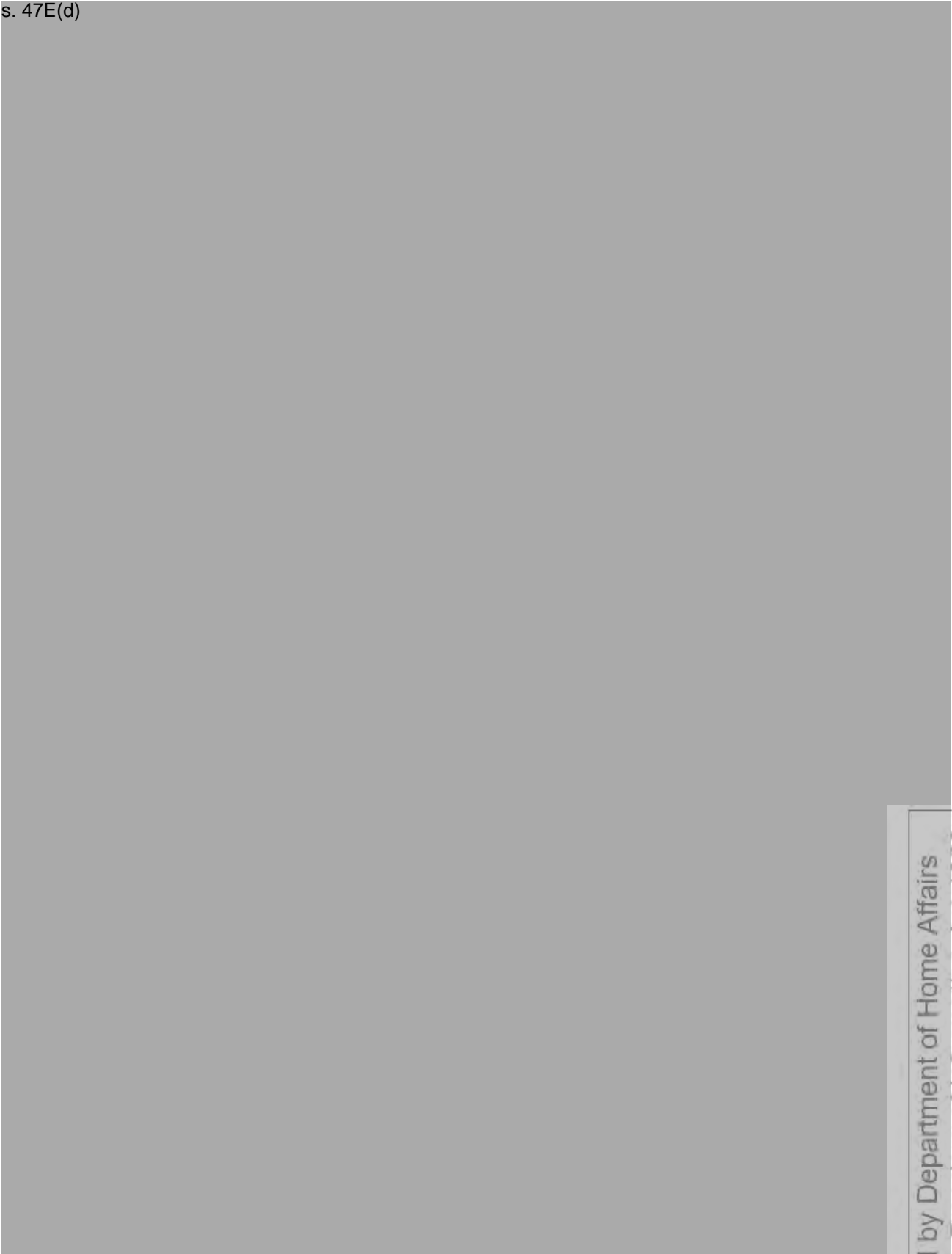


s. 47E(d)



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

s. 47E(d)



s. 47E(d)




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



s. 47E(d)



s. 47E(d)



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)



## **8. CMAL Guidelines - actioning and overriding MAL alerts**

As a result of a MAL check the client's MAL status is set to indicate whether there is a concern to be taken into account in determining the outcome of a client application. A concern is indicated by:

- documents that have matched the client and resulted in a Red MAL status
- identities that have matched the client and resulted in an Amber or a Red MAL status.

Depending on the circumstances, specific actions should be taken to determine how the alert should be treated.

Whenever practicable, the processing of an application may continue while awaiting a response on a referred potential match. If the decision maker determines that the person does not meet the prescribed requirements, for reasons other than those related to the MAL narrative, the decision on visa, citizenship or immigration clearance may be made without waiting for a response on the potential MAL match.

### **8.1. MAL is not a legislative instrument**

MAL is an administrative tool used in assisting decision makers to determine the risk associated with a particular identity or travel document to Australia. Therefore, a Red MAL status is not a legislative basis for refusing a visa or citizenship application, or denying entry into Australia.

It is important to understand that MAL is only one component of the immigration assessment process and a Red MAL status does not necessarily mean the application or applicant will be refused entry or a visa. MAL is a mechanism for alerting relevant decision-makers that further investigation is required before making a decision.

CMAL is similar to Safeguards in some aspects, as it is also a tool utilised to assess risk and, similar to CMAL, Safeguards has no direct legislative basis. CMAL should be considered as a 'tool of trade', informing various decision makers about information which they need to take into consideration prior to making a decision.

Decision makers in various roles throughout the Department (such as visa processing/case officers) will make decisions based on a holistic, evidence based approach. This will include information that has been obtained from numerous sources, including:

- the client
- internal and external stakeholders
- sourced documentation

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

- system searches
- the client's MAL status.

The final decision to grant or refuse an application or entry into Australia will be directly linked to a specific component of legislation, not on the client's MAL status.

Example: Refusal due to character concerns under s 501 of the *Migration Act 1958* (Migration Act).

s. 47E(d)

s. 47E(d)

### 8.3. Granting citizenship to a MAL-listed identity

A citizenship applicant may have a Red MAL status. The:

- nature of the concern will be taken into account in the citizenship process
- ARC policy and/or operational owner should be consulted in the citizenship process
- concern must be removed when citizenship is finalised.

**Note:** The ARC operational owner is responsible for updating MAL. They will be reminded to do this when the ceremony is complete and the citizenship is finalised.

s. 47E(d)

The table below sets out the steps that decision-makers must follow in response to a MAL alert for a document.

Step	Action
1	Read the narrative on the DAL record to determine the action required. s. 47E(d)

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

Step	Action
	<p>s. 47E(d)</p> <p>Note: Some document records on MAL will include a file number. This is an indication that a file exists that contains further information, and therefore it will be necessary to contact the originating area for a copy of the file.</p>
2	If stated in the narrative, contact the area that originally listed the document on MAL for further guidance. Go to Step 4.
3	<p>Consider the information in the narrative and determine what impact this has on the decision to continue processing the client or detaining them for further investigation.</p> <p><b>Tip:</b> If it is suspected that the document may be fraudulent, it may be beneficial to interrogate the travel document using the available authentication tools.</p>
4	<p>If it is determined that the document alert is:</p> <ul style="list-style-type: none"> <li>invalid, request that the document be expired from MAL if there are no other matches, or <b>Note:</b> If the BOC approves the expiry, the MAL status will change to Green once the record is expired</li> <li>valid, update the narrative to reflect the outcome and any subsequent actions, irrespective of whether the visa, citizenship or immigration clearance has been refused or granted.</li> </ul> <p><b>See:</b> <u>Reviewing and updating MAL identities and documents</u> s. 47E(d)</p>

### 8.5. Actioning MAL identity alerts with Amber status

The BOC assesses clients who have an Amber status to determine whether or not they are a true match with an identity listed on MAL. Decision makers who are informed of the alert should wait for the BOC to assess the case in line with the Amber Service Level Agreement.

In exceptional circumstances, such as a system outage, the decision-maker can contact the BOC to request an override key so that processing can continue. The BOC will investigate the specific match case and decide if an override key should be issued.

s. 47E(d)

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



s. 47E(d)

Clients who have been assessed as a true match against a MAL-listed identity are allocated a Red MAL status. Decision-makers who are informed of the alert must decide whether the:

s. 47E(d)

**Note:** If the BOC approves the expiry, the client's MAL status will change to Green once the record is expired.

s. 47E(d)

If a decision-maker wishes to proceed with the client's application, despite the alert, the alert must be overridden. Different override measures exist according to the risk category of the ARC under which the MAL identity is listed. Actions related to these measures are listed in the table below.

**Important:** An override does not change the client's MAL status; it temporarily changes the immigration directive. s. 47E(d)

s. 47E(d)

s. 47E(d)

## 8.8. Updating narratives

It is important for visa processing/case officers and decision-makers to update narratives in response to actions that they take regarding MAL alerts for documents or identities. This ensures that subsequent decision makers have access to all decisions and actions regarding a document or identity.

If a visa processing/case officer or decision maker proposes that a document or identity be expired from MAL, the CMAL system will require a narrative update as part of the process.

**See:**

Narrative requirements

s. 47E(d)

## 9. Process: manually expiring an identity or document record

The table below lists the process for manually expiring MAL identity and document records.

**Note:** All expired records are archived. Once archived, records cannot be reactivated or changed. However, officers with the relevant level of CMAL access can view the records. ARC owners have the final authority whether or not a proposed record should be expired on MAL.

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

Stage	Who	Description
1	Departmental officer	Creates a CMAL RIF proposal to expire an identity or document record. <b>Note:</b> <ul style="list-style-type: none"> <li>The narrative must contain the reason for the expiry including if applicable, the authority to expire.</li> <li>A proposal to expire an alert is sent to the ARC owner who can then make the decision to expire the alert or keep the alert on CMAL.</li> </ul> <b>See:</b> <a href="#">CMAL access</a>
2	ARC owners	Reviews the proposal to ensure that the record is not relevant to another area requiring it to remain on MAL. If the record: <ul style="list-style-type: none"> <li>needs to remain on MAL, the ARC owner will reject the proposal explaining why and the proposer has the option of resubmitting a revised proposal for the ARC owner's consideration. End process, or</li> <li>can be expired, go to Stage 3.</li> </ul>
3	System update	Approves the proposal to expire the identity or document record which will be reflected on MAL.

## 10. Disclosure and Classification of MAL Records

### 10.1. Security classification of MAL records

By default, the CMAL system classifies MAL records according to the table listed below.

Record type	Classification	Operational difference
s. 47E(d)	s. 47E(d)	s. 47E(d)
All other identity(PAL) and document (DAL) records	'OFFICIAL: Sensitive	Therefore extra security features have been incorporated into CMAL to accommodate this security classification. <b>Example:</b> <ul style="list-style-type: none"> <li>CMAL narratives for 'PROTECTED' records are only visible to staff working in the Border Operations Centre (BOC) and officers in particular sections of Intelligence division.</li> <li>Match cases with 'PROTECTED' records can only be overridden using an override key provided by the BOC following authorisation from the Alert Reason Code (ARC) operational owner.</li> </ul>

**Note:** Records can be re-classified if necessary. If there is a business need for this to occur, please contact the relevant ARC owners stating the reasons the record does not warrant the default security classification.

### 10.2. Privacy and Freedom of Information

From an operational perspective, Freedom of Information (FOI) means clients have the legal right to request a copy of the information the Department holds about them, including copies of:

- files
- system screen dumps
- notations made on systems with regards to clients activities
- interview notes.

Several documents relating to the *Privacy Act 1988* (Privacy Act) and the *Freedom of Information Act 1982* (FOI Act) are available from the Department's intranet site. A Freedom of Information and Privacy training package is available from the Department's eLearning on-line program. This course is designed to assist departmental officers understand their rights and responsibilities under the *Privacy Act* and the *FOI Act*. This on-line training course is available to all staff members and can be accessed from the Department's intranet site.

### 10.3. Further information

The Department's intranet contains information on the Department's obligations under the Privacy and Freedom of Information Acts, including disclosure of personal information from Home Affairs systems. The table below lists contact details for further information and guidance if required.

Contact	Information and guidance
The FOI and Privacy Policy Section	Privacy Act
Office of the Australian Information Commissioner	<ul style="list-style-type: none"> <li>Privacy Act, including the Australian Privacy Principles (APPs)</li> <li>FOI Act.</li> </ul>

### 10.4. Disclosing MAL business operations and stakeholders

MAL is an integral component of Australia's national security and border control strategy. Disclosure of information stored in or about the MAL may expose intelligence methods and other operational means of protecting the Australian community. Information related to the following must not be discussed or disclosed:

- How MAL information is obtained
- The stakeholders involved
- The MAL business processes, including when and where MAL checks occur.

Clients seeking information on MAL can be referred to Fact Sheet 77 - The Movement Alert List located on the Department's website. This document describes the existence and purpose of the MAL and is appropriately generic for the public domain. Officers considering disclosure of information that is not included in Fact Sheet 77 must seek the relevant ARC owner approval.

### 10.5. Disclosing personal information contained in MAL

Requests to disclose any personal information under the FOI Act must be referred to the National Office Freedom of Information Section: [foi@homeaffairs.gov.au](mailto:foi@homeaffairs.gov.au). This section will assess, in conjunction with ARC owner and the MAL record owner, what information may be released relating to the request. The release of information contained within MAL will depend on the content of information contained in the record/s and will be assessed on a case by case basis. Depending on the MAL record's information source, particularly those relating to national security matters, it may be exempt under the FOI Act.

Contact the FOI and Privacy Policy Section for further information regarding the FOI Act.

### 10.6. Disclosing adverse information to government agencies

Home Affairs staff should contact the relevant agency to arrange listing on other appropriate systems if:

- they have adverse information on people or clients, such as law enforcement or national security related information
- it is determined that the information does not meet the criteria for listing on MAL.

**Example:** The following are examples of situations in which staff must contact an agency:

- Contacting the Australian Federal Police (AFP) to list Australian citizens involved in criminal activity which is not:

- associated with the Migration Act, or
- relevant to any of the reasons associated with Alert Reason Codes (ARCs).
- s. 47E(d) to list fraudulent Australian passports or travel documents which do not meet the requirements for listing on MAL.

If required, ARC owners can advise whether it is appropriate to pass the information on and provide the necessary contacts.

The MAL referral process may involve forwarding information to other agencies or responsible areas within Home Affairs. As these enquiries may take some time to resolve, ARC owners may follow up by calling these agencies if there are compelling circumstances to resolve alerts in an urgent timeframe.

Before referring information to another agency, officers should consider any applicable restrictions on disclosure under the Privacy Act, the Migration Act and/or the *Australian Border Force Act 2015*.

**See:**

Considering Australian identities for MAL

Considering Australian documents for MAL

## 11. Policy Implications for Public Interest Criteria

This section describes the Public Interest Criteria (PICs) that are aligned to each MAL ARC. The PIC is often the legislative basis for:

- granting or refusing applications, or
- refusing entry into Australia.

**Important:** A MAL check does not constitute a PIC check. If the applicant falls within a profile requiring a security check in accordance with the agreed methodology, this is a separate action demanding separate advice from the relevant organisation.

### 11.1. Relationship between PIC and ARC

Each visa class will have specific criteria to be met including PIC, which may relate directly or indirectly to an ARC in MAL. The tables at the end of this section indicate what types of character concerns are addressed by records belonging to the one or more of the MAL ARCs.

**See also:** Alert Reason Codes

### 11.2. Section 501 of the Migration Act

In general terms under Section 501 of the Migration Act, grounds exist to consider cancelling a client's visa or refusing a visa application if the person is not of good character.

Section 501 grounds can apply if the person has:

- a substantial criminal record within the meaning of s 501(7) of the Migration Act
- associations with criminals or criminal groups
- issues relating to their past and present criminal conduct, or
- issues relating to their general conduct.

The MAL check only searches known concerns to determine whether there are grounds for not processing an application.

The character considerations under which Home Affairs may refuse to grant a visa are based on the character test as defined in Section 501(6) of the Act.

**See:** Section 501: The character test, visa refusal & visa cancellation, Migration Act on LEGEND.

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



### 11.3. PIC 4001 - Character Concerns ARC 03, 05, 09, 25

In general, character concerns are covered by PIC 4001 which details the Character Test.

**See:** Section 501: The character test, visa refusal & visa cancellation, Migration Act on LEGEND.

### 11.4. PIC 4002 - Security of the Australian Community s. 47E(d)

The relevant organisation's assessment of the applicant has found that they are not directly or indirectly a risk to security, within the meaning of the appropriate legislation.

A MAL check does not constitute a PIC 4002 check. If the applicant falls within the PIC 4002 profile, and therefore requires a security check in accordance with the agreed procedure, this is a separate action demanding separate advice from the relevant organisation.

The PIC 4002 is a completely separate process to MAL. Therefore, a MAL clearance under s. 47E(d) does not constitute PIC 4002 clearance – it is still relevant to complete the PIC 4002 process.

**Contact:** Security Assessment Liaison and Analysis (SALA). Email s. 47E(d)

### 11.5. PIC 4003(a) - National Security or Foreign Policy interest ARC 18

PIC 4003(a) deals with assessing a person's character against Australia's foreign policy interests.

**See:** Section 501: The character test, visa refusal & visa cancellation, Migration Act on LEGEND.

### 11.6. PIC 4003A/4003(b) - Weapons of Mass Destruction ARC 04

PIC 4003A and PIC 4003(b) specifically deal with the proliferation of weapons of mass destruction.

Contact the National Security Assessments and Counter Proliferation Operations section for information concerning PIC 4003A and PIC 4003(b). Further information *may not* be available on LEGEND.

**Email:** s. 47E(d)

**See also:** Section 501: The character test, visa refusal & visa cancellation, Migration Act on LEGEND.

### 11.7. PIC 4004 - Debts to the Commonwealth ARC 12

PIC 4004 deals with whether there is balance of outstanding debt to the Commonwealth of Australia.

**See:** Shd4 – 4004 – Debts to the Commonwealth, Migration Regulations on LEGEND.

### 11.8. PIC 4005/4007 - Health/Health Burden ARC 06

PIC 4005 and 4007 deal with a client's medical status in respect to their risk or treatment cost to the Australian community. They deal with:

- diseases or conditions, such as tuberculosis
- the requirements to comply with actions that a Medical Officer of the Commonwealth sets out.

**See:** Sch4/4005-4007 – The Health Requirement, Migration Regulations on LEGEND.

### 11.9. PIC 4012 - Unaccompanied Minors

PIC 4012 relates to an undertaking by a person of good character, in relation to minors, to ensure that their interests are protected and that Australia meets its international obligations.

**See:** PIC 4012 Unaccompanied minors, Migration Regulations on LEGEND.

**11.10. PIC 4013 - Cancellation ARC 07, 11, 13**

PIC 4013 deals with exclusion periods imposed on people whose visas have been cancelled because they have breached the conditions of their visa, or they have given incorrect answers to questions on their visa application or passenger card, or they have failed to update the Department of a change in their circumstances, or they have given a bogus document to the Minister or a tribunal, or because the Minister is not satisfied as to the person's identity.

**See:** PIC 4013 risk factor, Migration Regulations on LEGEND.

**11.11. PIC 4014 - Overstayers ARC 10**

PIC 4014 deals with enforcing exclusion periods on people who have overstayed their visa or have been unlawfully in Australia.

**See:** PIC 4014 risk factor, Migrations Regulations on LEGEND.

**11.12. PIC 4015/4017 - Child Custody (parental responsibility) concerns ARC 08**

PICs 4015 and 4017 deal with an applicant who is under 18 years of age having permission to be granted the visa through:

- the laws of their home country or
- an Australian court order or a court order issued by their home country or
- written permission being provided from all persons with parental responsibility (custody) for them.

An ARC 08 alert may also be raised where there are concerns that an adopted child may be brought to Australia without the permission of the child's home country, or without formal adoption proceedings having been finalised.

**See:** Sch4 - 4015-4018 - Custody (parental responsibility) and best interests of minor children, Migration Regulations on LEGEND.

**11.13. PIC 4020 - The Integrity PIC ARC 20**

PIC 4020 is intended to strengthen the integrity of Australia's migration program by minimising the level of fraud in visa applications and provide a ground to refuse to grant a visa.

PIC 4020(1) enables a visa to be refused if there is evidence that the visa application involves a bogus document or information that is false or misleading in a material particular. This can be in relation to a current application, or a visa the applicant held in the 12 months prior to the current application. If an applicant (other than a minor) fails to satisfy PIC 4020(1), they become subject to a non-grant period of three years.

PIC 4020(2A) enables a visa to be refused if the applicant fails to satisfy the Minister of their identity. If an applicant (other than a minor) fails to satisfy this aspect of PIC 4020, they become subject to a non-grant period of 10 years.

When applicants who were a minor at the time of application, are refused for failing to satisfy PIC 4020(1) or (2A), they will not be subject to the non-grant periods provided under PIC 4020(2) and (2B) in future applications.

If a visa is refused because of a failure to satisfy PIC 4020(1) or (2A), a member of that applicant's family unit (MOFU) may also fail to satisfy PIC 4020(2) or (2B) in both the same application, and in future applications. A MOFU is impacted by the refusal and may be subject to the relevant non-grant period.

PIC 4020(4) waiver provision gives delegates the discretion to waive the requirements of any or all of PIC 4020(1) or (2) if they are satisfied that:

- compelling circumstances that affect the interests of Australia; or

- compassionate or compelling circumstances that affect the interests of an Australian citizen, an Australian permanent resident or an eligible New Zealand citizen;

justify the granting of the visa.

**See:** Public Interest Criterion 4020, Migration Regulations on LEGEND.

#### 11.14. Illegal Foreign Fishers Legislation ARC 19

The Department's involvement with illegal foreign fishers begins when the person enters immigration detention, following the expiry of an Enforcement Visa. An Enforcement Visa:

- is granted to a non-citizen who is on a foreign boat outside the migration zone
- allows them to be brought into the migration zone lawfully.

The Australian Border Force (ABF) usually apprehend illegal foreign fishers at sea and brings them to Australia under relevant powers under the *Customs Act 1901*. They are then detained at port by the Australian Fisheries Management Authority and taken into fisheries detention.

**Note:** Immigration detention and fisheries detention are separate regimes. A person in fisheries detention cannot be subject to immigration detention or *Migration Act* powers.

Fishers held in fisheries detention may be physically held in an Immigration Detention Centre but cannot be in immigration detention at the same time. However, the Department's detention service provider is responsible for fishers whether they are in fisheries or immigration detention.

##### Fisheries Management Act and Torres Strait Fisheries Act

After being apprehended and detained under the *Fisheries Management Act 1991* or the *Torres Strait Fisheries Act 1984*, fishers may be held in custody for no longer than 168 hours or if a Papua New Guinean national, 72 hours.

Fishers must be released from custody if Australian Fisheries Management Authority decides not to charge the fishers with an offence. If this occurs, the Enforcement Visa ceases to have effect under the Migration Act and the fisher must be taken into immigration detention.

#### 11.15. Damaged passports and the *Australian Passports Act* ARC 17

The Australian Passport Act in conjunction with s175A of the *Migration Act* requires that a passport not be damaged in such a way as to obscure the identity of the holder; where the photo, personal information or other important information is not legible. . In 2005 it became policy to impound seriously damaged passports pending the cancellation or voiding in the Australian Passport database.

#### 11.16. Sanctions Regimes ARC 18

Persons are listed under ARC 18 if they are:

- subject to UNSC resolutions which impose travel sanctions, or
- subject to Australia's autonomous travel sanctions as imposed by the Foreign Minister.

##### United Nations Security Council (UNSC) Sanctions

Australia meets its obligations to enforce UNSC Travel Sanctions through the *Migration (United Nations Security Council Resolutions) Regulations 2007* (UNSC Resolutions Regulations). The Minister for Home Affairs has the power to specify, by legislative instrument, which UNSC Resolutions the Migration Regulations covers. The legislative instrument is revised:

- each time a resolution imposing new travel sanctions is passed, or
- if existing travel sanctions are removed or amended.

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

#### Australia's Autonomous Sanctions

Autonomous travel restrictions are implemented under the Foreign Minister's powers specified by Public Interest Criterion 4003(a) at Schedule 4 and regulation 2.43(1)(a)(i)(A) of the Migration Regulations, to support Australia's foreign policy objectives.

#### **11.17. Geneva Conventions Act 1957 ARC 03**

Home Affairs has a responsibility to identify and make determinations on war criminals and those who are involved in the proliferation of weapons of mass destruction.

Legislation cited as being relevant to ARC 03 includes:


- *War Crimes Act 1945*
- *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995*
- *Criminal Code Act 1995*.

#### **11.18. S166 Travel Document Requirement - DAL records**


Persons travelling to Australia must be properly documented.

**See:** Section 166 of the Migration Act in LEGEND for current detail.

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



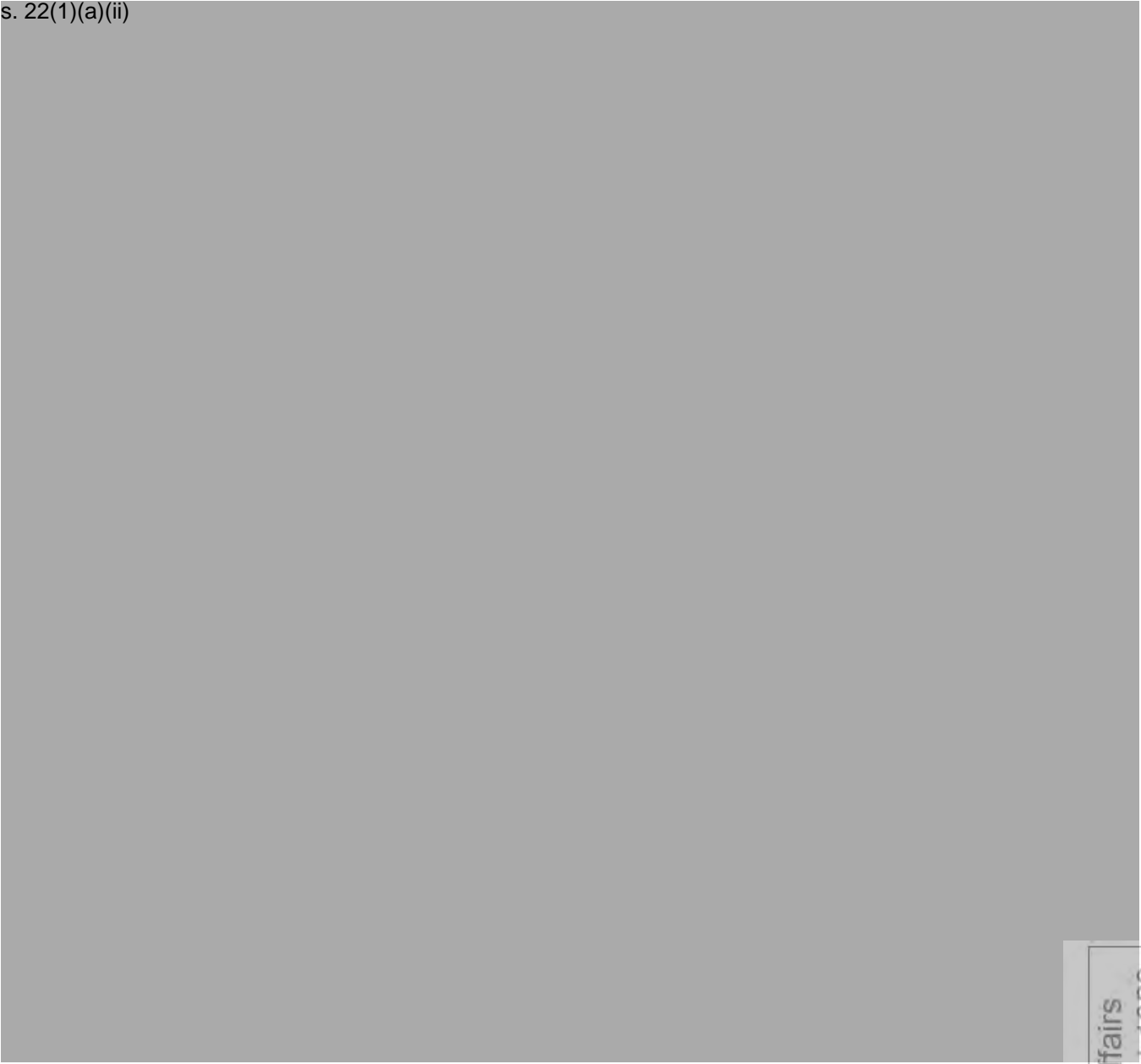
s. 22(1)(a)(ii)




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



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




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




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


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

A large rectangular area of the page is completely redacted with a solid grey fill.

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


A large rectangular area of the page is completely redacted with a solid grey fill.

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

A large rectangular area of the page is completely redacted with a solid grey fill.

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

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



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