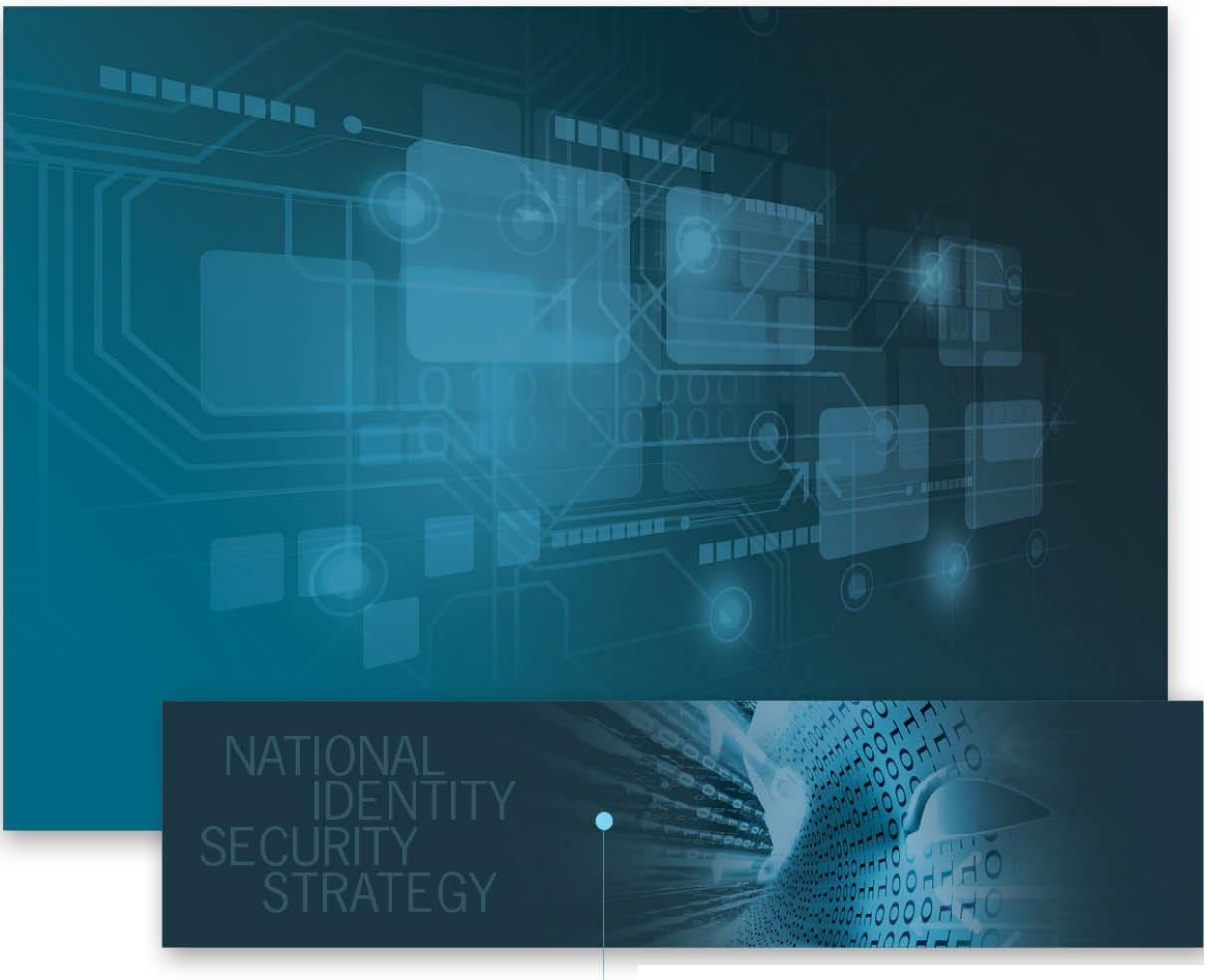

Face Verification Service (FVS) Access Policy

National Facial Biometric Matching Capability

IDENTITY SECURITY

Contents

FACE VERIFICATION 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 Verification Service (FVS).

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 FVS

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

2.2 The NFBMC 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 FVS enables a facial image or biographic information associated with an individual to be compared, on a one-to-one basis, against an image and/or biographic information held on a specific government record associated with that same individual to help verify that person's identity.

2.4 The FVS can perform the following functions:

a) **Match function**
This function allows a Nominated User to submit a person's document number, facial image and biographic details to a Data Holding Agency's data source(s) to verify that person's government identification documentation.

b) **Retrieve function**
This function allows a Nominated User to submit a person's document number and biographic details to a Data Holding Agency's data source(s) to retrieve either that person's facial image, that person's biographic details, or both.

c) **Search function**
This function allows a Nominated User to submit a person's facial image and biographic details to the Data Holding Agency's data source(s) to verify that person's government identification documentation.

2.5 While the functions of the FVS provide the option to return responses that include biographic details, this optional functionality can only be implemented with the agreement of the relevant Data Holding Agency via the FMS Participant Access Arrangement.

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

2.7 Over time, the Hub will also be able to receive queries via system-to-system connections with Participating Agencies' existing systems, using industry standard integration technologies such as web services. It is anticipated that the bulk of transactions to the Hub will be from identity document issuing Participants that will be sending identity verification queries from their systems to the Hub using web services (System-to-system connections).

2.8 An administration facility for the FVS is provided through the Portal. This facility enables the ability to add, manage (including password reset, access support, and access re-authorisation) and remove Nominated Users who can access the FVS. It provides the ability for Agencies to generate reports, perform audit queries of Nominated User activities and download audit data.

PART 3 - ACCESS CRITERIA

3.1 Prior to the Hub Controller granting access to the FVS, and to maintain that access, agencies must comply with the following access criteria.

FMS Participation Agreement and Participant Access Arrangements

3.2 Agencies must enter into the common Face Matching Services Participation Agreement (PA) to participate in the FVS.

3.3 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 FVS, as well as the level of service that the Hub Controller agrees to provide to the Participant. Contents of the PAA will be subject to negotiation between the Participants and the Hub Controller and must be consistent with this Access Policy and the PA.

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

Legislative Authority

3.5 Participating Agencies must provide a statement referencing the legislation that provides their legal basis for collecting, using and/or disclosing identity information via the FVS. This statement should form part of the Participant's PAA.

Privacy Impact Assessments

3.6 Where a Participant's use of the FVS 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.

3.7 The PIA must account for every information flow that occurs through the FVS, to which the Participant is 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 when conducting PIAs. PIAs should be conducted independently unless it is not feasible to do so.

3.8 Where a Participant's use of the FVS 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 FVS. This privacy statement should be provided to the Data Holding Agency and the Hub Controller.

Scope of data sharing

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

a) the type of identity information provided in response to FVS queries for each function and data source;

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

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

d) the method of access to the FVS for each Role Type (e.g. through the Portal, or via a system-to-system connection); and

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).

3.10 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

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

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

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

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

Management of Nominated Users

3.13 Only Nominated Users may submit queries via the FVS. Requesting Agencies must ensure that they only appoint as Nominated Users employees with a reasonable need to access the FVS to perform their functions and activities within the Agency. Any information technology (IT) system that the Requesting Agency proposes to be a Nominated User must have a reasonable need to use the FVS to perform operations required by the Requesting Agency. In both cases, the level of access must be commensurate with the requirements of those functions and activities.

3.14 With the exception of Nominated Users whose sole function is sanitise the data to protect legally assumed identities, for Security reasons, a Nominated User must not be provided with access to the FIS and FVS concurrently, for the same data source(s).

3.15 The addition and removal of Nominated Users is managed by a dedicated Client Administrator in each Requesting Agency and occurs through administration facility. Participants should record and advise each other of the person who is responsible for managing Nominated Users and ensuring compliance with the requirements of this Access Policy.

3.16 Requesting Agencies must maintain a register of Nominated Users 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 FVS every 180 days.

3.17 Once a Nominated User no longer requires access to the FVS, Participants must take reasonable steps to advise the Hub Controller and ensure that their access to the service is terminated.

Training of Nominated Users

3.18 Nominated Users must be trained in security awareness and privacy obligations (this may already occur as part of their ongoing employment). To gain access to the FVS, Nominated Users must be trained in how to use the Portal, including how to interpret the results of the FVS. Common training materials relating to the Hub are maintained by the Hub Controller and made available for these purposes.

3.19 Nominated Users that receive a facial image in response to a query must undergo facial recognition and image comparison training in accordance with the Face Matching Services Training Policy.

Auditing and Accountability

3.20 A Requesting Agency must audit all its data sharing via the FVS at least once every financial year. These audits should be conducted independently, unless it is not feasible to do so, and should be conducted to the satisfaction of each Data Holding Agency to which the Requesting Agency has conducted transactions. The Requesting Agency should be responsible for its own audit costs.

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

a) identify the time, purpose and Nominated User associated with each transaction;

- this information is available in the audit logs via the Portal

b) track the handling of any identity information provided as part of a response, including whether the Agency stored or destroyed the identity information;

c) detect anomalous or potentially suspicious transactions or patterns of transactions; and

- some of this information may need to be obtained from the Data Holding Agency

d) identify any complaints and review responses to them.

Security Accreditation

3.22 Prior to connecting an information technology system to the Hub using a system-to-system connection, Participants must prepare and implement a Security Risk Management Plan, and either: prepare and implement a System Security Plan; or receive a Security Accreditation Certificate and provide a copy of it to the Hub Controller.

3.23 Participants that intend to access the FVS through the Portal only 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

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

3.25 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.

3.26 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.

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

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

b) the number of instances that each Participant requested information via the FVS, 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.

3.28 Any use of the FVS by the Australian Security Intelligence Organisation will not be included in this reporting to protect that Agency's operations.

PART 4 - GOVERNANCE FRAMEWORK FOR THE FVS

4.1 In accordance with the IGA, Ministerial responsibility for the NFBMC, including the FVS, 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 FVS.

4.2 The Coordination Group is responsible for developing policy and procedures to support the operation of the FVS. It is also responsible for monitoring Participants' 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.

4.3 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.

4.4 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 FVS continues to meet the objectives of all participants.

PART 5 - RESPONSIBILITY OF PARTICIPANTS

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

5.2 It is the responsibility of the Participants sharing information via the FVS to ensure that their PAAs fulfil the Access Criteria. Participants are also responsible for developing business systems and processes to implement Access Criteria 3.12-3.21, including for identifying and promptly addressing any suspected or actual non-compliance.

5.3 Participants are responsible for ensuring that their PAAs 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 FVS.

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

PART 6 - THE ROLE OF THE HUB CONTROLLER

6.1 The Hub Controller manages the Hub which supports the FVS 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 FVS.

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

6.3 The Hub Controller retains discretion to determine the technical design of the FVS, including the Portal, to enhance the functionality of the service while ensuring it remains consistent with this Access 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.

6.4 The Hub Controller may exercise discretion not to facilitate or to modify or suspend the sharing of information between participating Agencies via the FVS.

6.5 This discretion must be exercised in accordance with the FMS Compliance Policy and the PA developed and maintained by the Coordination Group.