Face Identification Service (FIS) Access Policy

National Facial Biometric Matching Capability

IDENTITY SECURITY

Contents

FACE IDENTIFICATION SERVICE ACCESS POLICY

PART 1 - PURPOSE

1.1 This policy sets out the requirements that Participating Agencies must meet to gain and maintain access to the Face Identification Service (FIS).

1.2 This policy supports the *Intergovernmental Agreement on Identity Matching Services* and the Face Matching Services Participation Agreement. If there is an inconsistency between this policy and those agreements, those agreements prevail to the extent of the inconsistency

PART 2 - DESCRIPTION OF THE FIS

2.1 The FIS is one of the Face Matching Services provided by the National Facial Biometric Matching Capability ('the Capability').

2.2 The Capability adopts a 'hub-and-spoke' model, which is comprised of a central interoperability Hub (the Hub) a technical system that provides a mechanism for the secure and auditable transmission of facial images and associated information, or other information contemplated by the PA, between Participants.

2.3 The FIS enables a facial image associated with an individual to be compared on a one-to-many basis against images held in government records to help determine the identity of that individual, or to detect instances where an individual holds multiple, potentially fraudulent identities.

2.4 The FIS requires the Requesting Agency to submit a query containing a facial image, demographic details (such as age range and gender) and query authorisation details (such as purpose, authorising legislation and an internal reference number).

2.5 The response from a Data Holding Agency contains a gallery of the highest matching images, as determined by the facial recognition system used by the Data Holding Agency (based on a pre-configured match threshold). The size of the image gallery is determined by the Data Holding Agency and will not normally exceed 20 images.

2.6 The biographic details associated with the images will only be released to the Requesting Agency once the user selects or shortlists from the gallery any particular image(s) they wish to examine. The number of images that can be shortlisted from a gallery is also determined by the Data Holding Agency.

2.7 The Requesting Agency is responsible for reviewing the image gallery to resolve the identity of the person who was the subject of the request.

2.8 Access to the FIS is made available to Participating Agencies via a web-based user interface (the Portal) to the Hub that enables users to log in and manually enter queries.

2.9 An administration facility for the FIS is provided through the Portal. It provides the ability for Participants to generate reports, perform audits of user activities and query audit data.

PART 3 - ACCESS PRINCIPLES

3.1 The following access principles underpin the design and operation of the FIS.

a) Promote privacy and compliance with legal provisions

Provision of the FIS by the Hub Controller requires confidence to be maintained that Participating Agencies are exchanging information consistent with their legal basis for data sharing, and that anticipated impacts on the privacy of individuals are outweighed by the public benefit of the service. This dictates the way in which permitted uses are framed, and how supervision and authorisation requirements and other access controls are applied.

b) Protect assumed identities

Continuing provision of the FIS by the Hub Controller is dependent on effective measures to protect assumed identities being in place. This dictates the way in which access controls and authorisation requirements are applied, and audit data is managed. To help protect assumed identities, FIS users must not have concurrent access to the FVS for the same data sources.

c) Non-evidentiary system

The FIS is not designed as an evidentiary system and the results of FIS queries must not be relied upon as the sole basis for ascertaining a person's identity for evidentiary purposes. Requesting Agencies seeking to use FIS results to help identify a person for evidentiary purposes must confirm the accuracy of the information through other channels or processes. Data Holding Agencies are not responsible for decisions made by a Requesting Agency because of their use of the FIS.

d) Information Sharing

Data Holding Agencies should allow Requesting Agencies to access information via the FIS to the maximum extent permitted by law and in accordance with these principles. The details of the disclosure will be agreed between the Data Holding Agency and the Requesting Agency in accordance with the Face Matching Services Participation Agreement (PA) and the Face Matching Services Participant Access Arrangement (PAA).

e) Risk-Based Access Controls

The FIS has a range of access controls which are based on a risk-management approach that balances ***privacy*** and ***security*** safeguards, with ***usability*** and ***timeliness*** of the service for its users, so that the benefits of facial matching may be realised. These include, for example, requirements to seek additional authorisation for searches with greater privacy risks, controlled access to biographic information and limiting use of the FIS to certain permitted purposes.

f) Approved Agencies

Access to the FIS is restricted to agencies with law enforcement or national security related functions. Eligibility of an agency to access the FIS must be approved by the National Identity Security Coordination Group (the Coordination Group). A list of approved Agencies is included as

Attachment A to this policy. While a Requesting Agency may be deemed eligible to have access to the FIS by the Coordination Group, each Data Holding Agency retains discretion as to whether to enter into a Participant Access Arrangement with the Requesting Agency.

g) Permitted Purposes

Participating Agencies may only access the FIS for certain permitted purposes. These permitted purposes are set out in clause 4.21 of the IGA and are replicated in Part 4 of this policy. Individual Data Holding Agencies may choose to limit their provision of the FIS to a subset of these purposes.

h) Nominated Users

Within agencies approved to access the FIS, access must be limited to specific Nominated Users who: perform specialist investigative, intelligence, incident response, forensic, or protective security functions warranting use of the service; meet minimum security clearance requirements; and are sufficiently trained in facial comparison and other relevant areas to ensure privacy-respecting, efficient and effective use of the capabilities within the system.

i) Supervised access

Each Nominated User's access to the FIS must be subject to supervision by a more senior officer. Supervising Officers are responsible for ensuring appropriate use of the service by the nominated users under their management and for acting promptly on any suspected unauthorised use of the service.

j) Additional authorisation to access more delicate information

FIS queries that are for purposes that may be more delicate, or which involve restricted information, will be managed as exceptions, requiring an additional authorisation step in most cases. These authorisation requirements are outlined in Part 5 of this policy.

k) Controlled Access to Biographic Information

The FIS is designed to limit access to biographic information, such as the name and date of birth, of persons who are not the subject of the query. To help maintain the anonymity of these individuals, biographic information will only be made available after the FIS user shortlists an image from the return gallery.

l) Controlled Download and Export of returned images

Data Holding Agencies maintain the right to impose conditions under which Requesting Participating Agencies may download or otherwise export images returned in responses to an FIS query. Images must not be exported by means other than the approved download function. The Requesting Agency will be responsible and will be held accountable for securely managing any images downloaded through the FIS.

m) Auditing to ensure compliance and enable risk management

Sufficient transaction information will be captured by the Hub to support audits of Requesting Agencies for compliance purposes.

PART 4 - PERMITTED PURPOSES

4.1 Participants may only access the FIS for one or more of the following permitted purposes:

a) Preventing Identity Crime

The prevention, detection, investigation or prosecution of identity crime:

(i) manufacturing, dealing, possessing false identification material, or possessing equipment/materials to manufacture false identification material;

(ii) fraudulently using identity information to obtain a financial or other benefit or to avoid obligation; or

(iii) any unlawful act (not elsewhere specified) associated with the fraudulent use of identity information.

b) General Law Enforcement

The prevention, detection, investigation and prosecution of an offence under Commonwealth, State and/or Territory laws, applicable in the jurisdiction of the Requesting Agency, carrying a maximum penalty of not less than three years imprisonment, including but not limited to:

(i) Homicide and related offences

(ii) Offences causing harm to person

(iii) Abduction, harassment and other offences against the person

(iv) Theft and related offences

(v) Non-Identity Fraud and Financial Crime

(vi) Illicit drug offences

(vii) Prohibited and regulated weapons and explosives offences

(viii) Property damage and environmental pollution

(ix) People Smuggling and People Trafficking

(x) Riot and Affray

(xi) Terrorism offences

(xii) Other serious offences carrying a maximum penalty of not less than three years imprisonment;

Note: The scope of the general law enforcement purpose does not limit the ability of states and territories to share identity information between Participants within the same jurisdiction. This will be managed through the PAAs.

c) National Security
Conducting investigations or gathering intelligence for purposes relating to Australia's defence, security, international relations or law enforcement interests;

d) Protective Security
Activities to promote the security of agency assets, facilities or personnel, including but not limited to:

(i) the protection and management of assumed identities; or

(ii) security or criminal background checking

e) Community Safety
Activities to identify an individual:

(i) who is at risk of, or who has experienced, physical harm, including but not limited to:

a. investigating individuals that are reported as missing

b. identifying individuals who are reported as dead, or unidentified human remains

c. identifying individuals when addressing significant risks to public health or safety, or

d. identifying individuals in relation to disaster events or major events, or

(ii) who is reasonably believed to be involved with a significant risk to public health or safety.

PART 5 - SUPERVISION AND AUTHORISATION OF QUERY REQUESTS

Supervision of FIS access

5.1 Nominated FIS Users are generally authorised to submit queries that meet the permitted purposes. Their use of the FIS must be monitored by a Supervising Officer.

5.2 A Supervising Officer must be an officer holding the position of:

(i) for a policing agency:
a. the highest non-commissioned officer rank; and
b. unsworn individuals pursuant to current respective police force oversight arrangements;

(ii) for all other Participating Agencies, Executive Level 1 or equivalent or above.

5.3 The Supervising Officer is responsible for ensuring the Nominated User's use of the FIS is reasonably necessary for one or more of the permitted purposes and is conducted in accordance with the requirements of this Access Policy, the PA, the PAA and other relevant policy and legislation.

5.4 Supervising Officers are provided with access to a summary of the queries conducted by Nominated Users under their supervision and are responsible for reviewing this information, on a routine basis, to ensure compliance with these requirements.

Query requests requiring authorisation

5.5 In most cases envisaged by the permitted purposes, the potential privacy impacts on individuals involved in an FIS query would be clearly outweighed by the broader public interest in preventing or responding to criminal or other activities that cause harm to the community. These cases are standard queries.

5.6 In some cases the relative balance between the privacy impact on individuals and the broader public interests may be less clear. These types of FIS requests (non-standard queries) require an additional level of approval by an Authorising Officer. They involve:

a) queries relating to serious offences that are not listed in this policy (otherwise known as 'other serious offences');

b) queries to identify witnesses to a crime;

c) queries for the permitted purpose of community safety;

d) queries returning larger image galleries; and

e) queries involving persons suspected to be under the age of 18 years.

Queries relating to 'other serious offences'

5.7 The permitted purpose of general law enforcement outlines the categories of offences for which it is anticipated that most FIS queries will be conducted. This is not intended to exclude FIS queries for other types of offences, if they meet or exceed the minimum penalty threshold.

Queries to identify witnesses to a crime

5.8 FIS queries may only be conducted to identify a witness to a criminal offence where:

a) the offence is an offence carrying a maximum penalty of not less than three years imprisonment (as per Part 4 above); and

b) the person who is subject of the query is 18 years of age or older.

Queries for the permitted purpose of community safety

5.9 The permitted purpose of community safety recognises that there may be circumstances which warrant use of the FIS to help prevent harm to an individual or the broader community, but which do not involve serious offences.

5.10 FIS queries conducted for the permitted purpose of community safety must not be used to identify persons undertaking activities that involve the peaceful, lawful expression of political, religious or other views, such as public protests or demonstrations.

5.11 If there are reasonable grounds to suspect that an offence carrying a maximum penalty of not less than three years imprisonment has been committed, or is likely to be committed imminently, in connection

to such activities, and where it is reasonably necessary to use the FIS, the query should be conducted using the general law enforcement purpose, specifying the category of offence involved.

Queries returning larger image galleries

5.12 To manage privacy and security risks associated with potential misuse of the FIS, responses to FIS queries are normally limited to a maximum of the 20 highest matching images.

5.13 In limited circumstances, where the Nominated User has access privileges to do so and authorisation for the query has been provided, they may receive an additional number of those records with images that exceed the matching threshold. However, this would need to be agreed with the Data Holding Agencies and reflected in the PAA.

5.14 Data Holding Agencies may restrict the provision of larger image galleries to queries conducted for certain permitted purposes, or to certain categories of criminal offences within the general law enforcement purpose.

Queries involving persons under the age of 18 years

5.15 FIS queries where the Nominated User suspects the subject of the FIS query is under 18 may only be conducted where:

a) the query relates to a victim in relation to any of the permitted purposes in Part 4, or to a person who is otherwise at risk of harm, or has suffered harm; or

b) the query relates to a person of interest in relation to:

(i) an offence under the general law enforcement purpose, other than terrorism offences, in which case images of persons aged 14 years or over may be returned, or

(ii) a terrorism offence or national security investigation, in which case images of persons aged 10 years or over may be returned.

5.16 Agencies must ensure they have adequate safeguards and policies in place that will address any risks associated with matching the images of minors.

Note: Review of the post-query authorisation model will be undertaken by the Coordination Group as part of its 12-month review referred to in clause 4.25 of the IGA.

Authorising officers

5.17 An Authorising Officer must be an officer holding the position of:

(i) For a policing agency:
   a. commissioned officer rank (or equivalent); or
   b. unsworn individuals pursuant to current respective police force oversight arrangements

(ii) for all other Participating Agencies, Executive Level 2 or equivalent or higher.

5.18 Authorising Officers not only authorise transactions but are responsible for acting to address any unauthorised use by the Nominated Users under their supervision.

5.19 Where an Authorising Officer is also a Nominated User, they cannot approve their own query.

PART 6 - ACCESS CRITERIA

6.1 Prior to the Hub Controller granting access to the FIS and to maintain access to the FIS, agencies must comply with the following access criteria:

FMS Participation Agreement and Participant Access Arrangements

6.2 Agencies must enter into the common Face Matching Services Participation Agreement (PA) to become Participants in the FIS.

6.3 Participants must also enter into a Participant Access Arrangement (PAA) which forms part of the PA. Each Participant's PAA outlines the specific types of information to be made available via the FIS and the level of service that the Hub Controller agrees to provide to the Participant. Contents of the Participant Access Arrangement will be subject to negotiation between the Participants and the Hub Controller and must be consistent with this Access Policy.

6.4 The Hub Controller maintains a template PAA for use by Participants participating in the FIS that meets the requirements of this Access Policy. The Hub Controller must also maintain a register of all completed PAAs.

Legislative Authority

6.5 Participants must provide a statement referencing the legislation that provides their legal basis for collecting, using and disclosing personal information via the FIS. This statement should form part of the Participant's PAA.

Privacy Impact Assessments

6.6 Where a Participant's use of the FIS is not exempt from the relevant Commonwealth, State or Territory privacy laws, the Participant must undertake or contribute to a privacy impact assessment (PIA), a systematic assessment of the sharing of Identity Information between a Data Holding Agency and a Requesting Agency under an actual or proposed Participant Access Arrangement for the purpose of identifying any impacts on the privacy of individuals, and making recommendations for managing, minimising or eliminating any impacts identified, and that is conducted in accordance with the Office of the Australian Information Commissioner's Guide to Undertaking Privacy Impact Assessments.

6.7 The PIA must account for every information flow that occurs through the FIS, to which the Participants are a party. PIAs must be undertaken prior to the finalisation of the PAA and must consider the information sharing processes that are likely to occur under the PAA. Participants should refer to the Office of the Australian Information Commissioner's (OAIC) guidelines in conducting PIAs. PIAs should be conducted independently unless it is not feasible to do so.

6.8 Where a Participant's use of the FIS is exempt from the relevant Commonwealth or State and Territory privacy laws, the Participant must develop a privacy statement outlining the legislative, policy and other

safeguards that apply to the handling of personal information to be obtained using the FIS. This privacy statement should be provided to the Data Holding Agency and the Hub Controller.

Scope of data sharing

6.9 The Requesting and Data Holding Agencies should clearly understand the scope of the proposed data sharing via the FIS. For each data source that is to be accessed, Participants must record in their PAAs:

a) the type of information provided in response to FIS requests for each function and data source, including:

(i) the number of images that may be returned in responses to standard requests (up to a maximum of 20); and

(ii) the maximum number of images that may be shortlisted, to disclose biographic details, when reviewing image galleries.

b) the permitted purposes (under Part 4) for which FIS requests can be submitted

c) the characteristics (for example, security clearance and/or training) relating to agreed categories of Nominated Users (Role Types) and access permissions associated with each Role Type

d) the maximum number of Nominated Users for each data source and each Role Type

e) the agreed maximum number of transactions, expressed in terms of total estimated transactions annually, and estimated peak transaction rates per month (or other agreed time period);

f) the application of authorisation requirements, including:

(i) the types of queries for which authorisation is required, including any modification to the standard authorisation requirements of this Access Policy

(ii) the Role Types, if any, to have access privileges to receive larger galleries

6.10 This information must be provided to the Hub Controller in a format that enables implementation of the agreed data sharing via the Hub. Any changes to the matters above should be notified to the Data Holding and Requesting Agencies as soon as practicable. Such changes will also require a variation of the PAA, a copy of which must be retained by the Hub Controller.

Protection and use of personal information

6.11 Participants must record in their PAAs the arrangements for the protection of personal information that will be shared via the FIS, including:

a) arrangements for the retention and destruction of any images or other identity information obtained via the FIS, and

b) the circumstances where any release of identity information to third parties may occur, if at all.

6.12 Requesting Agencies must acknowledge that the FIS is designed to assist, but not replace, existing processes and procedures for determining a person's identity and that the Requesting Agencies are responsible for the information they access through the FIS and decisions they make using identity information or results obtained through the FIS.

Management of Nominated Users and Authorising Officers

6.13 Only Nominated Users may submit queries via the FIS. Requesting Agencies must ensure that they only appoint as Nominated Users employees who have a specialist investigative, intelligence, incident response, forensic, or operational security function and who have a reasonable need to access the FIS to perform their functions and activities with the agency. The level of FIS access must be commensurate with the requirements of their functions and activities.

6.14 For security reasons, a Nominated User must not be provided with access to the FIS and FVS concurrently, for the same data source(s), and must have an appropriate security clearance of:

a) for Australian Government personnel, Baseline clearance or higher; or

b) for state and territory personnel an equivalent clearance consistent with the Australian Government Personnel Security Protocol of the Australian Government Protective Security Policy Framework, Baseline clearance requirements, as approved by the Governing Body.

6.15 Exceptions may be made to the security clearance requirements for certain, limited number of staff in Data Holding Agencies providing technical support.

6.16 Authorising Officers and Supervising Officers are provided with access to the Portal to assist in fulfilling their obligations under this Access Policy.

6.17 The addition and removal of Nominated Users, Supervising Officers and Authorising Officers is managed by a dedicated Senior Client Administrator in each Requesting Agency, in conjunction with the Hub Controller. Participants should record and advise each other and the Hub Controller of the persons who are responsible for managing Nominated Users, Supervising Officers and Authorising Officers and ensuring compliance with the requirements of this Access Policy.

6.18 Requesting Agencies must maintain a register of Nominated Users, Supervising Officers and Authorising Officers for oversight and auditing purposes. Subject to any overriding legislative obligations, the register must not be made publicly available. Requesting Agencies must reconfirm the basis for each of their Nominated Users to access the FIS at 90-day intervals and Supervising Officers and Authorising Officers to access the FIS at 180 day intervals.

6.19 Once a Nominated User, Supervising Officer or Authorising Officer no longer requires access to the FIS, Participants must take reasonable steps to advise the Hub Controller and ensure that their access to the service is terminated.

Training of Nominated Users and Authorising Officers

6.20 Nominated Users and Authorising Officers must be trained in security awareness and privacy obligations (this may already occur as part of their ongoing employment). To gain access to the FIS, Nominated

Users and Authorising Officers must be trained in how to use the Portal, including how to interpret the results of the FIS. Common training materials relating to the Hub are developed and maintained by the Hub Controller and made available for these purposes.

6.21 Nominated Users must undergo facial recognition and image comparison training in accordance with the Face Matching Services Training Policy.

6.22 It is the responsibility of the Requesting Agency to ensure Nominated Users are appropriately trained to interpret FIS results and to provide assurances to this effect to the satisfaction of the Data Holding Agency. Where necessary, Data Holding Agencies may specify additional training requirements in PAAs.

Auditing and Accountability

6.23 A Requesting Agency must audit all its data sharing via the FIS at least once every financial year. These audits should be conducted by an independent auditor, or a business unit of the Requesting Agency that is functionally separate to any business unit using the service. The audit should be conducted to the satisfaction of each Data Holding Agency that the Requesting Agency has used. The Requesting Agency is responsible for its own audit costs.

6.24 Without limiting the scope of the audit, the audit report should examine the queries relating to the permitted purpose of community safety considering the greater privacy risk and whether authorisation was obtained for those circumstances that required authorisation.

6.25 Requesting Agencies must retain all necessary information to support audits of their use of the FIS. These information holdings should provide the ability to:

a) identify the time, Nominated User, purpose, internal reference number, and (where relevant) authorisation associated with each transaction;

    a. this information is available in the audit logs via the Portal;

b) demonstrate compliance with Nominated User access requirements;

c) demonstrate compliance with authorisation requirements

d) examine queries relating to the permitted purpose of community safety;

e) track the handling of any identity information provided as part of a transaction response, including whether and when the Participant stored or destroyed the identity information;

f) detect anomalous or potentially suspicious transactions or patterns of transactions;

    a. some of this information may need to be obtained from the Data Holding Agency; and

g) identify any complaints and review responses to them.

Security Accreditation

6.26 All Requesting Agencies must conduct a security risk assessment in a format approved by their internal information technology security adviser (or equivalent), a copy of which must be provided to the Hub Controller.

Transparency

6.27 Participants must ensure that information relating to their participation in the FIS is made publicly available.

6.28 This should include the publication of PIAs and details of legislative authority and may also include the PA where such publishing is practical for Participants. If a Participant does not publish these documents in full for security or other reasons, they should be published or made available upon request to the greatest extent possible. The Hub Controller maintains a public register listing the above documents and provides a link on its website to where Participants have published documents or their descriptions.

Where a Participant is not subject to Commonwealth, state or territory freedom of information laws, they are not required to publish documents under this Access Policy.

6.29 The Hub Controller will publish, on an annual basis, information on the usage of the FIS to enable the community to gain a broad understanding of the scope and volume of FIS use across Agencies. This information will include:

a) the Agencies that have made requests for access to the FIS

b) the number of instances that each Participating Agency requested information via the FIS, and

c) the number of those instances where the Participant received a response containing information in a government identification document, or confirmation of a person's identity.

6.30 Any use of the FIS by the Australian Security Intelligence Organisation will not be included in this reporting in order to protect that agency's operations.

PART 7 - GOVERNANCE FRAMEWORK FOR THE FIS

7.1 In accordance with the IGA, Ministerial responsibility for the Capability (including the FIS) sits with the Ministerial Council for Police and Emergency Management (MCPEM). The National Identity Security Coordination Group (the Coordination Group) is the officials-level body accountable to the MCPEM for the efficient and effective delivery and management of the FIS.

7.2 The Coordination Group is responsible for developing policy and procedures to support the operation of the FIS. It is also responsible for monitoring Participating Agencies' compliance with these policies and for taking appropriate action to address any non-compliance. The Coordination Group has in place advisory and consultation mechanisms to ensure its considerations are appropriately informed by the views of relevant stakeholder organisations.

7.3 This Access Policy has been informed by an initial, independent privacy impact assessment on the design and governance of the Hub, commissioned by the Hub Controller.

7.4 The Coordination Group monitors and reviews the operation of this policy and any supporting guidelines or procedures, updating them as required to help ensure that information sharing via the FIS continues to meet the objectives of all participants.

PART 9 - RESPONSIBILITY OF PARTICIPANTS

9.1 Participants sharing information via the FIS have the primary responsibility for ensuring that their participation in the service is conducted in accordance with this Access Policy.

9.2 It is the responsibility of the Participants sharing information via the FIS to ensure that their PIAs and the PAAs fulfil the Access Criteria. Participants are also responsible for developing business systems and processes to implement Access Criteria 6.12-6.27 including for identifying and promptly addressing any suspected or actual non-compliance.

9.3 Participants are responsible for ensuring that their PAAs with other Participants are consistent with the Access Policy, that they take steps to address any audit or compliance issues and ensure they have adequate privacy safeguards in place for the use of FIS.

9.4 It is the responsibility of Participants sharing information via the FIS to ensure they provide the Participant with which they have entered into a Participant Access Arrangement, any information that is necessary for them to fulfil the Access Criteria.

PART 10 - THE ROLE OF THE HUB CONTROLLER

10.1 The Hub Controller manages the Hub which supports the FIS and provides Secretariat support to the Coordination Group. In this capacity the Hub Controller is responsible for:

a) reviewing, coordinating and signing the PAAs entered into by Participating Agencies in order to be satisfied that they are consistent with this Access Policy;

b) reviewing audit and compliance reports to identify the potential need for compliance action, making recommendations to the Coordination Group as required; and

c) making recommendations to the Coordination Group for changes to this Access Policy to ensure the effective governance and operation of the FIS.

10.2 The Hub Controller is not responsible for endorsing the content of PIAs conducted on behalf Participating Agencies.

10.3 The Hub Controller retains discretion to determine the technical design of the FIS, including the Portal, while ensuring it remains consistent with the Principles and Access Criteria outlined in this policy. In doing so, the Hub Controller will consult closely with relevant Data Holding and Requesting Agencies with a view to reaching consensus agreement where possible.

10.4 The Hub Controller may exercise the discretion not to facilitate or modify or suspend; the sharing of information between Participants via the FIS.

10.5 This discretion is exercised in accordance with the FMS Compliance Policy and the FMS Participation Agreement developed and maintained by the Coordination Group.

Attachment A: Approved Agencies

This document lists those Agencies which have been approved to access the Face Identification Service (FIS), subject to their meeting the requirements of the FIS Access Policy.

Commonwealth Agencies

- Australian Border Force
- Australian Commission for Law Enforcement Integrity
- Australian Criminal Intelligence Commission
- Australian Federal Police
- Department of Foreign Affairs and Trade
- Department of Home Affairs – Australian Border Force
- Australian Security Intelligence Organisation

State and territory Agencies

Police Agencies

- New South Wales Police Force
- Victoria Police
- Queensland Police Service
- Western Australia Police Force
- South Australia Police
- Tasmania Police
- Northern Territory Police
- ACT Policing (AFP)

Crime and anti-corruption Agencies

- New South Wales Independent Commission Against Corruption
- New South Wales Law Enforcement Conduct Commission
- New South Wales Crime Commission
- Victorian Independent Broad-based Anti-corruption Commission
- Queensland Crime and Corruption Commission
- Western Australian Corruption and Crime Commission
- South Australian Independent Commissioner Against Corruption
- Tasmanian Integrity Commission
- Northern Territory Independent Commissioner Against Corruption