BAINBRIDGE
associates

March 2019

AUSTRALIAN GOVERNMENT
DEPARTMENT OF HOME AFFAIRS

Privacy Impact Assessment: Law Enforcement, Crime and Anti-Corruption Agency use of the Face Matching Services, NFBMC (v.1.0)

FOR OFFICIAL USE ONLY

This page left blank intentionally

Table of Contents

Glossary and Acronyms

ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
AGD	Attorney-General's Department
Agency	any agency, government sector agency, public sector agency or public sector body as defined in the *Public Service Act 1999* (Cth) or equivalent state or territory public service legislation, including any Road Agency, law enforcement agency or relevant Commonwealth agency that is participating in or may wish to participate in the NFBMC
APP Code	*Privacy (Australian Government Agencies – Governance) APP Code 2017*
APPs	Australian Privacy Principles (Cth)
Biographic information	biographic identity information pertaining to an individual, such as name and date of birth
Biometric indicator	any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification. Biometric indicators can be physiological or behavioural. An image of a person's face is a physiological biometric
Biometric template	produced by face recognition system following: a) capture of nodal points of an individual's facial image; and b) application of algorithms to the nodal points to create a unique file (biometric template) that can be stored within the face recognition system
Biometric information	defined as a form of sensitive information under the Privacy Act, includes biometric information *and* biometric template information on the basis that both have the capacity to identify or verify an individual.[1]
COAG	Council of Australian Governments
CSP	Contracted Service Provider
DFAT	Department of Foreign Affairs and Trade
DHA	Data Holding Agency
Data Holding Agency	a Participant that contributes Identity Information used in the Services to provide Responses to Queries from Requesting Agencies
Data Hosting Agency	the Agency of the Commonwealth of Australia responsible for managing and operating the NDFLRS where it holds a replicated copy of Identity Information contributed by Road Agencies; currently Home Affairs
Data Source	a database of Government Identification Documentation
Document Repository	the online secure portal comprising the document repository maintained by the Framework Administrator containing definitive versions of documents relating to the NFBMC
DVS	Document Verification Service

[1] While state and territory privacy legislation contain additional protections for information defined as 'sensitive' or 'health information', they do not include 'biometric information' or 'biometric templates' within their definitions.

Face Identification Service	as specified in the FMS Catalogue, which enables a facial image to be compared against multiple images held on a database of government records to establish an individual's identity
Face Verification Service	Face Verification Service As specified in the FMS Catalogue, which enables a Facial Image associated with an individual to be compared against a Facial Image held on a specific government record associated with that same individual to verify or confirm that individual's identity
Facial Image	includes digital photographs, live capture images, scanned photographs and other technical information related to those images (such as the time and date of capture and data capture standards used)
Facial Recognition System	a Data Holding Agency's (or, in the case of NDFLRS, the Data Hosting Agency's) system, which includes face detection, quality assessment, face template creation and identification components that enable requests for verification and/or identification and provides results to the Nominated User or system that made the request
FIS	Face Identification Service
FMS	Face Matching Service in the FMS Catalogue, including FIS, FRAUS, FVS and OPOLS
Framework Administrator	the Commonwealth, or any replacement entity appointed by the Governing Body, in its capacity as the Participant administering the FMS Participation Framework
FRAUS	Facial Recognition Analysis Utility Service
FVS	Face Verification Service
Governing Body	National Identity Security Coordination Group (NISCG)
Government Identification Documentation	any document or record, whether in physical or electronic form, containing Identity Information issued by a government body or entity
Home Affairs	Department of Home Affairs
Hub	Interoperability Hub
Hub Access Participant	A Data Holding Agency or a Requesting Agency that has access to the Interoperability Hub under a Participant Access Agreement
Hub Controller	the Commonwealth in its capacity as the Participant controlling and administrating the Interoperability Hub (or, as relevant, any replacement entity appointed by the Governing Body)
Identity Information	information, or a document, relating to an individual (whether living, dead, real or fictitious) that is capable of being used (whether alone or in conjunction with other information or documents) to identify or purportedly identify the individual
IDMS Administrator	the Hub Controller's organisational unit responsible for managing the Interoperability Hub, applicable Services, and Users accessing them
IGA	Intergovernmental Agreement
IMS	Identity Matching Services
IMSB	*Identity-Matching Services Bill 2018*

Information Security Manual	in relation to a Participant, either: a. The Australian Government Information Security Manual, which governs the security of government ICT systems, as produced and updated from time to time by the Australian Signals Directorate; or b. An alternate information security controls and guidance approved by the Framework Administrator
Intergovernmental Agreement	Intergovernmental Agreement on Identity Matching Services (5 October 2017)
Interoperability Hub	the technical system that provides a mechanism for the secure and auditable transmission of Facial Images and associated information
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
KYC	Know Your Customer
LECAC agencies	Law Enforcement, Crime and Anti-Corruption Agencies
Legally Assumed Identity	an assumed identity acquired under Part IAC of the *Crimes Act 1914* (Cth) or a corresponding assumed identity law, the *AFP Act 1979* (Cth), the *Witness Protection Act 1996* (Cth) or a corresponding witness protection program conducted by a state or territory under a complementary witness protection law
Match	means that a Facial Recognition System identifies a Facial Image (or relevant Biographic Information) in a relevant Data Source as matching relevant identity information in a Query
Match Candidate	a potential Match, which has a Match Score above the Matching Threshold
Match Function	the function of the FVS that allows an authorised user to submit a document number, individual's Facial Image and required Biographic Information to a Data Holding Agency's Data Sources to confirm whether it matches the individual's Government Identification Documentation
Match Score	a score determined by an algorithm within a Facial Recognition System that quantifies the assessed probability that a Facial Image (or as relevant Biographic Information) in a relevant Data Source matches relevant Identity Information submitted in a Query
Matching Threshold	the Match Score that must be achieved or exceeded for a Facial Recognition System to consider a Facial Image (or as relevant Biographic Information) in a relevant Data Source as being a Match Candidate for relevant Identity Information in a Query
MCPEM	Ministerial Council for Police and Emergency Management
National Driver Licence Facial Recognition Solution	the technology system by which Facial Images used on driver licences and other state and territory government issued documents may be accessed via the Services
NDLFRS	National Driver Licence Facial Recognition Solution
NISCG	National Identity Security Coordination Group, the body responsible to the MCPEM for the management of the Identity Matching Services

	defined in the IGA
NIST	National Institute of Standards and Technology (United States)
NFBMC	the National Facial Biometric Matching Capability, which comprises infrastructure, legislative and governance arrangements that enable the sharing and matching of Identity Information by Participants
NISS	National Identity Security Strategy
NSWPF	New South Wales Police Force
OAIC	Office of the Australian Information Commissioner
OPOLS	One Person One Licence Service
PAA	Participant Access Arrangement
Participant	a Party to the FMS Participation Agreement
Participant Access Arrangement	an arrangement formed between the Hub Controller, a Requesting Agency and one or more Data Holding Agencies (or the Hub Controller on their behalf), in relation to the Interoperability Hub and agreed Data Sources
PAA	Participant Access Arrangement
PbD	Privacy by Design
Personal information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: a) whether the information or opinion is true or not; and b) whether the information or opinion is recorded in a material form or not
PIA	Privacy Impact Assessment
POI	Person of interest
Portal	the user interface associated with the Interoperability Hub that allows Users to access Services or perform administrative functions
Privacy Act	*Privacy Act 1988 (Cth)*
Privacy Governance Framework and Management Standards	means: a) the Privacy Management Framework issued by the OAIC; or b) the framework of a state or a territory that sets out comparable standards to the OAIC's Privacy Management Framework, which must c) embed a culture of privacy that enables compliance; d) establish robust and effective privacy practices, procedures and systems; e) evaluate privacy practices, procedures and systems to ensure continued effectiveness; and f) enhance responses to privacy issues
Privacy Impact Assessment	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.
Protective Security Policy Framework	means the Protective Security Policy Framework maintained by the Attorney-General's Department, which sets out policy, guidance and better practice advice for governance, personnel, physical and information security, and which includes mandatory requirements to assist Agency heads to identify their responsibilities to manage security risks to their people, information and assets, as amended or replaced from time to time
PSPF	Protective Security Policy Framework
Query	means Identity Information submitted by a Requesting Agency either through the Portal or by a system-to-system connection that is intended to be compared against the Identity Information held in a Data Source
QPS	Queensland Police Service
RA	Requesting Agency
Requesting Agency	a Participant that submits a Query to a Data Holding Agency via the Interoperability Hub under a Participant Access Arrangement
Response	means Identity Information or a system response sent by a Data Holding Agency via the Interoperability Hub to a Requesting Agency in response to a Query submitted by that Requesting Agency
Retrieve Function	means the function of the FVS that allows an authorised user to submit a document number and person's Biographic Information to a Data Holding Agency's Data Source(s) to retrieve either that person's Facial Image, that person's Biographic Information, or both
Search Function	means the function of the FMS that allows an authorised user to submit a person's biographic details and Facial Image to the Data Holding Agency's Data Sources to verify that person's Government Identification Documentation held on that Data Source
Security Classification	means, in relation to a piece of information, the security classification designated by the Commonwealth and/or a state or territory of Australia as applicable
Sensitive information	means: a) information about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record;

	that is also personal information; or b) health information about an individual; or c) genetic information about an individual that is not otherwise health information or d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or e) biometric templates
Statement of Legislative Authority	means a detailed explanation of the legislative provisions and other relevant information that a Participant believes establishes that: a) where the Participant is a Requesting Agency, that its access to a specified Data Source via the relevant Services (including its submission of Queries and receipt and use of Responses) will be lawful; or b) where the Participant is a Data Holding Agency, that its provision of (and, as relevant, its offer to provide) access to a specified Data Source via the relevant Services will be lawful
Transaction	means both a Query and a Response sent through the Interoperability Hub

Executive Summary

Bainbridge Associates was commissioned by the Commonwealth Government to undertake a Privacy Impact Assessment (PIA) of Law Enforcement, Crime and Anti-Corruption (LECAC) agencies' proposed access to, and use of, the Face Verification Service (FVS) and Face Identification Service (FIS) provided under the National Facial Biometric Matching Capability (NFBMC).

The LECAC PIA was commissioned as a multi-party PIA to assess LECAC agencies' use of the FVS and FIS, considering LECAC information flows against the requirements of the Australian Privacy Principles (APPs) contained in Schedule 1 of the *Privacy Act 1988* (Cth). It is intended to fulfil the requirement imposed on LECAC agencies to undertake a PIA as a pre-condition to gaining access to the FVS and FIS. It is the sixth PIA to be undertaken in relation to the NFBMC, following an iterative PIA process aligned with the system development process. This PIA is focused upon LECAC agencies and related information flows only. A comprehensive NFBMC PIA will be commissioned prior to full implementation.

Findings and recommendations from the LECAC PIA process are documented in this PIA report. The recommendations must be actioned appropriately by the Department of Home Affairs (Home Affairs) and/or LECAC agencies in order to ensure that LECAC agency access to, and use of, the FVS and FIS meets the best practice privacy controls adopted by the NFBMC.

Key Findings

Home Affairs

The PIA finds that Home Affairs has undertaken a rigorous and systematic approach to identifying, mitigating or otherwise seeking to manage the privacy risks associated with the FVS and the FIS. This approach is consistent with obligations under the IMS IGA to ensure that the sharing and matching of identity information on a national basis will be subject to 'robust privacy safeguards'.

Home Affairs developed an FMS Data Sharing Framework to operationalise the Identity Matching Services (IMS) Intergovernmental Agreement (IGA), instantiating the intention of the parties to the IGA to build privacy into the NFBMC. The FMS Data Sharing Framework (including the FMS Participation Agreement, FVS Access Policy, FIS Access Policy, Compliance Policy and Training Policy) identifies a range of privacy and security controls and imposes privacy requirements upon LECAC agencies. Looked at in context, implementation of the FVS and FIS will encompass a multi-faceted approach to privacy, involving a complex and interlocking set of legislative, contractual, governance, technical, policy and security measures.

Home Affairs commissioned a single, multi-party PIA process for all LECAC agencies. This approach is provided for under the FMS Participation Agreement, subject to the stipulation that the PIA specifically addresses each agency's proposed use of the FVS and FIS. For the reasons outlined below, and detailed in the LECAC PIA report, this approach proved to be misconceived.

LECAC Agencies

Overall, the PIA finds that it is possible for LECAC agencies as a group to meet relevant privacy requirements set out in the FMS Data Sharing Framework, but further work is required to demonstrate how this will be achieved in practice.

In relation to LECAC agencies, the PIA finds that:

- it is intended that LECAC agency access to, and use of, the FVS and FIS will be supported by appropriate and specific legislation (i.e. 'authorised by law');
- implementation of LECAC agency access to the FVS and FIS will be staggered across Australia, making it difficult to obtain a full view of requisite information flows and standard operational procedures during the PIA process;
- there is variation in the authorising, privacy and protective security legislation and policy frameworks across the jurisdictions; this variation proved to be an impediment to a multi-party PIA process;
- the FMS Data Sharing Framework specifies a comprehensive range of privacy and security requirements and controls, ranging from legal, technical, and policy through to administrative; it has the capacity to provide a form of 'functional equivalence' across a federal system in which different privacy and protective security laws, standards and policies apply to federal, state and territory LECAC agencies; and
- while there is a degree of variation in the legal, privacy and security frameworks applicable to each agency, these frameworks nevertheless provide the foundation for the demonstration of effective privacy and security management within each jurisdiction; if a 'functional equivalence' approach is adopted by LECAC agencies, it will result in the effective operationalisation of FVS and FIS privacy and security measures (i.e. privacy in practice).

The LECAC PIA report provides a high-level assessment of LECAC agencies' proposed use of the FVS and FIS, based upon generic information flows, and informed by LECAC agencies' feedback.

'Exempt' LECAC Agencies to Develop Privacy Statements

The LECAC PIA was required to consider all LECAC agencies, including those that are fully exempt from privacy legislation. The FMS Participation Agreement provides for exempt agencies – usually 'CAC' (crime and anti-corruption) agencies – to develop a privacy statement rather than conduct or participate in a PIA process. The PIA finds that this is the preferred approach for fully exempt agencies. The PIA recommends that each exempt agency should develop an agency-specific privacy statement outlining how it will ensure appropriate privacy and protective security practices. The LECAC PIA report may contain relevant or useful information to inform the development of privacy statements.

FMS Data Sharing Framework and Privacy Management

The FMS Data Sharing Framework identifies a number of privacy and security controls to address potential FVS and FIS privacy risks. Each agency – to the degree that it is possible or relevant to do so – needs to demonstrate how it will comply with and operationalise these privacy requirements and controls. In most cases, agencies may refer to existing processes or procedures rather than privacy legislation. In other cases, new processes or procedures will need to be developed. Some measures require Home Affairs to take the initiative.

The PIA finds that *a combination of proposed and existing* arrangements, policies and procedures have the capacity to be adopted and/or used to demonstrate alignment between FVS and FIS privacy requirements and LECAC agency operations. For example:

- the negotiation of individual Participant Access Arrangements (PAA) will require agencies to document their particular access arrangements and the legal basis for the collection, use and disclosure of personal information;
- the incorporation of privacy requirements into LECAC agency operational policies and procedures (e.g. Police Manuals, privacy incident management or data breach policies) has the capacity to operationalise privacy requirements in a practical way, aiding privacy risk management overall; and
- the adoption of a formal privacy management framework (as required under the FMS Data Sharing Framework) will help to ensure consistency in approach across the various LECAC agencies.

The PIA supports the re-use of existing policies and procedures. It does not support the development of bespoke or stand-alone privacy compliance programs as this is more likely to fragment or separate privacy compliance from a LECAC agency's general compliance framework.

The PIA finds that privacy management, rather than privacy legislation, should comprise the focus of LECAC agency compliance efforts. Additionally, as outlined below, the PIA identified specific issues relating to privacy legislation and the FMS Participation Agreement that may, in fact, mandate a focus upon privacy management. The PIA report contains practical advice to help agencies identify, document and operationalise their approaches to privacy protection, adopting a privacy management framework approach. Where 'early adopters' develop relevant processes, these should be shared. For example, Victoria Police's process for the triaging of FIS queries provides a suitable model for other agencies to consider. This will also help to promote consistency.

As discussed in this report, appropriate operationalisation of the privacy requirements and controls contained in the FMS Data Sharing Framework and associated policies and arrangements will assist with privacy risk management.

Implementation of the NFBMC as a whole will introduce a number of privacy improvements, particularly in relation to data quality and data security. Subject to the recommendations contained in this report being actioned appropriately, there should also be improvements in relation to openness, transparency and accountability.

Role of Privacy Legislation within the FMS Data Sharing Framework

The FMS Data Sharing Framework incorporates multiple references to privacy legislation and privacy principles. These are intended to provide the foundation for LECAC agency privacy compliance and management.

If privacy legislation and the privacy principles enshrined within them were uniform across Australia, this would produce a substantial and straightforward legislative framework against which LECAC information flows and privacy risk management could be measured. However, not only is there a 'patchwork' of privacy legislation across Australia (and in some cases, no legislation), incorporating different privacy principles and covering different organisations or types of information – LECAC agencies are not covered by privacy legislation to the same degree as other agencies by virtue of their status as law enforcement, crime and anti-corruption agencies.

Where privacy legislation applies to LECAC agencies, they are provided with a range of privacy exemptions or exceptions on public interest grounds (either in whole, partially or within the privacy principles). This recognises that information privacy is not absolute and may need to be assessed against a range of countervailing public interests – in

particular, law enforcement activities or the regulatory objectives of government – which may override the application of privacy legislation or privacy principles.

While some form of law enforcement exemption or exception is necessary in order to ensure LECAC agencies are able to perform their functions and duties, there is no standard agreement as to the breadth of exemption required, resulting in *a diversity of* exemptions and exceptions. This does not cause specific issues to arise within a jurisdiction, but it does pose difficulties for the implementation of a collaborative, federal scheme like the NFBMC. This is further reason why the LECAC PIA report finds that privacy management, rather than privacy legislation, should be the focus of LECAC agency use of the FVS and FIS.

FVS and FIS Information Flows

Detailed FVS and FIS information flows, specific to each LECAC agency, were not available for the LECAC PIA. Based upon the high-level information that was provided, the PIA finds that the information flows to be supported by the FVS and FIS are, by design, limited, fully defined, and tightly constrained (on both a technical and policy level). Overall, this will reduce the degree of privacy risk involved in implementation of the FVS and FIS. For example:

- when LECAC agencies use the FVS or FIS as part of an investigation, it will represent one specific aspect of that investigation only; it will not displace existing investigatory processes;
- responses to FVS or FIS queries will not establish identity or guilt or provide sufficient evidence to obtain a warrant in their own right. They may contribute to the development of a case in which, for example, a witness or person of interest identified through the FIS, may become a suspect with the addition of further information (such as phone call records); and
- where previous PIA processes have identified specific privacy risks – for example, in relation to metadata or the matching of images of children or young people – Home Affairs has taken steps to address those risks.

To a large degree, proposed use of the FVS will be consistent with existing verification processes, checks and balances, while the FIS will be subject to stringent additional requirements. The PIA finds that a distinction should be maintained between the FVS and FIS, i.e. they should not be conflated under the single umbrella term of 'Face Matching Services' (or FMS). There are important differences between the FVS and FIS, which impact upon the degree of potential privacy perceptions and risks. The PIA finds that the FVS is closer to the (non-biometric) DVS in that both are concerned with the verification of identity. The FIS's focus upon identification (one-to-many) puts it into a different category altogether, which is why access to the FIS is limited to specific agencies and incorporates additional compliance requirements. Maintaining specific references to the 'FVS' and 'FIS' will help to ensure that issues and risks specific to the FIS are not extended uncritically or inaccurately to the FVS, and vice versa.

The PIA finds that the technology under consideration – biometrics – may be more controversial than its proposed utilisation by LECAC agencies, at least within the *specific, restricted context* of the LECAC PIA. The PIA finds that this is compounded by a lack of information in the public arena about the NFBMC, which has contributed to misunderstandings or inaccurate assumptions (for example, that the 'FMS' will provide real-time, many-to-many matching). Further information about the NFBMC can and should be provided to the community, subject to any operational sensitivity.

Biometric Face Matching Privacy Risks

The PIA identified a range of general and specific privacy risks associated with LECAC agency use of a biometric face matching system. These include *actual* privacy risks as well as *perceived* privacy risks. Both types of risk have the potential to undermine community confidence in the deployment of the FVS and FIS.

The PIA finds that these should not pose a significant risk to LECAC agency use of the FVS and FIS, provided appropriate privacy management measures are put into place and there is a willingness for LECAC agencies to take account of a number of important privacy perception issues documented in this report. One of the most significant privacy impacts – the re-purposing of passport, visa, citizenship and driver licence data for the purposes of the NFBMC – falls outside of the scope of the LECAC PIA.

Iterative ('Privacy by Design') PIA Process

In developing the NFBMC, the Commonwealth made a commitment to 'privacy by design', including its incorporation as a guiding principle within the IGA and the commissioning of PIAs as a key risk management tool during the build of the various components of the NFBMC. While a 'privacy by design' approach was clearly intended to embed privacy within the NFBMC, the decision to commission multiple, independent PIAs in alignment with the iterative build process has proved to be increasingly problematic over time.

Consistent with earlier PIA reports, the LECAC PIA finds that the iterative, 'privacy by design' approach taken to PIAs may be obscuring the privacy risks posed by the NFBMC as a whole. As a result, the final PIA proposed for the NFBMC will provide the first opportunity for the NFBMC to be examined 'end-to-end' and from a 'whole-of-lifecycle perspective', at the very end of the development process.

Based upon Bainbridge Associates' experience undertaking the LECAC PIA, it is considered that a tight focus upon 'in scope' issues – e.g. for the LECAC PIA this excluded consideration of technical, governance and/or legislative underpinnings because they have been subject to previous PIA processes – may meet the requirements of a specific PIA process but will not necessarily deliver 'privacy by design'.

In this context, Bainbridge Associates considers that assigning a privacy resource to work directly with LECAC agencies (e.g. through a working group or other collaborative mechanism), with the aim of embedding privacy and security requirements within standard operating procedures (or other relevant policies or processes), is likely to produce more meaningful and proactive privacy outcomes than an 'independent' PIA process. Future PIA processes should take this finding into account. At the very least, requisite information – such as data elements, information flows and relevant supporting documentation (e.g. standard operating procedures) – should be available at the beginning of the PIA process.

Governance, Transparency and Accountability

In addition to the specific LECAC issues outlined above, the PIA documents a number of other issues relating to governance, transparency and accountability that should be taken into account by LECAC agencies.

- There is increasing civil society, academic and community interest in biometric facial recognition systems. Government and LECAC agencies have a role to play in increasing information about their use of such systems.

- In order to promote transparency, increased and good quality information about the NFBMC should be made publicly available – for example, via an NFBMC website – including maximising the publication of PIA reports.
- In order to promote transparency and accountability, consideration should be given to:
    - the potential benefits that the adoption of algorithmic impact assessments could make within government;
    - other options to benchmark biometric face recognition system against other like systems and assess its accuracy (similar to the role played by National Institute of Standards and Technology (NIST) in the United States); and
    - completion of the NFBMC benefits realisation project and publication of its key findings (positive and negative).
- NFBMC Participants should consider reviewing/enhancing privacy governance at the executive level (Coordination Group) to reflect the high importance of privacy within the IMS IGA and the FMS Data Sharing Framework.
- NFBMC Participants should consider investigating further options to appoint independent members to the Coordination Group. This could include individuals with specific legal, privacy or protective security skills.

Consolidated Set of Recommendations

A consolidated set of recommendations is provided below. These are divided into recommendations addressed to LECAC agencies (12 recommendations), recommendations addressed to Home Affairs (8 recommendations) and three findings addressed to all Participants. Each recommendation contains a cross reference to the relevant section and page number for further reading.

General Recommendations – LECAC Agencies

Recommendation 1 – Exempt Agencies to Develop Privacy Statement
It is recommended that, consistent with clause 45.2 (p) of the Participation Agreement, LECAC agencies that are exempt from privacy legislation and privacy principles should develop a privacy statement, instead of relying upon a PIA. The privacy statement must: • outline the legislative, policy and other safeguards that apply to the handling of personal information to be obtained via the specific service; • be developed in consultation with the relevant Data Holding Agency or Agencies from which the information will be obtained; and • be approved by the Coordination Group. Section 3.3.2, p.39

Recommendation 2 – Privacy Governance Framework and Management Standards
Clause 16.4 (a) of the Participation Agreement requires each agency to develop (or amend) its Privacy Governance Framework and Management Standards to ensure that they are adequate and reflect the management of the flow of information through the FVS and FIS. The OAIC's *Privacy Governance Framework and Management Standards* provides a default approach to privacy management. Clause 16(b) provides that each LECAC agency must provide a copy of its Privacy Governance Framework and Management Standards to the Hub Controller upon

request.

It is recommended that all relevant LECAC agencies be required to demonstrate an effective approach to privacy governance and management prior to negotiating a Participation Access Arrangement. In particular, each LECAC agency must identify a suitable regulator within its jurisdiction that is capable of receiving and dealing with complaints.

Section 3.4, p.41

Recommendation 3 – Focus upon Operationalisation of Privacy Requirements

It is recommended that LECAC agencies should be required to demonstrate how they will operationalise all relevant privacy requirements as a pre-condition to gaining access to the FVS and FIS, including the incorporation of relevant FVS and FIS requirements into agency/Police Manuals, Standard Operating Procedures (or equivalent), policies and processes.

Each agency must document its approach to achieving practical privacy compliance and submit it as part of the Participation Access Arrangement process. This recommendation should be read alongside the requirement for each agency to review, update and/or develop its Privacy Governance Framework and Management Standards as required under clause 16.4(b) of the Participation Agreement (Recommendation 2).

Section 3.4, p.42

Specific FVS/FIS Recommendations – LECAC Agencies

Recommendation 4 – Quality of images

It is recommended that recognising that poor quality images will impact on the quality of match results generated, Requesting Agencies should demonstrate how they will:

- obtain the highest quality probe images, including where practicable optimising the environmental conditions around capture such as subject pose and lighting;
- apply relevant tools and techniques to pre-process and enhance the images before submitting them for matching, such as normalising the tilt, yaw, pitch and roll of the subject's face; and
- provide periodic reports to the governance group as to progress in implementing this recommendation.

Section 6.5, p.65

Recommendation 5 – Establish Community of Practice

It is recommended that LECAC agencies should consider establishing a community of practice that can:

- advise authorised users on relevant facial biometrics standards around image quality, storage and image processing techniques;
- share lessons learned and best practice in relation to use of the Face Matching Services; and
- assist in the development of Standard Operating Procedures or equivalent.

Section 6.5, p.66

Specific FVS Recommendations – LECAC Agencies

Recommendation 6 – LECAC Agency use of the FVS with Consent

It is recommended that where a LECAC agency *wishes to access the FVS on the basis of individual consent,* the agency should:

- ensure the consent is freely given and fully informed;
- a record is kept of the individual having provided consent; and
- as far as practical, provide a viable alternative method for individuals who do not wish to consent to a FVS check.

Section 6.6, p.66

Recommendation 7 – System-to-system connection

It is recommended in the event that a law enforcement or anti-corruption agency establishes a system-to-system connection to the Interoperability Hub, the agency must demonstrate how it will:

- adhere to best-practice information and personnel security arrangements in accordance with the Commonwealth's Protective Security Policy Framework and Information Security Manual;
- have documented processes for managing information security risks and responding to incidents, and review these documents annually to ensure they remain relevant to address emerging risks; and
- institute appropriate system access and user management controls in accordance with the Participation Agreement, FVS Access Policy and all other relevant policies as agreed by the National Identity Security Coordination Group.

Section 6.6, p.66

Recommendation 8 – FVS 'in the field'

It is recommended if a law enforcement or anti-corruption agency deploys FVS access to authorised officers in the field, for example on mobile devices or in-car computers, the agency must demonstrate how it will:

- maintain individual role-based access controls so that every transaction can be ascribed to a particular user and there is personal accountability and audit logs; and
- ensure that field-based access only comes from agency-issued or approved devices.

Section 66, p.67

Specific FIS Recommendations – LECAC Agencies

Recommendation 9 – FIS Gallery

It is recommended that where a FIS user has the ability to request more than 20 images from a Holding Agency with approval from the Authorising Officer, these requests should be utilised only where necessary and proportionate to the matter being investigated. FIS users should recognise that such requests:

- have a greater net impact on the privacy of individuals;
- should only be made in exceptional circumstances; and
- may lead to degradation in speed and performance across the whole system.

Section 6.7, p.67

Recommendation 10 – FIS users to receive minimum access required
It is recommended that authorised users of the FIS should only receive the minimum level of access needed to perform their role, with access maintained only as long as required. LECAC agencies must demonstrate that they have incorporated this requirement into their Standard Operating Procedures or equivalent. Section 6.7, p.67

Recommendation 11 – Gallery download
It is recommended LECAC agencies demonstrate the steps they have taken to ensure that FIS users with the ability to download the image gallery and/or shortlist response: • download the least amount of personal and sensitive information from the FIS; • any information downloaded is stored appropriately and only retained for the minimum period necessary, in accordance with the Participation Agreement and legislative obligations; • the dissemination of information downloaded from the FIS is limited only to those persons within the Requesting Agency with a legitimate 'need to know'; and • that the Requesting Agency retains sufficient tracking and audit information within its internal systems to prove compliance with these privacy safeguards and/or a request from the Holding Agency about the use of personal and sensitive information they disclosed. Section 6.7, p.67

Recommendation 12 – Eliminating candidates
Noting that within the gallery response to an FIS query there will be images of people whose face matched the probe image but are not the subject of the request, it is recommended that FIS users should as soon as possible eliminate candidates from the gallery response. Section 6.7, p.68

Recommendations – Home Affairs

Recommendation 1 – FMS Privacy Policy
It is recommended that: • Home Affairs develop an NFBMC (FMS) privacy policy and provide the 'home' for (e.g. website), or a link to, that privacy policy; • Home Affairs include information about the NFBMC within the Home Affairs' privacy policy; • all LECAC agencies ensure that they leverage the same core privacy information, adjusted to fit local circumstances as necessary, for publication at the jurisdictional level (e.g. within their own privacy policies). Section 5.1, p.58

Recommendation 2 – Coordinated Template Collection Notice Text

It is recommended that Home Affairs coordinate the development of standard or template NFBMC (FMS) collection notice text. This can be adopted by Data Holding Agencies (and LECAC agencies to the degree that this is relevant).

Section 5.1, p.58

Recommendation 3 – Management (of Perceptions) of Function Creep

It is recommended that careful consideration be given to any proposed extensions to the use or disclosure of biometric information/templates or the participation of additional agencies or the private sector in the NFBMC so as to avoid scope creep as well as perceptions of function creep. Any process adopted to explore extensions to use and disclosure should be as transparent and accountable as possible, involve consideration by the Coordination Group, be subject to a PIA, and enable stakeholders to participate in the debate about the merits or drawbacks of a particular position. Following agreement between the signatories to the IGA, significant changes should be subject to parliamentary review and disallowance

Section 5.1, p.58

Recommendation 4 – Full NFBMC PIA

It is recommended that the proposed, full NFBMC PIA:

- be commissioned in a timely manner and supported by appropriate documentation;
- be expressed as requiring an 'end to-end' and 'whole-of-information-lifecycle' PIA process;
- not be subject to restrictions in scope unless there is agreement between the Commonwealth and the PIA consultant that there is no privacy benefit in revisiting certain aspects of the NFBMC; and
- should encompass consideration of all relevant design components, including legislation, governance and information governance arrangements, protective security and privacy frameworks and associated fairness, accountability and transparency measures.

Section 7.1.2, p.71

Recommendation 5 – Commissioning a PIA Process

It is recommended that Home Affairs take a strategic approach to the commissioning of PIA processes, recognising that there is no 'one size fits all' PIA process. At time engaging an 'independent' PIA consultant may be best option while, at other times, it may be preferable to engage a PIA consultant to assist in the development of Approach to Market documentation or to conduct a PIA process in collaboration with a project team.

Section 7.1.2, p.71

Recommendation 6 – Transfer of NFBMC from AGD to Home Affairs

It is recommended that Home Affairs address privacy perception issues arising from the transfer of responsibility for the NFBMC from AGD to Home Affairs. It is considered desirable for Home Affairs to develop and publish information outlining how the separation of various

NFBMC roles and responsibilities (System Administrator, Data Holding Agency, Requesting Agency) will be maintained within a single organisation (Home Affairs).

Section 7.2.2, p.73

Recommendation 7 – Publication of PIA Reports

It is recommended that, where the full publication of a PIA report is withheld on the grounds of operational secrecy, the Commonwealth investigate all appropriate options for publishing as much of the content of a PIA report as is possible. At a minimum, a PIA report's key findings and recommendations should be published online.

Section 7.2.3, p.74

Recommendation 8 – Enhanced Technical Accountability Measures

It is recommended that Home Affairs should consider publishing an account of the technical and other steps it has taken and will continue to take to:

a) benchmark the NFBMC biometric face recognition system against other like systems;

b) ensure the accuracy of the NFBMC biometric face recognition system; and

c) undertake a NFBMC benefits realisation project.

Section 7.3.2, p.75

Specific Findings – Relevant to All Participants

Finding 1 – Clause 16.1 of the Participation Agreement

It is considered that Participants may wish to review the operation clause 16.1 of the FMS Participation Agreement in order to ensure that it achieves the intended set of outcomes, including the institution of a consistent approach for all LECAC agencies (i.e. a level privacy playing field).

Section 3.2.1, p.38

Finding 2 – Enhancing Privacy Governance

It is considered important that a review of the approach taken to privacy governance within the FMS Data Sharing Framework be undertaken at an appropriate point in time, e.g. review of the IGA on Identity Matching Services. This will help to balance the high degree of privacy protections offered through the IGA, Participation Agreement and associated policies and procedures with those provided via the Coordination Group.

Section 7.4.1, p.78

Finding 3 – Enhancing Governance Independence and Skills

As part of the review of the IGA on Identity Matching Services, consideration should be given to appointing independent members to the Coordination Group. This could include individuals with specific protective security, legal or privacy skills.

Section 7.4.1, p.78

1 Introduction

1.1 The NFBMC

On 5 October 2017 the Commonwealth, state and territory governments signed an Intergovernmental Agreement (IGA) on Identity Matching Services (IMS). Under this agreement, authorised agencies in all jurisdictions will be able to access passport, visa, citizenship, and driver licence images via a number of biometric face matching services. These services form part of the National Facial Biometric Matching Capability (NFBMC) (see Figure 1, below).

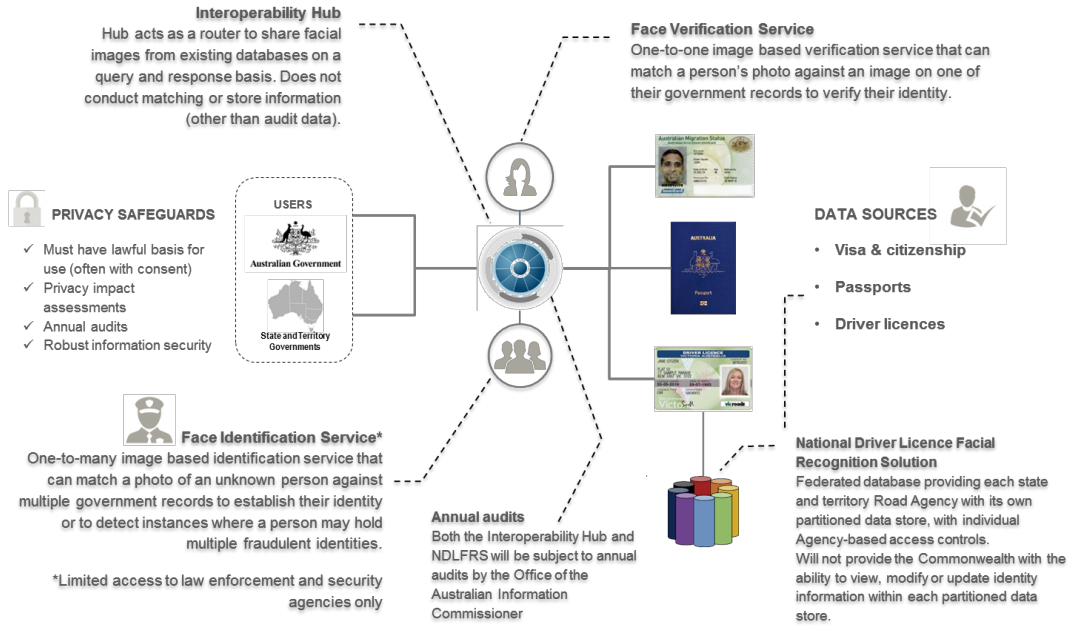


Figure 1 – National Facial Biometric Matching Capability

The NFBMC is an umbrella term covering the technical infrastructure, associated services, and legislative and governance arrangements that will enable the sharing and matching of Identity Information (personal information) by a number of authorised agencies on a national basis via the Interoperability Hub (the Hub). The NFBMC is intended to:

- protect people from identity theft, and help victims restore their compromised identities;
- prevent criminals and terrorists creating and using fraudulent identity documents;
- assist police to investigate other serious criminal activity; and
- help people to prove who they are when using government services online.[2]

Home Affairs is leading the development of the NFBMC.

1.2 LECAC PIA

Bainbridge Associates was commissioned by the Commonwealth Government to undertake a Privacy Impact Assessment (PIA) of Commonwealth, state and territory Law Enforcement, Crime and Anti-Corruption (LECAC) agencies' access to and use of two Face Matching Services (FMS):

[2] Department of Home Affairs, Fact Sheet – Face Matching Services: https://www.homeaffairs.gov.au/criminal-justice/files/face-matching-services-fact-sheet.pdf

1. the Face Verification Service (FVS), which provides one-to-one image matching or retrieval to *confirm* a known identity; and
2. the Face Identification Service (FIS), which provides one-to-many image matching to *establish* the identity of an unknown individual or to detect identity fraud.

As illustrated above (see Figure 1), the FVS and FIS are components of the NFBMC. They will draw upon a number of data sources for image matching, including:

- Australian Passport images held by the Department of Foreign Affairs and Trade (DFAT);
- Visa, Citizenship and some other image holdings maintained by the Department of Home Affairs (Home Affairs); and
- Driver Licence images held by state and territory road agencies.

In a *LECAC context*, the FVS and FIS will be used to:

- identify persons of interest (POI) in criminal and national security investigations;
- enhance the integrity of the issuance process for identity credentials; and
- support regulatory activities where a high level of assurance in a person's identity is required.

1.3 LECAC PIA Scope and Purpose

The LECAC PIA was restricted to Commonwealth, state and territory police and anti-corruption/integrity agencies that require access to the FVS and FIS in order to perform their functions and duties. Figure 2, below, provides a list of LECAC agencies designated 'in scope'.

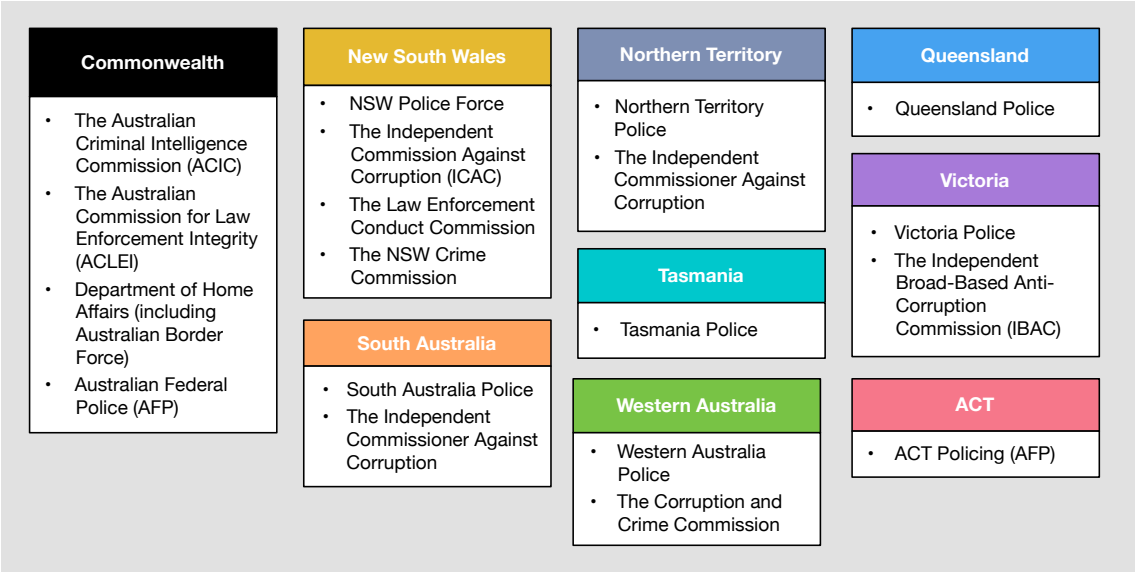


Figure 2 – 'In scope' Commonwealth, State and Territory Agencies

It was established during the PIA process that the Tasmanian Integrity Commission does not require any access to the FVS/FIS and the Queensland Crime and Corruption Commission (CCC) does not require access to the FVS/FIS except in relation to sanitisation activities. Both agencies were subsequently excluded from the PIA.[3] Other agencies whose functions may include some law enforcement activities are not within the scope of this PIA.

[3] The Queensland CCC will sign a Participation Agreement in order to undertake the sanitisation exercise.

The purpose of the LECAC PIA is to ensure alignment between LECAC agencies' use of the FVS and FIS and the best practice privacy controls adopted by the NFBMC (See Appendix A for a summary of legislative, privacy and security requirements). The PIA was required to focus upon:

1. LECAC agencies' proposed use of the FVS and FIS, including their access to specified data sources and the consideration of representative FVS and FIS use cases;
2. LECAC agencies' proposed deployment models, including Standard Operating Procedures, authorisation processes, number of users and estimated volumes of use, and minimum-training requirements for nominated users; and
3. any other relevant issues arising during the conduct of the LECAC PIA that have not been examined in previous PIA processes.

Other aspects of the design of the FVS and FIS, related services, the technical systems supporting the services, and/or the NFBMC operating model, governance and legislative arrangements were designated *out of scope* on the basis that these components have already been subject to, or will be subject to, their own separate PIA processes.

The LECAC PIA is a partial PIA as it focuses upon one particular set of participants (LECAC agencies), services (FVS, FIS) and information flows. It does not examine the NFBMC end-to-end or from a whole-of-information-lifecycle perspective.

1.4 LECAC PIA Methodology and Key Inputs

The LECAC PIA was required to follow the OAIC's *Guide to Undertaking Privacy Impact Assessments*, including assessment of FVS and FIS information flows against the requirements of the APPs contained in the *Privacy Act 1988* (Cth) (Privacy Act).[4]

1.4.1 Consultation

The LECAC PIA involved limited consultation with privacy regulators and LECAC agencies.

- Home Affairs convened a National Privacy Commissioners' Forum on 21 February 2018 to provide all Commonwealth, State and Territory privacy regulators (or equivalent) with an update about the NFBMC and the LECAC PIA process.[5]
- An initial teleconference with representatives of all LECAC agencies was held on 22 February 2018 to seek information about applicable jurisdictional legal, security and policy frameworks and proposed use cases for the FVS and FIS.
- A final teleconference (13 December 2018) was scheduled with LECAC agencies to obtain feedback in response to the review draft of the LECAC PIA report (v.0.14).

1.4.2 Previous PIA Processes

Prior to the LECAC PIA, Home Affairs had commissioned an independent PIA for each of the NFBMC's main systems and services, in alignment with the iterative NFBMC system design and release ('go live') process.

1. NFBMC Interoperability Hub PIA (August 2015) (Information Integrity Solutions)
2. FVS PIAs (Commonwealth Agencies) (August 2016) (Lockstep Consulting)
3. FIS PIA (Commonwealth Agencies) (August 2016) (Information Integrity Solutions)
4. NDFLRS PIA (November 2017) (Information Integrity Solutions)
5. IMSB Legislative PIA (January 2018) (Australian Government Solicitor)

[4] See https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.
[5] Subsequent written feedback provided by the Queensland and Victorian Commissioners was taken into account during the PIA process.

Bainbridge Associates received copies of previous PIA reports (except for the IMSB Legislative PIA) and was required to take their findings into account.[6]

1.4.3 LECAC PIA Documentation

Home Affairs provided Bainbridge Associates with a suite of FMS documents, including the FMS Participation Agreement, FVS and FIS Access Policies, FMS Training Policy and FMS Compliance Policy (See Appendix B for a full list of PIA documentation).

As noted above (section 1.3), the LECAC PIA was required to examine representative FVS and FIS use cases. While Home Affairs provided Bainbridge Associates with a range of relevant background material –including NFBMC User and Operational Scenarios – this did not include specific LECAC PIA use cases. Towards the end of the PIA process, Victoria Police helped Bainbridge Associates document a number of FVS and FIS use cases. The LECAC PIA was also required to consider proposed deployment models, including Standard Operating Procedures (SOPs) (see section 1.3, above). Bainbridge Associates was not provided with specific deployment models or relevant SOPs.

No draft or proposed Participant Access Arrangements (PAA) were available for consideration during the PIA process. The PAA template is relevant because it will document, at a detailed level, the specific data elements and information flows involved in LECAC agency use of the FVS and FIS.

1.5 LECAC PIA Report

By the time the LECAC PIA was commissioned, a significant volume of information had been generated about the NFBMC, including via previous PIA processes. This information establishes the broader context of the LECAC PIA. Much of this information was excluded from the LECAC PIA on the grounds of being out of scope.

This affected the drafting of the LECAC PIA report. Best practice requires a PIA report to 'tell the story' of an initiative in a way that can be understood by non-expert readers.[7] However, providing sufficient context – within the constraints of a partial PIA process and at the tail end of an overarching, iterative PIA process – risked introducing an additional layer of complexity likely to impede, rather than facilitate, key privacy messages. Taking account of feedback from LECAC agencies, the LECAC PIA report favours simplicity over complexity because this is considered likely to produce the best privacy outcomes. As a consequence, the report is best suited to informed rather than non-expert readers.

1.5.1 LECAC PIA Report Prerequisites

The LECAC PIA report assumes that readers are familiar with each of the following:

- Australia's *Identity Security Policy Framework;*
- the broader remit of the *Intergovernmental Agreement on Identity Matching Services* (beyond LECAC agency use of the FVS and FIS);
- the division of responsibilities between the Commonwealth and state/territory governments and associated legislation in relation to NFBMC data sources and law enforcement, national security and border control activities;
- the *NFBMC legal framework* designed to ensure that the NFBMC is subject to an interoperable legal framework;
- *best practice governance and information governance*, as successful governance will be key to the success of the NFBMC; and

[6] Prior to full implementation, Home Affairs will commission a comprehensive, independent NFBMC PIA, i.e. a PIA that examines NFBMC privacy issues end-to-end and from a whole-of-information-lifecycle perspective.
[7] See OAIC PIA Guide

- *'Privacy by Design'* – both as a practice intended to entrench a more integrated approach to privacy and a specific approach to privacy management, developed in the 1990s, and subsequently adopted internationally.

A high-level summary of these topics is provided at Appendix C.

It is also assumed that readers are familiar with the NFBMC as a whole. This includes all of the NFBMC services, technical systems and operating model, including its policy and governance framework and legislative arrangements.

1.5.2 LECAC PIA Report Structure

The LECAC PIA report contains seven chapters.

- *Chapter 1 – Introduction*
  - Summary of LECAC PIA scope, purpose, methodology and key inputs
- *Chapter 2 – LECAC PIA Participants and Information Flows*
  - Provides an overview of 'in scope' LECAC agencies, the FMS Data Sharing Framework and a summary of FVS and FIS information flows (provided by Home Affairs)
- *Chapter 3 – Privacy Issues, Exemptions and 'Functional Equivalence'*
  - Outlines key privacy risks and identifies an approach to FVS/FIS privacy management, informed by the FMS Data Sharing Framework, which addresses issues raised by LECAC agencies' varying legislative, privacy and policy frameworks
- *Chapter 4 – Legislation, Privacy and Protective Security*
  - Provides an account of relevant legislation, privacy and protective security arrangements applicable to LECAC agency access to the FVS and FIS under the terms of the FMS Data Sharing Framework
- *Chapter 5 – Mapping the APPs*
  - Provides a high level mapping of FVS/FIS information flows against the APPs contained in the Privacy Act and identifies common or core privacy principle requirements that LECAC agencies should take into account (regardless of whether or not they are subject to privacy legislation and/or privacy principles)
- *Chapter 6 – Operationalising Privacy Requirements*
  - Outlines generic FVS and FIS use cases and an approach to the operationalisation of privacy requirements and controls required under the IGA and FMS Data Sharing Framework across LECAC agencies/jurisdictions
- *Chapter 7 – Additional Privacy Issues and Risks*
  - Identifies a number of privacy issues and risks that are 'out of scope' for the LECAC PIA, but which nevertheless have broader relevance to the FVS/FIS, the NFBMC and/or LECAC agencies

1.6 Caveat

While the LECAC PIA report includes legal policy analysis, it is important to note that the report *does not* constitute legal advice. Any legal issues raised within this PIA report will need to be assessed by Home Affairs.

2 LECAC PIA Participants and Information Flows

The Commonwealth has taken significant steps to develop a coherent FMS Data Sharing Framework for the NFBMC. 'FMS' refers collectively to the FVS, FIS, Face Recognition Analysis Utility Service (FRAUS) and One Person One Licence Service (OPOLS). For the purposes of the LECAC PIA, only *the FVS and FIS are in scope*.

The FMS Data Sharing Framework operationalises the IMS IGA, instantiating the intention of the parties to the IGA to build privacy into the NFBMC and to ensure consistency across a federal system in which different laws, standards and policies apply to participants. This approach recognises explicitly that, while the NFBMC was agreed under the aegis of the IMS IGA and will involve the participation of a range of Commonwealth, state and territory agencies in addition to LECAC agencies, there is no obvious or straightforward way to ensure consistent and transparent compliance with relevant FVS and FIS privacy requirements and controls.

2.1 Participant Roles

The following roles and participants, as defined in the FMS Participation Agreement, are relevant to the LECAC PIA.[8]

- *Framework Administrator:* Home Affairs is the current Framework Administrator
- *Hub Controller:* Home Affairs is the current Hub Controller
- *Hub Access Participant:* refers to any Data Holding Agency or a Requesting Agency that has been authorised/provided with access to the Interoperability Hub
- *Data Holding Agency:* DFAT, Home Affairs and state and territory roads agencies will participate as Data Holding Agencies (DHAs), providing facial images/templates from passport, visa and citizenship databases, and driver licence databases respectively
- *Requesting Agency:* LECAC agencies will participate as Requesting Agencies and access DHA data holdings for verification and/or identification purposes

The PIA process identified the need for an additional role – subsequently termed *Sanitising Agency* – to cover a LECAC agency that will gain access to the FMS to confirm/ensure that protected identities will not be breached as a result of FVS and FIS implementation, but will not otherwise need to access/use the FMS. Sanitising agencies will enter into a Participation Agreement, but will not receive data for operational purposes.

2.2 LECAC Agency Preconditions to Access

Before gaining access to the FVS and FIS, each LECAC agency is required to enter into a standard, legally binding Participation Agreement containing common terms and conditions and including detailed privacy and security safeguards and regular auditing and oversight arrangements. Under this arrangement, LECAC agencies must:

- provide a statement of legislative authority outlining the legal basis for their participation;
- establish an appropriate privacy governance and management framework – including compliance mechanisms – based upon requirements set out in the:
    - FVS Access Policy;
    - FIS Access Policy;
    - FMS Compliance Policy;
    - FMS Training Policy; and

[8] See clause 3.1 of the FMS Participation Agreement.

- comply with mandated security standards and testing.

LECAC agencies will also enter into individual PAAs documenting the specific details of data sources being accessed or shared. A common Data Source Catalogue will contain 'standing offers' made by Data Holding Agencies. Standing offers will comprise the minimum data required for use.

Figure 3, below, provides an overview of the full set of agreements supporting implementation of the FMS, including the FVS and FIS.

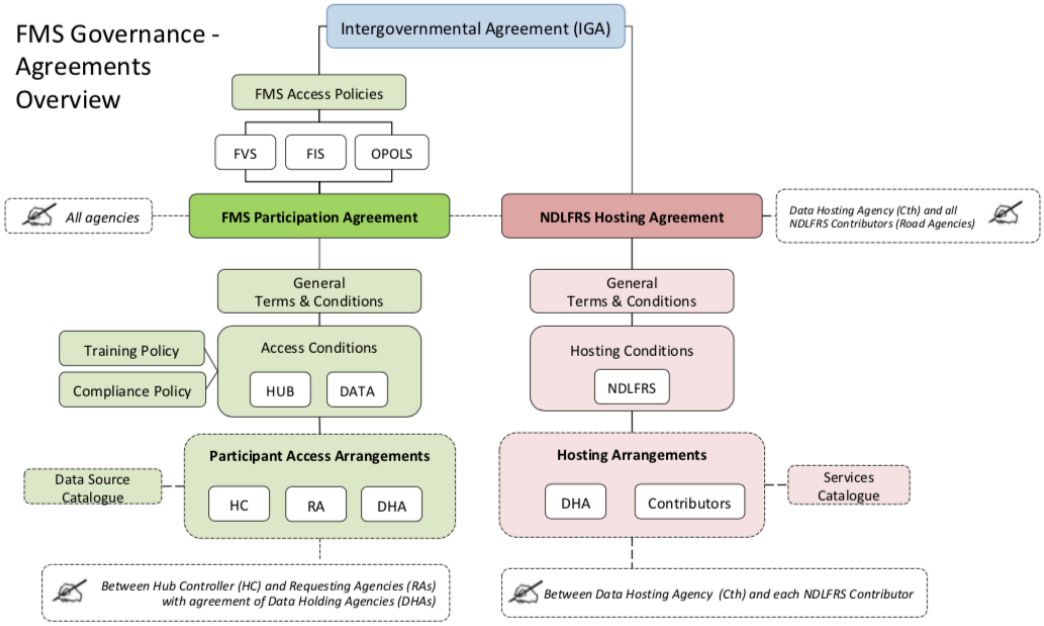


Figure 3 – FMS Governance Agreements

2.2.1 Lawful Basis Requirement

LECAC agencies must have a lawful basis to collect, use, store and disclose biometric facial images. In practice, this will apply differentially to the FVS and the FIS, as provided for in their respective access policies:

- For the FVS:
  - collection requires the individual's informed consent or, alternatively, a legislative basis or authority to collect the information;
  - use of the FVS must be compliant with the Privacy Act, relevant state and territory privacy legislation and/or other applicable legislation or, where privacy legislation does not exist, with the APPs.
- For the FIS, which has a higher privacy risk rating because of its 'one-to-many' capability:
  - access is informed by a set of access principles, which underpin the design and operation of the FIS;
  - a legislative basis or authority is a prerequisite to the collection of information via the FIS;
  - use of the FIS must be compliant with the Privacy Act, relevant state and territory privacy legislation and/or other applicable legislation or, where privacy legislation does not exist, with the APPs;
  - access is restricted to agencies with law enforcement or national security related functions that are approved by the Coordination Group;

- use of the FIS for *general law enforcement purposes* means the prevention, detection, investigation or prosecution of an offence under Commonwealth, state and/or territory laws carrying a maximum penalty of not less than three years.

s37(2)(b) [redacted]

2.3 Contextualising the FVS and FIS

Looked at in context, the FVS and FIS form part of a continuum of Identity Matching Services, from the DVS (no biometric matching capability) through to the FVS (biometric capability on a one-to-one or Match/No Match basis) and the FIS (one-to-many biometric capability). The LECAC PIA is focused upon LECAC agency use of the FVS and FIS as they involve biometrics and raise new privacy impacts. The PIA contract required Bainbridge Associates to consider these two services together via the LECAC PIA process. In terms of the continuum, the DVS is excluded from consideration, as it does not involve biometrics (see Figure 4, below).

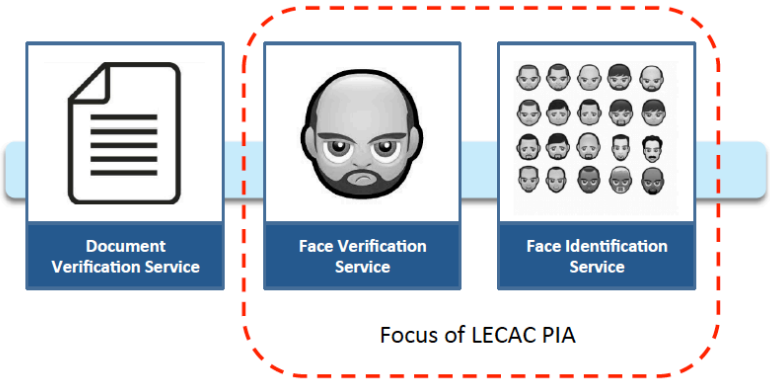


Figure 4 – LECAC PIA Focus

However, this combination (referred to collectively as 'FMS') has the potential to create misunderstandings, particularly in a privacy context. While LECAC agencies will use both the FVS and FIS to support their activities, these services cover different ground and raise different privacy issues and risks. The FVS is largely consistent with existing verification processes while the FIS is significantly more sensitive and subject to more stringent access requirements than the FVS (although both services will need to be accessed and used appropriately).

In practical terms, there is a greater correlation between the DVS and FVS in terms of *identity verification* by a range of authorised users (or, in the terminology of the Participation Agreement, 'Requesting Agencies'). Viewing the FVS as part of a broader approach to 'identity verification' has a number of benefits:

- it helps to maintain a focus upon verification (building upon the existing Identity Security Policy Framework);
- it recognises that, beyond LECAC agencies, a wider range of agencies (and, in the future, private sector organisations) will be provided with access to the FVS for verification purposes; and
- it indicates that, *where relevant, appropriate and desirable*, access may occur on the basis of individual consent (if consent is not provided, relevant legislative authority will be required).

In contrast, the use of the FIS will be restricted to police and national security agencies and limited in terms of access. It differs from the DVS and FVS in that:

- it has the capacity to *identify* an individual from a very large pool of biometric (template) information;
- it will be used as a powerful tool for *identification* purposes, both to identify an unknown individual or to identify an individual with multiple fraudulent identities;
- it represents a transformational – as opposed to incremental – benefit for law enforcement and crime agencies;[9] and
- access to the FIS will be provided on the grounds of legal authority; individual consent is not relevant.

As there is no proposed intention to extend access to the FIS beyond police and national security agencies or to incorporate a consent mechanism within the FIS, maintaining a distinction between the FVS and FIS helps to clarify that *only the FVS*:

- will be accessible to a broader set of agencies and organisations; and
- will be subject to individual consent or, alternatively, legal authority (as relevant).

From the perspective of the LECAC PIA, the issues raised by the FIS are of a different order to those raised by the FVS. Presenting LECAC agency use of the FVS and FIS as separate services focused upon verification and identification respectively does not prevent them being managed collectively by LECAC agencies at an operational level. It will allow privacy issues and risks to be explained in a more comprehensible way (see Figure 5, below). This finding is consistent with previous PIA processes.

In this PIA report the collective term 'FMS' is avoided if its use has the potential to conflate the FVS and FIS or leading to misunderstandings.

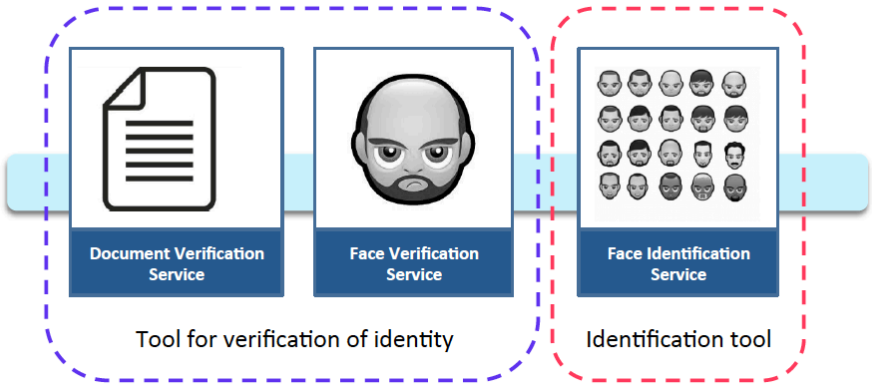


Figure 5 – Verification v. Identification

2.4 LECAC PIA Information Flows

A key input to any privacy analysis is an information flow diagram illustrating how personal information (including health and sensitive information) will be collected and handled for the purposes of a particular initiative, data collection or information system.

In a standard PIA, the information flow diagram provides the basis for mapping the information flows of personal information against the relevant set(s) of privacy principles; in turn identifying whether or not those information flows comply with the requirements set out in the privacy principles.

[9] Department of Home Affairs, *Benefits to State and Territory Law Enforcement & Related Agencies: NFBMC* (April 2016).

In a complex, multi-party PIA – like the LECAC PIA – multiple data flow diagrams may be required. As noted above (section 1.4.3), detailed information about data elements and/or information flow diagrams illustrating what happens to personal information (including sensitive biometric information) once it *crosses the boundary* from the NFBMC into LECAC agencies' information systems were not provided to Bainbridge Associates. Home Affairs provided standard FVS and FIS information flow diagrams, documenting data elements and illustrating information flows in relation to the services. These diagrams provided the basis for the LECAC PIA. It is notable that:

- the FVS and the FIS are subject to a limited and defined set of information flows; and
- a full set of FVS and FIS data elements have been identified and documented.

This means that the information flows are 'known knowns' and, therefore, amenable to privacy management.

2.4.1 FVS Information Flows

Figure 6 (below), illustrates FVS information flows from the perspectives of a LECAC agency (Requesting Agency), the Hub and a Data Holding Agency.

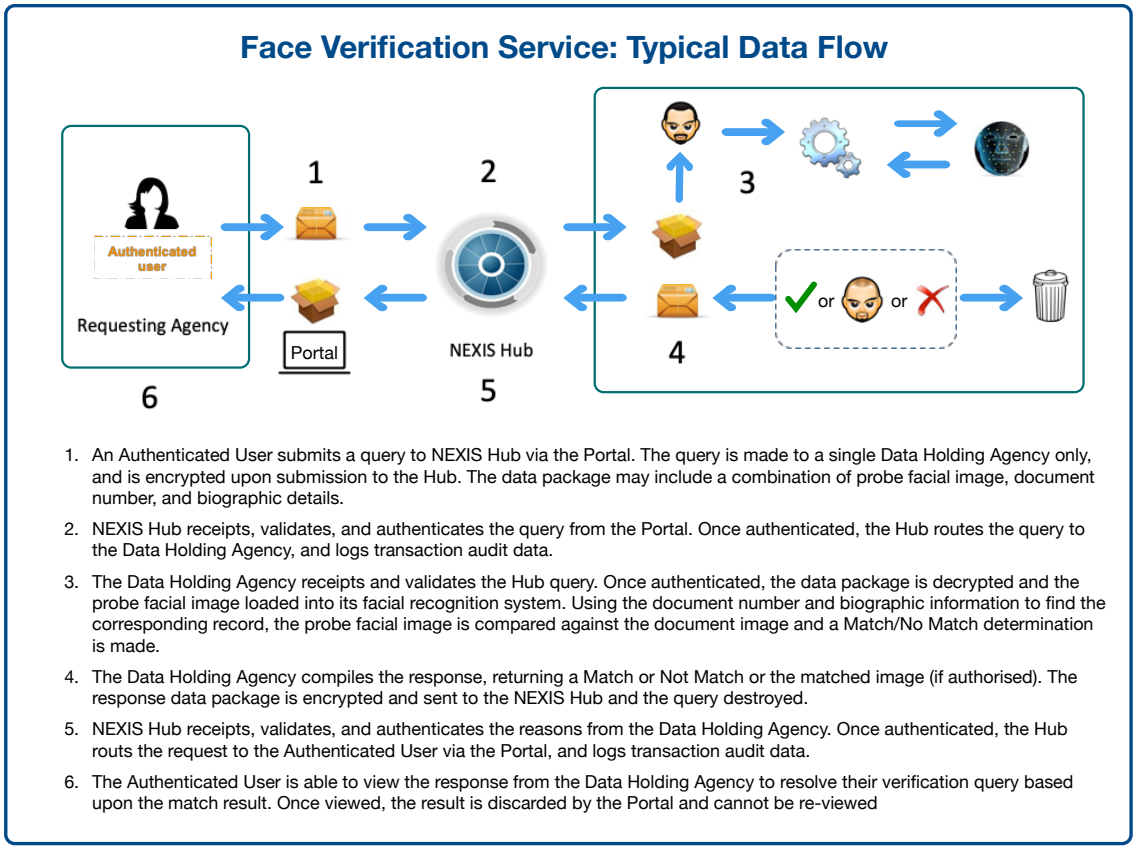


Figure 6 – FVS Information Flows

Further information provided by Home Affairs included:

- a detailed account of FVS information flows, including data attributes (as inputs and outputs), processing and audit functionality for the PIA process:
    - at the level of detailed information flows, privilege indicators will reflect the privileges assigned to a User's role, i.e. whether or not he/she is

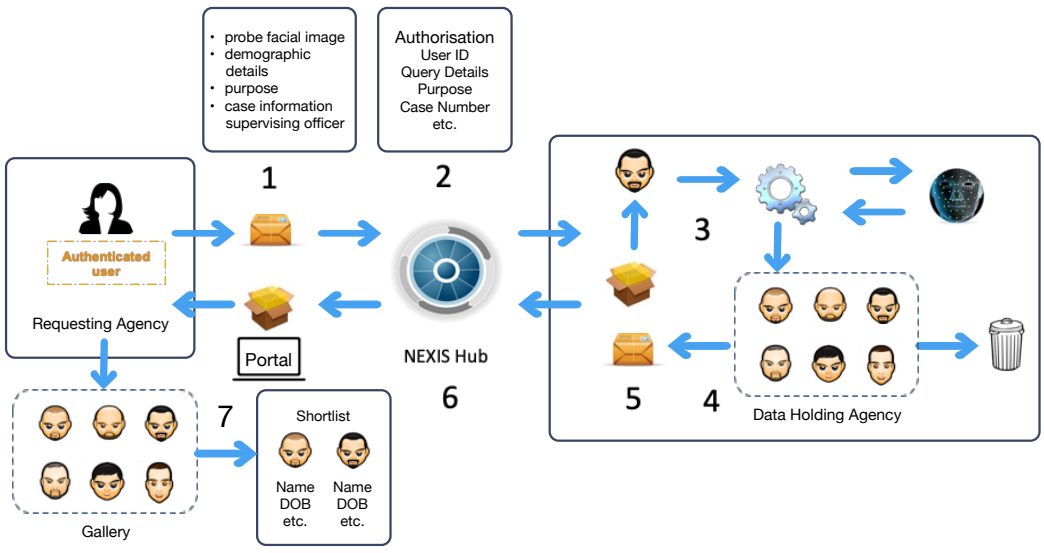
allowed to view specific data elements as agreed between the Requesting Agency and Data Holding Agency;

- the attributes listed by Home Affairs comprise the generic 'full' set of elements that may be returned in a search (additional, specific data elements may be returned by some Data Holding Agencies);
- any privilege indicators sent in a request may mean that some data elements may not be returned; and

- a detailed account of the audit process for an FVS transaction, noting that different attributes may be added/updated at various times during the audit lifecycle.[10]

2.4.2 FIS Information Flows

Figure 7 (below), illustrates FIS information flows from the perspectives of a Requesting Agency (LECAC agency), the Hub and more than one Data Holding Agency.



1. An Authenticated User submits a query to NEXIS Hub via the Portal. The query is made to one or more Data Holding Agency, and is encrypted upon submission to the Hub. The data package includes a combination of probe facial image, demographic details, purpose, case information and supervising officer (and where required authorising officer).
2. NEXIS Hub receipts, validates, and authenticates the query from the Portal. If the query details and purpose entered by the user require authorisation, the Hub notifies an authorising officer that a FIS query requires approval. Once the query is approved, the Hub routes the query to the Data Holding Agency(ies), and logs transaction audit data.
3. The Data Holding Agency receipts and validates the Hub query. Once authenticated, the data package is decrypted and the probe facial image loaded into its facial recognition system. The probe facial image is compared against all of the images within that database, then the demographic filters are applied to narrow down the result set.
4. The Data Holding Agency compiles the response. For standard FIS queries, the top 20 matching facial images within the demographic filters are returned to the user. In exceptional circumstances, such as counter-terrorism or critical incidents, and with authorisation, a greater number of matching images can be returned. The Data Holding Agency can determine how many images are returned.
5. The response data package is encrypted and sent to the NEXIS Hub, and the query destroyed.
6. NEXIS Hub receipts, validates and authenticates the response from the Data Holding Agency. Once authenticated, the Hub routs the request to the Authenticated User via the Portal, and logs transaction audit data.
7. The Authenticated User is initially able to view only the facial images from the Data Holding Agency. Once once they have shortlisted a smaller number of images can they view the associated biographic information. Once the result is viewed, it is discarded by the Portal and cannot be re-viewed. Authorised users can download the result set.

Figure 7 – FIS Information Flows

[10] This detailed information is not reproduced in the PIA report due to length, but is available from Home Affairs.

Home Affairs provided a full account of FIS information flows, including data attributes (as inputs and outputs), processing and audit functionality for the PIA process.[11]

As noted in the detailed information flows:

- When preparing a query, an authenticated user must list the purpose of the search, the relevant legislative authority (i.e. Act) and relevant section within the Act. Purpose, Act and Section are populated based upon pre-defined lists that the user can select from;
- Authorising Officers are only required where specific criteria has determined that it is a prerequisite. This may be based upon one or more factors: subject/category selections; age range values; number of records to be returned; request priority;
- the FIS roles assigned to a user will: specify the age ranges the user can enter for the selected subject/category; indicate if the user is able to select a non-default number of records to return; indicate if they are able to select match threshold and/or priority value; and
- the attributes listed comprise the generic 'full' set of elements that may be returned in a search (additional, specific data elements may be returned by some Data Holding Agencies). Any privilege indicators sent in a request may mean that some data elements may not be returned.

Figure 8, below, illustrates the construction of the FIS query, in particular, the specification of legal authority (Act and Section) and permitted Purpose.

Figure 8 –Specification of Legal Authority and Permitted Purpose in FIS Query

[11] This detailed information is not reproduced in the PIA report due to length, but is available from Home Affairs.

3 Privacy Issues, Exemptions and Functional Equivalence

3.1 General privacy risks

From the time the NFBMC commenced development, participants and stakeholders have agreed that the implementation of a biometric facial recognition system poses a significant degree of privacy risk. Previous PIA reports have confirmed that the privacy risks are high on three main grounds:

- biometric information is considered to be intrinsically sensitive;
- extremely large data holdings of facial images will be made available for automated facial recognition system analysis and matching on a national basis; and
- the 're-purposing' of government-held images for use by LECAC agencies falls outside of the initial purpose of collection.[12]

In response, Home Affairs has taken a proactive approach to privacy management. This can be seen in the extensive privacy and protective security safeguards adopted by the IGA, the FMS Data Sharing Framework developed to support implementation (including multiple PIA processes), as well as the technical and governance underpinnings of the NFBMC.

However, perhaps as a result of the broad agreement about the existence of privacy risk, surprisingly little has been documented about *the specific reasons* for concern. At times, statements about NFBMC privacy risk appear generic or overly simplistic. When this is coupled with mainstream media reports about biometric applications, which are often inaccurate (or not fit-for-purpose), it is easy for misunderstandings to arise, making it difficult to have an informed debate about NFBMC privacy risks.

It is equally important to distinguish between the *potential* uses of a technology from its *actual* use. In a context in which it may be difficult to distinguish biometric fact from fiction, it is necessary to understand what the FVS and the FIS will actually do (i.e. how these services will be deployed and operationalised by LECAC agencies) in order to identify their privacy risks (or 'privacy slack') accurately, neither overstating, nor understating, the degree of risk.

In consultation with Home Affairs, a high-level literature review was undertaken to identify a range of common or general privacy issues and risks arising from law enforcement use of biometric systems. A summary of the findings is provided at Appendix F. These have been drawn from around the world and are not specific to the NFBMC. They are intended to provide context for the presentation of specific issues and risks raised by LECAC agencies' use of the FVS and FIS canvassed in the body of this report.

One specific privacy risk – law enforcement exemptions or exceptions from the application of privacy legislation and/or privacy principles – warrants discussion in the body of the report because of its impact upon the PIA process.

3.2 Law Enforcement Privacy Exceptions/Exemptions

One of the key reasons why the use of biometric information for law enforcement purposes is considered to pose a privacy risk – both within Australia and internationally – is because law enforcement, crime and anti-corruption agencies (and national security agencies) are usually granted:

- an exemption (partial or full) from privacy legislation; and/or

[12] See, for example, IIS, NDFLRS PIA, p.6.

- exceptions within the privacy principles.

Law enforcement exemptions/exceptions are provided on public interest grounds, recognising that information privacy is not absolute. Privacy may need to be considered against a range of other, sometimes countervailing, public interests – such as law enforcement and/or the regulatory objectives of government. These may override the application of privacy legislation or the operation of the privacy principles.

References to law enforcement 'exemptions' and 'exceptions' have specific meaning. In this report, adopting the wording of the ALRC:

- An *exemption* applies where a specified entity or a class of entity is not required to comply with any of the requirements in privacy legislation.
- A *partial exemption* applies where a specified entity or a class of entity is required to comply with either: some, but not all, of the provisions of privacy legislation; or some or all of the provisions of privacy legislation, but only in relation to certain of its activities.
- An *exception*, as applied to the privacy principles, applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct.[13]

3.2.1 LECAC Agencies and Privacy Exemptions, Exceptions

Agencies subject to the LECAC PIA fall into two broad categories: (1) law enforcement agencies (police agencies), and (2) crime and anti-corruption agencies. As confirmed during the PIA process, federal, state and territory LECAC agencies are subject to a range of legislation that may require, authorise or permit them to collect, use and/or disclose personal information for specific purposes, and in particular ways. These laws provide the authorising environment for LECAC agencies' use of the FVS and FIS.

Legal authority is also relevant to a PIA process as an act or practice 'required or authorised by or under law' is an exception to privacy principles regulating the use and/or disclosure of personal information. In order to rely upon these privacy principle exceptions, agencies need to identify the relevant law or laws. Except for South Australia and Western Australia, all Australian jurisdictions have enacted privacy legislation.[14] These laws incorporate a variety of law enforcement agency exemptions/exceptions to LECAC agencies. Depending upon their jurisdiction and 'category' (type of agency), LECAC agencies may rely upon a number of exemptions and/or exceptions. These vary in terms of the breadth of exemption/exception granted (see Table 1, below). [15]

Privacy Exemptions/Exceptions by Jurisdiction	
Exemption/exception	**Jurisdiction (Agency)**
• Law enforcement/legal authority exceptions within the APPs only	Commonwealth (AFP), ACT

[13] ALRC, *For Your Information: Australian Privacy Law and Practice,* Report 108 (May 2008): § 37.18, pp.1288-1289.
[14] While it does not have privacy legislation, South Australia has had an administrative instruction in place for many years (Information Privacy Principles Instruction).
[15] As described by the ALRC, crime and anti-corruption agencies are wholly exempt from privacy legislation for a number of reasons, including: their coercive, inquisitorial powers, which may be exercised in a public or private hearing; their law enforcement functions and powers; the special nature of those who may fall subject to investigation (e.g. law enforcement officers engaged in corruption who are also skilled in counter-surveillance and other law enforcement methodologies); and their focus upon prosecutions and disciplinary outcomes rather than remedies for complainants. They are also subject to a separate system of oversight and accountability. ALRC, *For Your Information*, Chapter 37: Agencies with Law Enforcement Functions, pp.1265-1297.

• Partial exemptions permitting noncompliance with the relevant set of privacy principles 'on reasonable grounds' (or equivalent) • Law enforcement/legal authority exceptions within the relevant set of privacy principles • Law enforcement documents exempt from the IPPs	Victoria, Northern Territory, Queensland, Tasmania (Queensland only)
• Complete exemption from compliance with the IPPs contained in the *Privacy and Personal Information Protection Act 1998* (NSW) except for administrative and educative functions • Complete exemption from the *Health Records and Information Privacy Act 2002* (NSW) except for administrative and educative functions	New South Wales (ICAC, NSW Police Force, LECC, NSW Crime Commission)
• Exemption from privacy legislation altogether	Commonwealth (ACIC, ACLEI)

Table 1 – Privacy Exemptions/Exceptions by Jurisdiction

This variation introduces a significant degree of complexity to the LECAC PIA that is not easily resolved. As a means of demonstrating compliance with privacy requirements set out in the FMS Data Sharing Framework, considerable emphasis is placed upon:

- LECAC agency compliance with privacy legislation;
- LECAC agency compliance with privacy principles; and
- regulatory oversight by a privacy commissioner (or equivalent).[16]

However, to the degree that LECAC agencies are not required to comply with privacy legislation or the privacy principles, references to privacy law compliance within the FMS Data Sharing Agreement will be illusory (not to mention potentially misleading if these give an impression that exempt or partially exempt LECAC agencies are subject to privacy legislation, regulatory oversight, and so on).

If privacy legislation or privacy principles do not apply to a LECAC agency, it is reasonable to ask what role privacy legislation and privacy principles are expected to play in relation to its access to, and use of, the FVS and FIS. Clause 16.1 of the FMS Participation Agreement introduces the distinction between the application of privacy legislation on the one hand, and the absence of privacy legislation on the other. In the latter case, the Participation Agreement imposes a contractual obligation upon relevant agencies (i.e. the police forces of South Australia and Western Australia) to comply with the APPs as if they were APP entities under the Privacy Act. The Participation Agreement excludes the Corruption and Crime Commission of Western Australia, the Independent Commissioner against Corruption of South Australia, ACIC and ACLEI from contractual compliance with the APPs.

As a (potentially) unintended consequence of this approach, participants that are subject to privacy legislation, but exempt from complying with the associated set of privacy principles, are not required to follow privacy law/privacy principle requirements. This appears to be a technical defect in drafting, producing an outcome that is inconsistent with the intention of the IMS IGA. If a LECAC agency is exempt from the privacy principles, it cannot rely upon privacy legislation to authorise the collection, use or disclosure of FVS and FIS data. This means that *greater weight attaches to the contractual, governance and*

[16] For example, clause 16.1 of the Participation Agreement relies upon each participant's ability to comply with 'the Privacy Act, relevant state and territory privacy legislation and/or other applicable legislation' or, alternatively, contractual compliance with the federal Privacy Act and its APPs. This does not take account of agencies that may be subject to local privacy legislation but fully exempt from compliance with the privacy principles contained within therein.

policy arrangements that will enable alignment between FMS privacy controls and agency practice.

Finding 1 – Clause 16.1 of the Participation Agreement
It is considered that Participants may wish to review the operation of clause 16.1 of the FMS Participation Agreement in order to ensure that it achieves the intended set of outcomes, including the institution of a consistent approach for all LECAC agencies (i.e. a level privacy playing field).

3.3 LECAC PIA Process

3.3.1 Participation Agreement PIA Process

Under clause 45.2 of the Participation Agreement, all Participants other than Sanitising Agencies are required to conduct a PIA in relation to 'those uses of the Services that are proposed to be enabled by a Participant Access Arrangement' and to obtain a Privacy Impact Assessment report.

Under clause 45(2)(c), the Participation Agreement provides that:

> A Privacy Impact Assessment may be conducted, and Privacy Impact Assessment Report may be obtained, for multiple Data Holding Agencies and Multiple Requesting Agencies at the same time, provided that the Privacy Impact Assessment and the Privacy Impact [*sic*] Report specifically addresses each Requesting Agency's use of the Services that is proposed to be enabled by each proposed Participant Access Agreement.

Home Affairs commissioned a multi-party PIA process on behalf of all LECAC agencies. However, the varying application of privacy legislation to LECAC agencies, as well as the importance given to privacy legislation in the FMS Data Sharing Framework, raised a threshold issue for the LECAC PIA because:

1. there is no consistent or equivalent privacy law framework in place to measure privacy compliance and practice against;
2. LECAC agencies operate with exemptions (partial or full) from privacy legislation or exceptions from privacy principles; and
3. there are significant differences between law enforcement and crime/anti-corruption agencies in relation to their authorising environments.

Additionally, as noted in Chapter 2, detailed data elements and information flows *for each agency* were not available for assessment. This had a significant impact upon the LECAC PIA process.

3.3.2 Exempt Agencies

An exception to the requirement to conduct a PIA is provided to 'exempt' agencies under clause 45.2 (p) of the Participation Agreement:

> Where access to information through a Service is exempt from otherwise applicable Commonwealth, state or territory privacy laws, the Requesting Agency may develop a privacy statement, instead of obtaining a PIA. The privacy statement must outline the legislative, policy and other safeguards that apply to the handling of personal information to be obtained via the Service; be developed in consultation with the relevant Data Holding Agency or Agencies from which the information will be obtained; and be approved by the Governing Body.

While a multi-party approach – whereby a PIA process can be conducted and PIA report obtained for multiple Data Holding Agencies and multiple Requesting Agencies at the same time – is provided for under clause 45.2 (c) of the Participation Agreement, it is not clear that this provided the most appropriate option for exempt agencies to pursue. The option provided under clause 45.2 (p) – namely development of a privacy statement outlining the legislative, policy and other safeguards that apply to the handling of personal information – is preferable.

The PIA recommends that exempt agencies (ACIC, ACLEI, the Corruption and Crime Commission of Western Australia and the Independent Commissioner against Corruption of South Australia) develop a privacy statement rather than rely upon the PIA process. This does not mean that the findings and recommendations of the LECAC PIA are not relevant to them. Indeed, the findings of the LECAC PIA should help exempt agencies to develop an appropriate statement. It does mean that this 'category' of LECAC agency should be removed from the scope of the LECAC PIA.

Recommendation 1 – Exempt Agencies to Develop Privacy Statement
It is recommended that, consistent with clause 45.2 (p) of the Participation Agreement, LECAC agencies that are exempt from privacy legislation and privacy principles should develop a privacy statement, instead of relying upon a PIA. The privacy statement must: • outline the legislative, policy and other safeguards that apply to the handling of personal information to be obtained via the specific service; • be developed in consultation with the relevant Data Holding Agency or Agencies from which the information will be obtained; and • be approved by the Coordination Group.

Noting that, even with the remaining LECAC agencies, the LECAC PIA found it difficult to conduct a multi-party PIA process because of the high degree of legislative variation, compounded by the lack of specific and detailed information about agencies' proposed use of the FVS and FIS or proposed deployment models and operational arrangements.

As a practical alternative, the PIA proposes that the remaining LECAC agencies be required to focus upon the operationalisation of privacy controls, in particular, to demonstrate how they will meet relevant requirements prior to gaining access to the FVS and FIS. This should include documentation of data elements, specific information flows, deployment models, standard operating procedures and related privacy policies and processes (e.g. documenting an approach to data breaches/privacy incident management). This process should be aligned with the PAA negotiation process, noting that some aspects will overlap.

For the purposes of the LECAC PIA, this has been termed a 'functional equivalence' assessment process. It is intended to apply to all agencies (except for exempt agencies), regardless of the breadth of their privacy exemptions (see section 3.4, below). Aligning this process with PAA negotiations will help to ensure that there is minimal duplication of effort.

3.4 Functional (Privacy) Equivalence

A key issue raised by the single, multi-party PIA process is the level of detail at which each LECAC agency should be assessed. It is clear that there was no intention to commission (up to) nineteen individual PIA processes; apart from anything else, the level of

consultation and the resources required to do so far exceed the scope of the LECAC PIA.[17] It is equally clear, based on feedback from Home Affairs, that the LECAC PIA was intended to deliver more than a high-level assessment of the FMS Data Sharing Framework. Indeed, Home Affairs believed that a multi-party LECAC PIA process could meet the requirements set out under clause 45(2) (c) of the Participation Agreement.

Resolving this issue is not clear-cut, as there is a degree of circularity about the timing of the PIA vis-à-vis agencies gaining access to the FVS and FIS.

- As a precondition to gaining access to the FVS and FIS, LECAC agencies are required to complete a PAA template. As provided for in Part 4 of the Participation Agreement, this template must record all relevant arrangements for the protection of personal information to be shared through the FVS and FIS as well as all arrangements for sharing information through the FVS and FIS (clause 46). As part of the template process, each agency must confirm its legislative basis for participation.
- Before entering into a PAA, agencies are required to conduct a PIA of their proposed access to, and use of, the FVS and FIS (clause 45.2(b)).

In order to conduct a multi-party LECAC PIA under clause 45.2(c):

- the data elements and information flows *for each* LECAC agency (where these vary) must be available to inform the PIA process so that specific (as opposed to generic) information flow diagrams can be prepared and assessed from a privacy perspective; and
- relevant information about agencies' legislative authority, privacy and security arrangements must be available so that a judgement can be made about the capability of agencies to align their practices with specified privacy controls and requirements.

Specific data elements, information flows, proposed deployment models and SOPs (or equivalent) were not available, despite request, during the PIA process, nor was a PAA template available for review.

Information regarding the applicable state and territory legislative, privacy, and protective security arrangements was available but incomplete. As this information provides the foundation for LECAC agencies meeting the requirements set out in the FMS Data Sharing Framework, a consultation process was undertaken with state and territory LECAC agencies using a Questionnaire developed by Bainbridge Associates to identify applicable legislative, privacy and protective security arrangements as specified in the FMS Data Sharing Framework. The results of the Questionnaire process are summarised in Chapter 4. Appendix D provides a collation of all agency responses. These provided the baseline for the LECAC PIA.

In order to determine whether or not LECAC agencies are capable of meeting the Commonwealth's 'best practice privacy controls' adopted for the NFBMC (which they have signed up to), a *purposive approach* has been taken to the privacy analysis. This approach focuses upon each LECAC agency's ability to meet legislative, privacy and protective security requirements via SOPs and/or other agency-level policies and procedures. This recognises that agencies are subject to a wide range of mandated government policies and processes already, including for information-sharing purposes as well as in relation to protective security and information privacy. These can be leveraged for FVS/FIS purposes.

[17] With the benefit of hindsight, it is apparent that the LECAC PIA required significantly more time assigned to consultation activities. The NDFLRS PIA, for example, involved individual consultations with privacy regulators and all roads agencies. At a minimum, the LECAC PIA warranted individual (and potentially multiple) consultations with all LECAC agencies rather than the two-hour teleconference provided for in the PIA project brief.

This finding proceeds from an assumption (based on the outcomes of the Questionnaire Process), that it is possible for LECAC agencies to demonstrate – or adjust their internal processes to demonstrate – that they can achieve functional privacy equivalence. Jurisdictions with well developed privacy and security frameworks will find it easier to establish their 'credentials' than agencies that do not have existing frameworks to reference.

This approach considers that:

- Rather than seeking to ground the responsible collection and handling of personal information in privacy legislation or privacy principles alone, it may be both feasible and desirable (as well as necessary in some cases) to recognise or highlight *other options* for providing meaningful privacy protection.
- As currently acknowledged by LECAC agencies, whether or not privacy legislation or principles apply to their activities, they are committed to protecting the privacy and security of FVS/FIS data information that comes into their possession *as a consequence of* their execution of the IGA.
- In the absence of a consistent privacy law framework and the presence of privacy law exemptions, it will be critical for LECAC agencies to deploy an effective approach to *privacy management*. (This is also a requirement under clause 16(4) of the Participation Agreement.) Put another way, privacy management rather than privacy legislation should comprise the (practical) focus of compliance efforts following the LECAC PIA.
- To the degree that LECAC agencies are exempt from compliance with data quality and data security privacy principles, it will be critical for them to deploy an *effective approach to protective security*.
- There is significant value in LECAC agencies understanding the relevance and importance of privacy and data protection requirements, regardless of their privacy 'status'. This includes:
    - specifying the purpose of collection;
    - limiting the collection, use and disclosure of personal data to that which is necessary and proportionate;
    - ensuring there is fairness, accountability and transparency;
    - ensuring appropriate data quality, integrity and security measures;
    - ensuring that complaints are handled appropriately; and
    - implementing processes to monitor the way the FVS and FIS are functioning over time (e.g. establishment of metrics and collection of relevant data) and undertaking a benefits realisation process.
- In practical terms, embedding or operationalising FMS Data Sharing Framework requirements within Police Manuals, SOPs or other policies and processes – including identifying where these may already exist – will have a positive impact upon LECAC agencies' privacy and security practices and is the preferred approach to LECAC agency privacy compliance.

Further information about operationalising privacy is provided Chapter 6.

Recommendation 2 – Privacy Governance Framework and Management Standards
Clause 16.4 (a) of the Participation Agreement requires each agency to develop (or amend) its Privacy Governance Framework and Management Standards to ensure that they are adequate and reflect the management of the flow of information through the

FVS and FIS. The OAIC's *Privacy Governance Framework and Management Standards* provides a default approach to privacy management. Clause 16(b) provides that each LECAC agency must provide a copy of its Privacy Governance Framework and Management Standards to the Hub Controller upon request.

It is recommended that all relevant LECAC agencies be required to demonstrate an effective approach to privacy governance and management prior to negotiating a Participation Access Arrangement. In particular, each LECAC agency must identify a suitable regulator within its jurisdiction that is capable of receiving and dealing with complaints.

Recommendation 3 – Focus upon Operationalisation of Privacy Requirements

It is recommended that LECAC agencies should be required to demonstrate how they will operationalise all relevant privacy requirements as a pre-condition to gaining access to the FVS and FIS, including the incorporation of relevant FVS and FIS requirements into agency/Police Manuals, Standard Operating Procedures (or equivalent), policies and processes.

Each agency must document its approach to achieving practical privacy compliance and submit it as part of the Participation Access Arrangement process. This recommendation should be read alongside the requirement for each agency to review, update and/or develop its Privacy Governance Framework and Management Standards as required under clause 16.4(b) of the Participation Agreement (Recommendation 2).

4 LECAC PIA – Legislation, Privacy and Protective Security

4.1 LECAC PIA Questionnaire

As noted above (section 3.4), in the absence of draft or proposed PAAs, LECAC agencies were asked to identify the legislative authority, privacy legislation and protective security arrangements applicable to each LECAC agency.

Bainbridge Associates developed a Questionnaire to obtain information about these arrangements directly from each state and territory LECAC agency participating in the PIA process. While some of this information had already been provided by some agencies, the questionnaire process was intended to provide a comprehensive, 'point in time' record of state and territory arrangements, giving agencies an opportunity to confirm the accuracy and completeness of the information or to provide updated or new information. A list of the LECAC agencies that responded to the Questionnaire is provided below (see Figure 9).

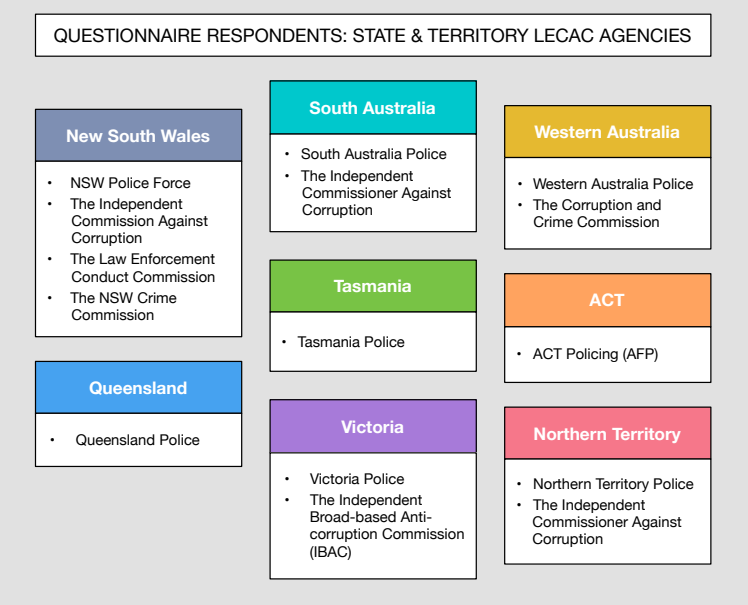


Figure 9 – Questionnaire Respondents - State and Territory LECAC Agencies

LECAC agencies' responses to the Questionnaire directly informed Bainbridge Associates' findings and recommendations in relation to state and territory LECAC agencies' use of the FVS and FIS. Home Affairs provided summaries of Commonwealth LECAC agencies' legal and protective security arrangements, which provided the basis for findings and recommendations in relation to Commonwealth agencies.

4.2 FVS and FIS Arrangements

As discussed in Chapter 3, the FVS and FIS will operate within a complex and interlocking set of binding arrangements, including the IGA and the FMS Data Sharing Framework. Looked at from the perspective of access, the IGA provides the overarching authority for the NFBMC, while the Participation Agreement functions as the key to LECAC agencies' access to, and use of, the FVS and FIS.

A review of FMS documents *as a whole* demonstrates a clear intention that FMS information sharing will be based upon a foundation of legislative authority, privacy protections (including regulatory oversight), and protective security requirements. While the specific role of privacy legislation within the FMS Data Sharing Framework has been

questioned in this PIA report, it is apparent that privacy principles and privacy management remain highly relevant to LECAC agency access to, and use of, the FVS and FIS.

The primary issue is *how* LECAC agencies will meet, comply with or support the requirements set out in these arrangements.

A summary of the requirements relating to legislative authority, privacy and security in the IGA, the Participation Agreement and the FVS and FIS Access Policies, identified via the Questionnaire process, is provided at Appendix A. These can be further summarised as follows (see Figure 10, below).

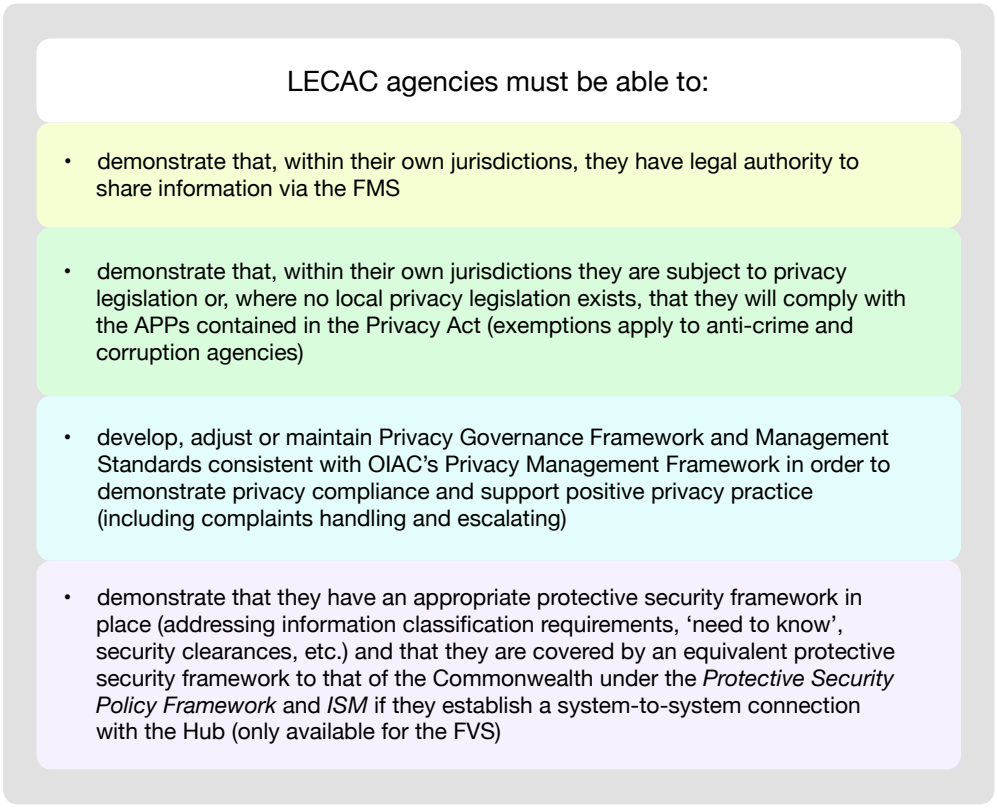


Figure 10 – Core Legal, Privacy and Protective Security Requirements

Three of these categories – privacy law, privacy management and protective security – have a Commonwealth default in the event that a state or territory LECAC agency does not have coverage. These are:

- *Privacy legislation: Privacy Act 1988* and the APPs
- *Privacy management*: OAIC's Privacy Governance Framework and Management Standards
- *Protective security:* Protective Security Policy Framework (PSPF) and Information Security Manual (ISM)

4.3 Overview of State and Territory LECAC Questionnaire

4.3.1 Legal Authority

There is a range of existing legislation and common law authorising LECAC agencies to undertake various law enforcement functions and activities. However, obtaining a complete list of legal authorities via the Questionnaire process proved difficult, partly

because of the way the questions were formulated and partly because of the way LECAC agencies interpreted the questions.

While an 'NFBMC Act' is not required to support implementation of the FVS and FIS, legal authority has been established as a pre-condition to sharing data via the FVS and FIS.[18] As illustrated above (Figure 8, section 2.3.3), in order to construct a query for the FIS, step 1 requires LECAC agencies to cite the relevant legal authority and section and specify the permitted purpose. Using Figure 8 as an example, this includes specifying the relevant legal authority (e.g. the *Crimes Act 1914*) and section reference (e.g. s.24AA (Homicide)). These fields will be chosen from a pre-set, drop-down menu, which indicates that there is an intention to identify and list relevant legislation in relation to FIS access. This information will also be required for the PAA.

Another question sought to identify whether or not legislative amendments were required at the state or territory level in order to enable full participation. The responses indicated a degree of uncertainty as to whether or not amendments to state/territory legislation will be required. Queensland provides a useful example, having enacted the *Police and Other Legislation (Identity and Biometric Capability) Act 2018.* This legislation was developed in response to the requirement under the IGA for each jurisdiction to make necessary legislative amendments to facilitate the collection, use and disclosure of facial images and associated identity information between NFBMC participants (clause 8.5).

Queensland identified a need to amend transport and Queensland Police Service (QPS) legislation in order to provide explicitly that relevant information may be shared for the purposes of the FMS. Amendments to transport legislation were required to enable the collection, use and disclosure of driver licence data while amendments to QPS legislation were intended to overcome 'potentially perverse outcomes' arising from the fact that – in the absence of legislative amendment – other jurisdictions would gain access to Queensland drivers' licence data for non-transport law enforcement purposes without the requirement for an authority from a justice of the peace, while Queensland Police would be unable to access drivers' licence data for non-transport law enforcement purposes and on a request-by-request basis. Since the PIA commenced, New South Wales has also enacted legislation to support the NFBMC at the state level: *Road Transport Amendment (National Facial Biometric Matching Capability) Act 2018.*

As each State and Territory LECAC agency operates under, and is subject to, different legislative regimes, it is not possible to extrapolate directly from the Queensland and New South Wales amendments whether other jurisdictions will need to undertake similar amendments. However, the approach taken in the Queensland legislation, in particular, the potential for disjunctions to arise between local and national information flows, does point to the relevance of each jurisdiction confirming whether or not additional legislative support is required prior to seeking access to the FVS and FIS. This will enable LECAC agencies to meet the requirement outlined in clause 8.5 of the IGA, to ensure that they have all relevant legislative authorisations required to share identity information via the NFBMC.

4.3.2 Compliance with Privacy Legislation

The impact of Australia's privacy patchwork, in conjunction with a varying range of privacy law exceptions and exemptions, means that consistent compliance will require consistent operationalisation. Table 2, below, provides an overview of the responses received from LECAC agencies regarding their compliance with privacy legislation.

[18] For example, no Victorian statute confers specific powers on police to collect and handle FMS or like information. In general terms the legal authority of Victorian police to do so is derived from s.51 of the *Victoria Police Act 2013*, which confers on police officers the duties and powers of a constable at common law.

Commonwealth, State and Territory Privacy Legislation			
Juris-diction	**Privacy Law**	**Agency**	**Exemption**
Cth	*Privacy Act 1988*	• Home Affairs (ABF) • AFP • ACIC (ACC) • ACLEI	Applies Applies Exempt [s.7 (1)(a)(iv)] Exempt [s.7 (1)(a)(iiia)]
NSW	*Privacy and Personal Information Protection Act 1998* *Health Records and Information Privacy Act 2002*	• NSW Police • Independent Commission Against Corruption • NSW Law Enforcement Conduct Commission • NSW Crime Commission	Each agency is exempt except for administrative and educative functions
VIC	*Health Records Act 2001* *Privacy and Data Protection Act 2014*	• Victoria Police • Victoria Police • Independent Broad-based Anti-corruption Commission	Applies Applies with additional exemptions to exceptions Partially exempt
QLD	*Information Privacy Act 2009*	• Queensland Police Service	Partially exempt through a combination of specific exemptions, permitted non-compliance and a specific document exemption.
SA	South Australia has no privacy legislation. Information privacy is regulated by administrative arrangements established under Premier and Cabinet Circular 12 (as amended 6 February 2017)	• South Australia Police • Independent Commission Against Corruption	N/A The instruction does not apply
ACT	*Information Privacy Act 2014* *Health Records (Privacy and Access) Act 1997*	• ACT Policing (AFP)	Covered by the *Privacy Act 1988* (Cth), not ACT legislation
TAS	*Personal Information Protection Act 2004*	• Tasmania Police	Applies with additional exemptions to exceptions
WA	Western Australia has no privacy legislation. The Western Australia Public Sector Commissioner's Circular Premier's Circular 2014-2	• Western Australia Police • Western Australia Crime and Corruption Commission	N/A N/A

	establishes a Policy Framework and Standards for Information Sharing between Government Agencies and refers to Information Privacy Principles but does not provide a definition of these		
NT	Information Act 2003	• Northern Territory Police	Applies with additional exemptions to exceptions

Table 2 – Compliance with Privacy Legislation

In addition to the practical issues this raises – for example, ensuring consistent or equivalent privacy protection across the board for Commonwealth, state and territory agencies – privacy exemptions raise potential privacy perception risks.

The most significant of these relates to the role assigned to privacy legislation in the FMS Data Sharing Framework. As illustrated in Appendix A, each of the major agreements, policies and arrangements places considerable emphasis upon the need for participants to protect privacy and comply with applicable privacy legislation or – in the case of Western Australia and South Australia, where no privacy legislation is in place – to comply with the Privacy Act's APPs as if they were APP entities (i.e. they will be contractually bound under the Participation Agreement).

References to strong privacy protection throughout the FMS agreements will only be credible if they are matched in practice. Any misalignment between promised protections and reality may result in significant privacy perceptions arising that are not easily addressed or mitigated.

The PIA finds that, in this context, a focus upon privacy legislation does not provide the most effective response to concerns about privacy. Instead, as outlined in Chapter 3, it is preferable for LECAC agencies to demonstrate how they will operationalise the privacy requirements and controls contained in the FMS Data Sharing Framework (i.e. the 'functional equivalence' approach).

4.3.3 Protective Security

The question about the applicability of privacy legislation and privacy principles to the FVS and FIS also points to a potential weakness in some jurisdictions in relation to protective security. Table 3, below, illustrates the responses received from LECAC agencies about their compliance with protective security requirements

State & Territory Protective Security Frameworks		
Jurisdiction	**Security instrument**	**Comment**
NSW	NSW Digital Information Security Policy	Coverage restricted to information security, not protective security. Not as comprehensive as the Commonwealth PSPF
VIC	*Privacy and Data Protection Act 2014* (Vic) Victorian Protective Data Security Framework Victorian Protective Data Security	Legislatively-based protective security framework and standards consistent with Commonwealth PSPF

	Standards	
QLD	Information Security Information Standard (to October 2018) Information Security Policy IS 18:2018 (from October 2018)	ISP covers some protective security issues but is not as comprehensive as the Commonwealth PSPF
SA	Department of Premier and Cabinet Protective Security Policy Framework PC030, February 2012	Covers protective security
TAS	Tasmanian Government Information Security Policy 2011 Tasmanian Government Information Security Policy Manual	Coverage is not as detailed as Commonwealth PSPF
WA	Whole of Government Digital Security Policy 2017	Focus is on digital (ICT) security, not protective security
ACT	ACT Protective Security Policy Framework.	ACT Policing is subject to the AFP protective security policy framework and is covered by the Commonwealth PSPF.
NT	Nil	

Table 3 – Protective Security Frameworks

Where state and territory LECAC agencies are required to comply with a set of privacy principles, this includes a data security principle. This provides a stronger (legislative) basis for compliance with important information security requirements. This has an important flow-on effect: in the absence of compliance with a data security principle, the need to demonstrate compliance with a formal protective security framework will be higher.

In relation to protective security, having been subject to legislatively backed law enforcement data security standards since 2008 (since superseded by the regime established under the *Privacy and Data Protection Act 2014*) and the Victorian Protective Data Security Standards since 2014, Victoria Police can point to a documented set of standards that it is required to comply with and that have legislative backing. The Victorian Protective Data Security Standards were designed to align with Commonwealth protective security arrangements, enabling broadly consistent practices (subject to specific jurisdictional requirements). A number of other LECAC agencies state that they already comply with the PSPF or an equivalent state or territory protective security policy framework. Currently, there is no agreed way to assess consistency in approaches to protective security across Australia without examining arrangements at a detailed level within each jurisdiction.[19] This makes it difficult to judge whether or not an appropriate or equivalent standard is in place.

Questionnaire responses indicated that a number of agencies are currently preparing to implement protective security policies or frameworks. Until these processes are complete, they will need to explain how they plan to meet protective security requirements listed in the Participation Agreement (e.g. classification processes and security clearances). Where agencies stated that they will be adopting the 'default' position of Commonwealth privacy and security arrangements, i.e. the APPs contained in Schedule 1 of the Privacy Act 1988 and the PSPF (and ISM) (presumably in relation to system-to-system connections for FVS

[19] It is important to note that the LECAC FMS PIA was not commissioned as a set of nine individual PIA processes.

processing), it will be necessary to confirm that this occurs and that steps are taken to ensure that security requirements are adhered to on an ongoing basis.

Some of the concerns raised above may be addressed through the security risk management plans specified in the FMS Data Sharing Framework and other related requirements but no plans were reviewed during the PIA process.

The requirement to prepare annual compliance statements should help to ensure that there is a sufficient degree of transparency and accountability at the level of each LECAC agency. However, as noted above, LECAC agencies need to demonstrate how they will operationalise the security requirements and controls contained in the FMS Data Sharing Framework.

Prior to finalisation of the PAA process, a statement of legislative authority is subject to a local review process (including legal sign off). It is considered that the PAA template format has the capacity to document legislative compliance requirements at a sufficient level of detail and 'readability' to establish that FMS Data Sharing Framework requirements have been met. In particular, the PIA finds that the PAA process will help LECAC agencies confirm that they have the requisite legal authority to share information via the FVS and FIS.

The statement of legislative compliance developed for each LECAC agency's PAA can be used to develop a summary statement of each agency's rationale for accessing, using and disclosing FVS and FIS data. This information can also be re-used in jurisdictional privacy policies and statements about LECAC agency participation in the NFBMC.

5 Mapping the APPs

In Australia:

- privacy legislation and privacy principles differ across the Commonwealth, states and territories; Western Australia and South Australia do not have privacy legislation;
- privacy legislation applies differentially to LECAC agencies; and
- all Australian privacy laws contain some form of law enforcement exception or exemption, including:
    - exceptions within the privacy principles;
    - exemptions within the privacy law; and
    - exemption from the privacy legislation.

As noted above, this complicates the PIA process, but does not mean that privacy is redundant. Information privacy legislation is intentionally principles-based. Privacy laws enshrine a set of information privacy principles based upon the information lifecycle (collection through to destruction) and a common antecedent – the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980).[20] This means that – while the wording and details may differ – there is a degree of consistency across the various privacy laws and principles.

Informed by the FVS and FIS information flows documented in Chapter 2, this chapter considers the APPs contained in the Privacy Act. While Bainbridge Associates was required to map LECAC information flows against the APPs, the APPs do not apply to a majority of LECAC agencies. In the context of the LECAC PIA, therefore, the APPs are considered as a generic or common set of privacy principles, capable of guiding privacy practice and policy development rather than regulatory/compliance requirements. Where recommendations are made, they relate to Home Affairs, which is subject to the Privacy Act and the APPs.

APPs relating to private sector entities and private-sector specific privacy principles are excluded from the following account.

The high-level APP mapping exercise outlined below should be viewed as contributing to a general understanding of FVS and FIS privacy issues and risks overall. It does not purport to be a full PIA mapping process, which would require the input of more detailed information flow diagrams.

APP 1 – Open and transparent management of personal information

This 'openness' principle aims to ensure that agencies manage personal information in an open and transparent way. It requires agencies to have clearly expressed and up-to-date policies on their management of personal information and to ensure that the information is readily available should anyone ask for it. APP 1 obligations aim to ensure that agencies take reasonable steps to:

- Comply with the APPs; and
- Deal with privacy inquiries and complaints appropriately.

Compliance with APP 1 is a critical foundation stone for general privacy governance and compliance as well as a clear demonstration of an agency's awareness of, and commitment to, the responsible collection and handling of personal information (including health and sensitive information). APP 1 is relevant to all participants in the NFBMC, although operational responsibility

[20] Organisation for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980): http://oecdprivacy.org. See also, OECD, *Thirty Years After the OECD Guidelines* (2011): http://www.oecd.org/sti/ieconomy/49710223.pdf.

for addressing openness issues lies with Home Affairs as the scheme administrator.

Relevance of the Openness Principle to LECAC Agencies

The openness principle is relevant to LECAC agency's access to, and use of, the FVS and FIS. As a foundation stone for effective information privacy practice, APP 1 goes to the heart of FVS and FIS privacy management. It requires that implementation of the FVS and FIS be accompanied by a relevant privacy policy and related privacy information. Compliance with APP 1 is also a matter of good governance. Failure to provide information about the FVS and FIS (as services within the NFBMC) impacts negatively upon individuals' privacy.

However, openness cannot be addressed effectively in relation to the FVS and FIS in isolation from consideration of the NFBMC as a whole. The PIA considers that it is important for participants to conceptualise the NFBMC as an *information-sharing scheme* in which privacy and security, FVS and FIS, are viewed as requiring an *end-to-end* and *whole-of-information-lifecycle* approach across the whole of Australia.

The PIA finds that, as the scheme administrator and department responsible for the NFBMC, Home Affairs is best placed to take primary responsibility for developing a relevant and fit-for-purpose NFBMC privacy policy, as well as other privacy-related information, with input provided by participants on an as-needs basis. This information could be published via an NFBMC website managed by Home Affairs.

Once Home Affairs has developed an NFBMC privacy policy, other Commonwealth, state and territory agencies should leverage the content developed by Home Affairs within their own privacy policies in order to promote consistency. While it is not desirable for each participant to have a different FMS privacy notice or policy, some variation will be necessary. For example, the ACT has noted the importance of human rights, specifically the right to privacy, and the need to ensure that participation in the NFBMC is consistent with the human rights principles as set out in the *Human Rights Act 2004* (ACT). This may require some amendment to, or extension of, the template text.

The Home Affairs privacy policy currently provides information about the individual's right to seek access to and/or correction of personal information held by an agency and how to do so and how to make a complaint about a potential breach of privacy. The NFBMC privacy policy will also need to provide information about making a privacy complaint and will require the development of a consistent complaints-handling process.

Any development of an NFBMC privacy policy should draw upon the work that has already been undertaken to build privacy into the FMS (NFBMC). For example, the guiding principles that have underpinned the development of the FMS should be referenced. These include:[21]

- *Privacy by Design:* the NFBMC adopts a 'hub and spoke' architecture to avoid the creation of a centralised biometric database. In other words, the hub will *not store any data* other than the necessary audit information.
- *Data owners maintain access controls:* each agency participating in the NFBMC will *retain control* over which other agencies may access its information. The scope of terms of this access will be set out in formal agreements between participating agencies.
- *Identity resolution by users:* the NFBMC provides a tool to assist agencies with identity-based decisions, but ultimate *responsibility for identity resolution decisions rests with individual user agencies* (i.e. the agency that requests a data match).
- *Protect legally assumed identities:* the NFBMC must *protect assumed identities* from either deliberate or inadvertent *discovery*.

Home Affairs has already published the FVS Access Policy and the FIS Access Policy online. This contributes to openness. Further publication of relevant policies and reports should be considered. Consideration could also be given to the development of a NFBMC 'logo' to be placed on each participant's website. Clicking on the logo could launch an NFBMC website, containing a range of relevant information about the NFBMC, including a privacy policy (incorporating reference to the

[21] AGD, *Privacy Commissioners Forum – NFBMC Presentation:* (21 February 2018).

FMS).

APP 2 – Anonymity and pseudonymity

APP 2 requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym with limited exceptions.

APP 2 is designed to ensure the ability of people to interact with organisations – including government organisations – without identifying themselves where this is lawful and practicable. For example, accessing the Home Affairs website to read the *Face Matching Services Fact Sheet* does not require individuals to identify themselves.

Relevance of the Anonymity Principle to LECAC Agencies

This principle has limited relevance to LECAC agencies. It is not practicable for the FVS or FIS to operate on an anonymous/pseudonymous basis as its core purpose involves the verification and/or identification of individuals. Further, the use of, or participation in, the FMS will be subject to legislation authorising the verification and/or identification of individuals (with or without consent, depending upon the particular use case scenario).

APP 3 – Collection of Solicited Information

APP 3 outlines when an agency can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information. If the initial collection requirements outlined in APP 3 are managed well, it is likely to result in compliance with the other APPs. To the degree that collection is not handled well, it will invariably lead to problems 'downstream'. Thus, APP 3 is critical to achieving privacy compliance under the Privacy Act.

At the Commonwealth level, 'sensitive information' includes biometric information and templates. Ordinarily, under APP 3.3, consent is a precondition to the collection of sensitive personal information. However, APP 3.4(a) provides that consent is not required where the collection is required or authorised under law.

Relevance of the (Solicited) Collection Principle to LECAC Agencies

The consideration of collection principle requirements is relevant to all participants in the NFBMC, not just LECAC agencies, as it focuses attention upon issues of necessity, proportionality and transparency. At times, collection requirements can operate alongside privacy exceptions, providing a means of demonstrating a commitment to privacy. APP 3 provides that sensitive information (here, biometric information or biometric template) can be collected with the individual's consent (APP 3.3) or on the basis of legal authority (APP 3.4).

LECAC agency participation in the FMS differs in relation to the FVS (verification of identity) and FIS (identification). Collection of data via the FVS is predicated upon LECAC agencies either obtaining consent or relying upon a relevant legal authority. Collection of data from the FIS does not require individual consent.

Where consent is relied upon for the FVS (e.g. the FVS is used to verify a job applicant's identity), it must be fully informed and voluntary. However, this should not be viewed as overriding existing law enforcement practices where consent is not sought, e.g. checking a driver's details in relation to road safety. The introduction of the FVS will not require agencies to develop new consent processes where they are not currently required. Existing policies and procedures should be extended to the use of the FVS.

It is preferable for LECAC agencies to rely upon legislative authority to access/use the FVS, rather than consent where it is available. If there is doubt about the ability to obtain a valid consent (in particular, that it is freely given and fully informed) it is preferable to rely upon legal authority. Based on feedback from LECAC agencies, a minority of FVS access will be consent based.

There is a need to ensure clarity when considering the use of the FVS in a law enforcement context

(the subject of this PIA) versus its use as part of Australia's identity infrastructure, which is out of scope. See section 2.3.1, above.

The FIS poses a higher degree of privacy intrusiveness than the FVS. However, it is noted that limits have been imposed on the amount of data provided and when it is provided; maximum limits have been set on the return of images and specific provisions will be developed for children and young people (to provide additional safeguards). Policies, arrangements and the Participation Agreement found within the FMS Data Sharing Framework indicate the sensitivity of biometric information/templates. This is important, as state and territory privacy laws do not include biometric information/templates within their definitions of sensitive information.

The development of standing offers (pre-determined sets of data) should consider requirements to limit collection; they should not result in the provision of more data than is required for a specific purpose.

APP 4 – Dealing with Unsolicited Personal Information

APP 4 outlines how APP entities must deal with unsolicited personal information. As access to and use of the FVS and FIS will not involve the collection of unsolicited personal information, APP 4 is not relevant to LECAC agencies.

APP 5 – Notification of the collection of personal information

APP 5 outlines when and in what circumstances an agency that collects personal information must notify an individual of certain matters. Notice requirements exist in addition to privacy policy requirements listed under APP 1.

A privacy notice performs two main functions:

1. It provides a mechanism to promote transparency and accountability in relation to the collection of personal information.
2. It provides individuals with information to help them make a decision about whether or not to provide personal information. (Noting that it may be nonsensical to refer to the 'voluntary provision' of personal information where the information is collected on the basis of legal authority and no 'choice' is being offered to the individual.)

A privacy collection notice is not the same as an APP entity's privacy policy. A privacy policy as required under APP 1 is meant to articulate an agency's overarching approach to its management of personal information; it is unlikely to address the specificities of a particular initiative, data collection or program. A collection notice is drafted to fit the specific circumstances of an initiative, data collection or program. This requirement applies to Commonwealth/ACT LECAC agencies unless they are subject to an exemption. Equivalent requirements apply to LECAC agencies where state/territory privacy legislation is applicable.

In practice, APP 5 requires agencies to document their approach to specific collection issues, in particular:

- Who is collecting the personal information
- Whether collection occurs directly from the individual or via a third party
- Whether the collection is required or authorised by law
- The purposes for which the information is collected
- The main consequences for the individual (if any) if the information is not collected
- Any other entities to which the APP entity usually discloses personal information
- That the APP privacy policy provides information about how to access and/or seek correction of personal information held by an APP entity
- That the APP privacy policy provides information about how to make a complaint about a potential breach of privacy
- Whether the APP entity is likely to disclose the personal information to overseas recipients and what this involves

Relevance of the Notification Principle to LECAC Agencies

An NFBMC (FMS) collection notice is relevant to all NFBMC participants and can be implemented alongside the exercise of any legislative authority or agency exemption (subject to any need for operational secrecy).

As discussed above in relation to APP 1, to the greatest degree possible, privacy content should aim for consistency and clarity across the NFBMC scheme as a whole, for example, it should explain how the NFBMC works, how it is governed, how it is informed by and aligned with privacy requirements and so on.

Notice requirements are primarily the responsibility of Data Holding Agencies. Where an indirect collection of information occurs – for example, a LECAC agency collects driver licence information via the FVS or FIS – Data Holding Agencies should advise individuals that their information might be disclosed to LECAC agencies in this way. LECAC agencies should check that –where applicable – Data Holding Agencies have appropriate notices in place that account for LECAC agencies.

It is expected that Data Holding Agency/Requesting Agency's existing privacy collection notices will be reviewed and updated (as/if required) to incorporate reference to the NFBMC. As each LECAC agency signs up to the Participation Agreement, a simple compliance check could be undertaken to see whether or not existing notices are sufficient or require amendment.

APP 6 – Use or Disclosure of Personal Information

APP 6 outlines the circumstances in which an APP entity may use or disclose personal information that it holds. APP 6 is concerned with ensuring that personal information is only used and disclosed for the primary purpose for which it was collected or (in the case of agencies) a related secondary purpose that an individual would reasonably expect (directly related in the case of sensitive or health information). All other uses or disclosures should operate on the basis of consent or lawful authority or as otherwise permitted under APP 6.2. Any future extensions to use or disclosure will require careful management and justification (i.e. in relation to necessity, proportionality) otherwise they risk being (perceived) as function creep.

Relevance of the Use or Disclosure Principle to LECAC Agencies

All LECAC agencies are exempt from/have an exception to the use and disclosure principle to enable them to undertake their law enforcement activities effectively. However, the basic principle of aligning the purpose of collection with use or disclosure is useful and likely to be consistent with data security requirements (e.g. regarding unauthorised access). The primary purpose of the FVS is the verification of an individual's identity; the primary purpose of the FIS is to assist in the identification of unknown individuals.

As noted above, LECAC agency participation differs in relation to the FVS and FIS. Use of the FVS is predicated upon LECAC agencies obtaining consent or relying upon a relevant legal authority, while use of the FIS is predicated upon LECAC agencies exercising a relevant legal authority. However, as noted in relation to the discussion of APP 3, where legal authority exists and it is being exercised for law enforcement purposes it should be used instead of a consent mechanism. Other APP 6 exceptions may be available to agencies participating in the FMS, such as APP 6.2(e), which is designed to enable non-law enforcement agencies to disclose information to a LECAC agency, but are not directly relevant to LECAC agencies.

APP 6 raises the issue of function creep (which also applies to APP 9 in relation to the adoption, use or disclosure of government identifiers). Currently, the umbrella acronym of 'FMS' covers each of the services to be provided by the NFBMC. These are broader than the LECAC PIA, which is focused upon the FVS and FIS only. For example, there is an intention to extend access to the FVS to parts of the private sector for 'Know Your Customer' purposes or to enhance government services relating to identity verification.

If/as the FVS is extended to the private sector, a potential privacy perception risk relating to function creep may arise. The role of the Coordination Group and the Minister's proposed powers under the IMSB should also be considered from a privacy perspective, as they have the capacity to

improve or detract from NFBMC privacy safeguards. General concerns about FVS function creep will inevitably 'leak into' the FIS, despite athe intention to restrict the FIS to law enforcement and national security agencies. This adds to the argument that there be a clear demarcation between law enforcement access to and use of the FVS (as a verification tool) and the FIS (as an identification tool) as well as the presentation of the FVS as a broader, consent-based, identity verification service.

Finally, there is no privacy requirement forcing information systems to remain the same over time. There may be legitimate public policy reasons for extending the FMS to cover additional purposes or participants at a future point in time. Developing processes to prevent function creep and foster the informed extension of information systems provides one way to avoid (actual or perceived) examples of function creep.

APP 7 – Direct Marketing

APP 7 outlines the conditions under which private sector organisations may use or disclose personal information for direct marketing purposes. It is not relevant to the FVS/FIS, which are restricted to government agencies at this point.

APP 8 – Cross-border disclosure of personal information

APP 8 outlines the steps that an APP entity must take to protect personal information before it is disclosed overseas.

APP 8 is designed to address issues about the transfer of personal information beyond national boundaries. In particular, it focuses on situations where the transfer of personal information overseas may result in the loss of protection for privacy unless steps are taken to mitigate this risk.

Relevance of Cross-border disclosure of personal information to LECAC Agencies

The FVS/FIS will not involve any international, cross-border disclosure of personal information (sometimes referred to as transborder data flows); all data will be held within Australia. No specific compliance issues identified at this point in time.

APP 9 – Adoption, use or disclosure of government related identifiers

APP 9 outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 9 addresses the privacy issues that may arise from the allocation and use of unique identifiers, particularly where these have been issued by government(s) on a large scale.

Relevance of the Identifiers Principle to LECAC Agencies

APP 9 applies differentially to agencies (public sector) and organisations (private sector). APP 9 does not apply to Commonwealth, state or territory LECAC agencies except to the degree that section 7A (or an equivalent State/Territory provision) may apply. This scenario does not arise in relation to the FMS.

It is noted that APP 9 (and equivalent privacy principles at the state and territory level) has the capacity to raise issues around function creep if there is any future proposal to expand access to the FVS/FIS to the private sector and the collection/handling of identifiers is also involved.

APP 10 – Quality of Personal Information

APP 10 requires agencies to take reasonable steps to ensure that the personal information they collect is accurate, up-to-date and complete. An agency must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having

regard to the purpose of the use or disclosure.

Relevance of the Data Quality Principle to LECAC Agencies

Data quality – including its integrity – is core to an effective FVS and FIS. Overall, the deployment of the FVS is expected to improve the data quality of government databases, resulting in a reduction of data quality issues.

Importantly, while the FVS and FIS will provide a tool to help LECAC agencies resolve verification or identification issues, they will not be the primary or only source of information. Any data obtained via the FVS and/or the FIS will be subject to further assessment and subsequent confirmation, thus there are further checks and balances in the system. Annual compliance audits should also assist in the identification of any data quality and security issues.

As noted in Chapter 7, and in previous PIA reports, the algorithms enabling biometric face matching services may raise concerns – particularly in relation to the generation of false positives and false negatives including where matching involves images of minors – if appropriate steps are not taken to mitigate or otherwise manage these risks. Recommendations have been made in this report to address these types of concerns, both at a technical level and in relation to benefits realisation and personnel training. Previous PIAs have also made relevant recommendations to promote data quality. The approach taken by Home Affairs – which is based upon a combination of human and technological (biometric) face matching – represents best practice/is most likely to produce accurate results.

Feedback provided in response to the review draft of the LECAC PIA report stated that data quality was a significant concern. However, the basis for this statement – discussions held by a jurisdictional working group – is not available to Bainbridge Associates for review. The PIA is not in a position to make a judgement call about its accuracy.

APP 11 - Security of Personal Information

APP 11 requires agencies to take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An agency has obligations to destroy or de-identify personal information in certain circumstances.

Bainbridge Associates was not able to review FVS and FIS security arrangements directly but was provided with a summary of relevant security arrangements during the PIA process. This information documented a range of significant and specific security measures that will be applied to the FVS and FIS (and NFBMC as a whole). This information has been relied upon to produce the following summary. Previous PIA processes also examined security arrangements in detail (for example, review of an NFBMC IRAP Compliance report).

FVS and FIS security and retention requirements will be addressed through a combination of legislative, technical and policy measures. Obligations under APP 11 initially – and largely – accrue to Home Affairs as the party responsible for the development, implementation and ongoing management of the FVS and FIS. However, LECAC agencies will be responsible for ensuring that all relevant security requirements have been operationalised at the state/territory level. A table summarising the key security measures to be instituted by the Commonwealth is provided below.

Relevance of the Data Security Principle to LECAC Agencies

The data security principle is directly relevant to LECAC agencies. It has been assigned a high priority throughout the development of the NFBMC. A number of security arrangements have been established for the NFBMC that will help LECAC agencies provide a secure environment for FVS and FIS data. Commonwealth, state and territory LECAC administrators will be able to review audit information against authorised users to check every transaction relating to their own data. This will require LECAC agencies to ensure that they have appropriate policies in place to monitor and review audit logs. Additionally, there are requirements for LECAC agencies to keep their own audit data in relation to their transactions (as Requesting Agencies) in addition to the audit data captured by the Hub. This data is also required in order for LECAC agencies to produce their annual compliance statements.

The level and type of auditing required will differ in the case of system-to-system connections to the Hub (for the FVS). State and territory LECAC agencies must be able to demonstrate that they have appropriate protective security arrangements in place (i.e. jurisdictional frameworks provide equivalent protection and are aligned with the Commonwealth's PSPF). Commonwealth LECAC agencies are already subject to the PSPF. Additionally, in order to meet general security requirements set out in the FMS Data Sharing Framework, state and territory LECAC agencies will be required to demonstrate how they will ensure FMS data is protected within their sphere of control, including data sensitivity assessment and classification.

It is unclear at this point in time whether or not all LECAC agencies are both (1) subject to an appropriate protective security framework, and, if so, (2) capable of complying with the designated protective security framework. (See also, section 4.3.3, above.)

KEY SECURITY MEASURES (Commonwealth)	

Information and Physical Security
• The Commonwealth has committed to the adoption of best practice security and access arrangements aligned with the PSPF and the ISM;
• Home Affairs will commission independent penetration and vulnerability tests prior to 'go live' as well as ongoing testing and monitoring;
• ASD will be consulted on system design;
• FMS will be subject to IRAP assessment and certification;
• Ongoing 24/7 monitoring and deployment of state-of–the-art encryption, anti-virus and intrusion detection as required for an IT system that has been classified as 'Protected' under the PSPF; and
• Physical and personnel security arrangements in accordance with Zone 4 (Secret) requirements.
	Access Controls
	• Once operational, the FMS will be subject to a 'highly flexible and secure access model';
	• Access will be subject to formal Participant Access Arrangements between LECAC agencies (as Requesting Agencies) and Data Holding Agencies, these will specify how and under what conditions participants may access data via the FMS, including;
	  • Multi-factor authentication at login;
	  • System access re-justified and renewed every 3-6 months;
	  • Access to data will be restricted to prescribed individuals, i.e. in order to access the FMS, individuals must be specifically authorised to use the FMS;
	  • Individuals will only be given access to specific functions of the FMS that they have been authorised to perform (i.e. FIS and FVS access treated differently in recognition of the greater privacy risk posed by the FIS);
	• Regular audits will be undertaken; and
	• Audit data will be captured in the Hub and the NDFLRS for every transaction

APPs 12 and 13 – Access to and Correction of Personal Information

APP 12 outlines an agency's obligations when an individual requests access to his/her personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 outlines an agency's obligations in relation to correcting the personal information it holds about individuals. This includes a requirement to enable correction unless a specific exception applies.

APPs 12 and 13 are designed to provide individuals with a statutory right to seek access to (and correction of) personal information about them. In terms of application, they overlap with public sector regimes established under Freedom of Information (FOI) legislation.

Relevance of the Access and Correction Principles to LECAC Agencies

The principles addressing access and correction are relevant to LECAC agencies. For the purposes of the FVS and FIS, FOI legislation will provide the primary access point to FVS and FIS data held by LECAC agencies, including information about the individuals themselves. It is noted that there may be reduced or no access to personal information held by LECAC agencies on operational grounds. This is consistent with current FOI arrangements and will not change as a result of implementation of the FVS/FIS. On the whole, requests for access and/or correction should be directed to the information source (i.e. usually the Data Holding Agency). As this may not be transparent to

individuals, this issue should be addressed via the proposed NFBMC privacy policy and/or notice discussed above (see discussion of APP 1 and APP 5, above). The relevance and applicability of FOI legislation to the FVS and FIS is also addressed within the Participation Agreement, where it is specified that FOI arrangements must be maintained in relation to FVS/FIS data. On the whole, this principle will have minimal impact upon LECAC agencies' current practices.

5.1 Recommendations – Home Affairs

Recommendation 1 – FMS Privacy Policy

It is recommended that:

- Home Affairs develop an NFBMC (FMS) privacy policy and provide the 'home' for (e.g. website), or a link to, that privacy policy;
- Home Affairs include information about the NFBMC within the Home Affairs' privacy policy; and
- all LECAC agencies take steps to leverage the same core privacy information, adjusted to fit local circumstances as necessary, for publication at the jurisdictional level (e.g. within their own privacy policies).

Recommendation 2 – Coordinated Template Collection Notice Text

It is recommended that Home Affairs coordinate the development of standard or template NFBMC (FMS) collection notice text. This can be adopted by Data Holding Agencies (and LECAC agencies to the degree that this is relevant).

Recommendation 3 – Management (of Perceptions) of Function Creep

It is recommended that careful consideration be given to any proposed extensions to the use or disclosure of biometric information/templates or the participation of additional agencies or the private sector in the NFBMC so as to avoid scope creep as well as perceptions of function creep. Any process adopted to explore extensions to use and disclosure should be as transparent and accountable as possible, involve consideration by the Coordination Group, be subject to a PIA, and enable stakeholders to participate in the debate about the merits or drawbacks of a particular position. Following agreement between the signatories to the IGA, significant changes should be subject to parliamentary review and disallowance

5.2 Assessing FVS and FIS Information Flows Against the APPs

The privacy principle discussion provided above highlights a number of key principles that should (and can) be taken into account by LECAC agencies. In particular, these relate to openness, collection, notice, use and disclosure, data quality and data security. Considering these findings against the information flow diagrams documented in Chapter 2, it is apparent that LECAC agencies, Home Affairs and Data Holding Agencies (depending upon which organisation carries responsibility for a particular action) will be able to take action to address key privacy requirements, such as through the development of an NFBMC privacy policy, publication of a wide range of information about the NFBMC, ensuring that collection notices are up-to-date and fit-for-purpose, and so on.

On the whole, these measures can be put into place even where an exemption applies. This is a positive finding. Additionally, compliance with other privacy principles has been built into the system.

- During the development of the NFBMC – partly in response to previous PIA findings – and using a combination of technical and policy measures, a number of steps have been taken to reduce the amount of personal information captured in the FVS and FIS to the minimum amount needed (proportionality).
- Data is encrypted while in transit and subject to detailed audit logs and information is destroyed once it is no longer needed – either at the level of the Hub or as a result of a policy requirement – when information is downloaded by a LECAC agency (security).
- LECAC agencies' access to specified data sources will occur on the basis of consent or legal authority (FVS) or legal authority (FIS). This means that the use of the FVS and FIS will be able to comply with legislative requirements.
- LECAC agencies will be required to provide appropriate training to personnel involved in the use of the FIS and conduct annual compliance audits in relation to the use of the FVS and FIS. These contribute to open, transparent and accountable processes.

In terms of privacy risk as a whole:

- The FVS provides an enhancement to the existing DVS. It will improve the ability for agencies to identify fraudulent identities, including those used as enablers for organised crime. It will be deployed lawfully and consistent with its primary purpose. It is broadly consistent with existing measures for the verification of identity. It involves 'incremental' change and a relatively low level of privacy risk once specified privacy and security controls have been operationalised.
- The FIS represents a 'transformational' change – it brings new opportunities at the same time as it carries potential privacy risks. Delivering on a commitment to a benefits realisation process is one measure to monitor NFBMC risks and benefits. Ensuring relevant metrics are available to assess the utility of the FIS can help to ensure its operations are proportionate and deliver value. The FIS will be deployed lawfully and used for the primary purpose of collection. Subject to the effective operationalisation of privacy and security controls, the level of privacy risk associated with use of the FIS (e.g. data breach) has been minimised to a significant degree.

Overall, the mapping of the APPs supports the view articulated earlier in this report that privacy management, rather than privacy legislation, should comprise the (practical) focus of LECAC agency compliance efforts.

6 LECAC Agency Use Cases and Privacy Management

6.1 FVS Use Case Information Flows

In order to assess how FVS information flows would work in practice, an FVS use case has been developed for illustration purposes, with input provided by Victoria Police (see Figure 11, below).

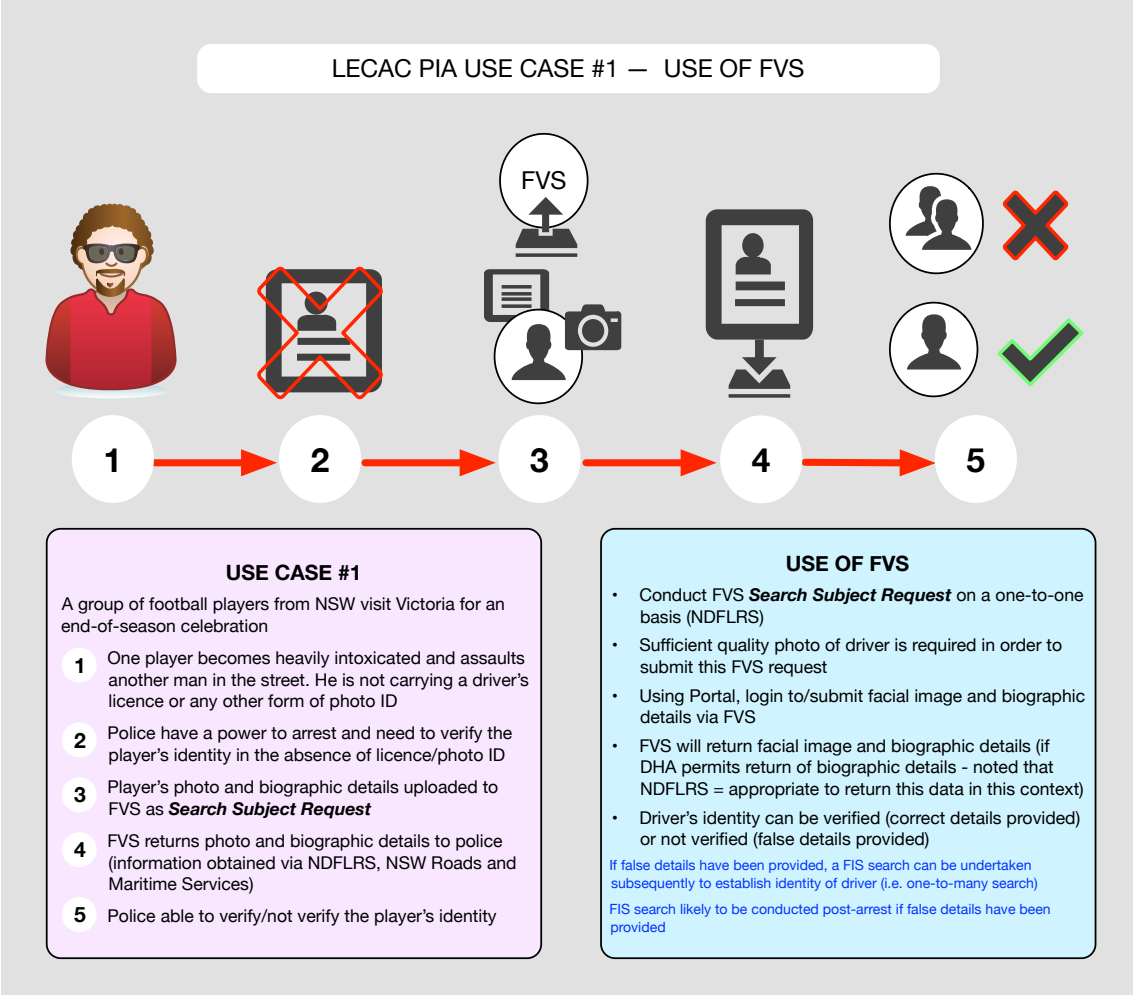


Figure 11 – FVS Use Case

6.1.1 Comments

This use of the FVS would rely upon police powers to arrest to request identity information from the player. To the extent that privacy legislation applies, this would be 'authorised by law', meaning that consent issues to collect the information under privacy law would not arise.

This use of the FVS meets the requirement that use of the FVS be subject to legal authority to collect and use the information sought via the FVS.

Road agencies will be authorised by law to disclose this information. It would be beneficial for all roads agencies, as well as good privacy practice, to develop and publish an appropriate privacy collection notice to inform drivers that their licence information and image may be used by the NFBMC.

All information transmitted via the Hub is encrypted. Information requests are recorded in an audit log.

Existing information management arrangements would apply to this information. No additional or new privacy compliance requirements are indicated in order to operationalise this process. The information flows involved in this use case do not raise any unusual or specific privacy issues.

Relevant internal resources capable of supporting effective privacy practice include:

- LECAC agency information privacy policy
- LECAC agency governing legislation
- Police Manual – Policy Rules – Professional Standards and Conduct (duty of confidentiality)
- Police Manual – Policy Rules – Use and Disclosure of Information
- PSPF/protective security standards or equivalent policy framework

6.2 FIS Use Case Information Flows

In order to assess how FIS information flows would work in practice, two high-level FIS use cases have been developed for illustration purposes, with input provided by Victoria Police (see Figure 12, below).

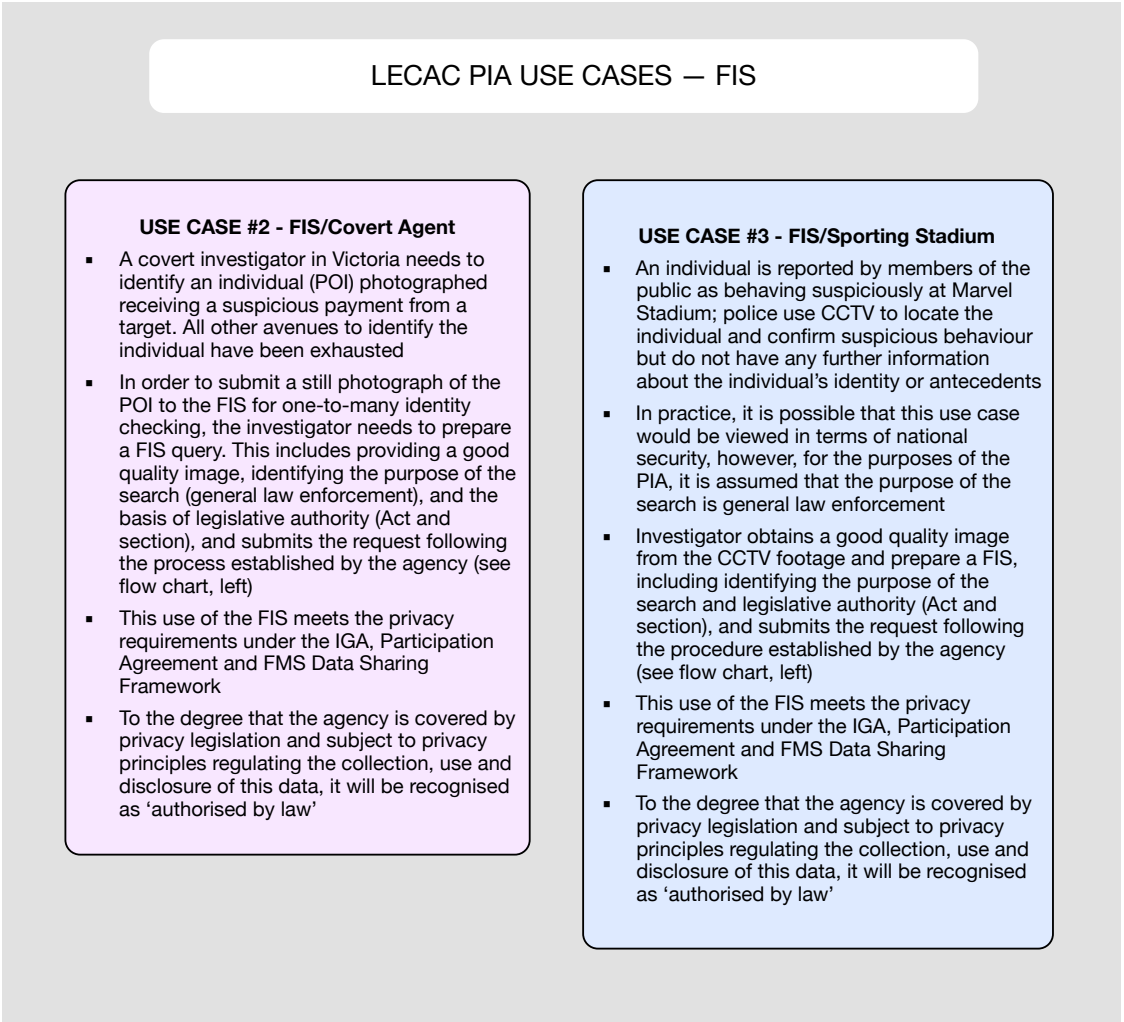


Figure 12 –FIS Use Cases

6.2.1 Comments

These uses of the FIS will meet the requirements illustrated above at section 2.4.2 (Figure 8), i.e. the need to identify the legal authority (Act and section) and purpose specification. An authorisation flow chart, developed by Victoria Police is provided below (Figure 13).

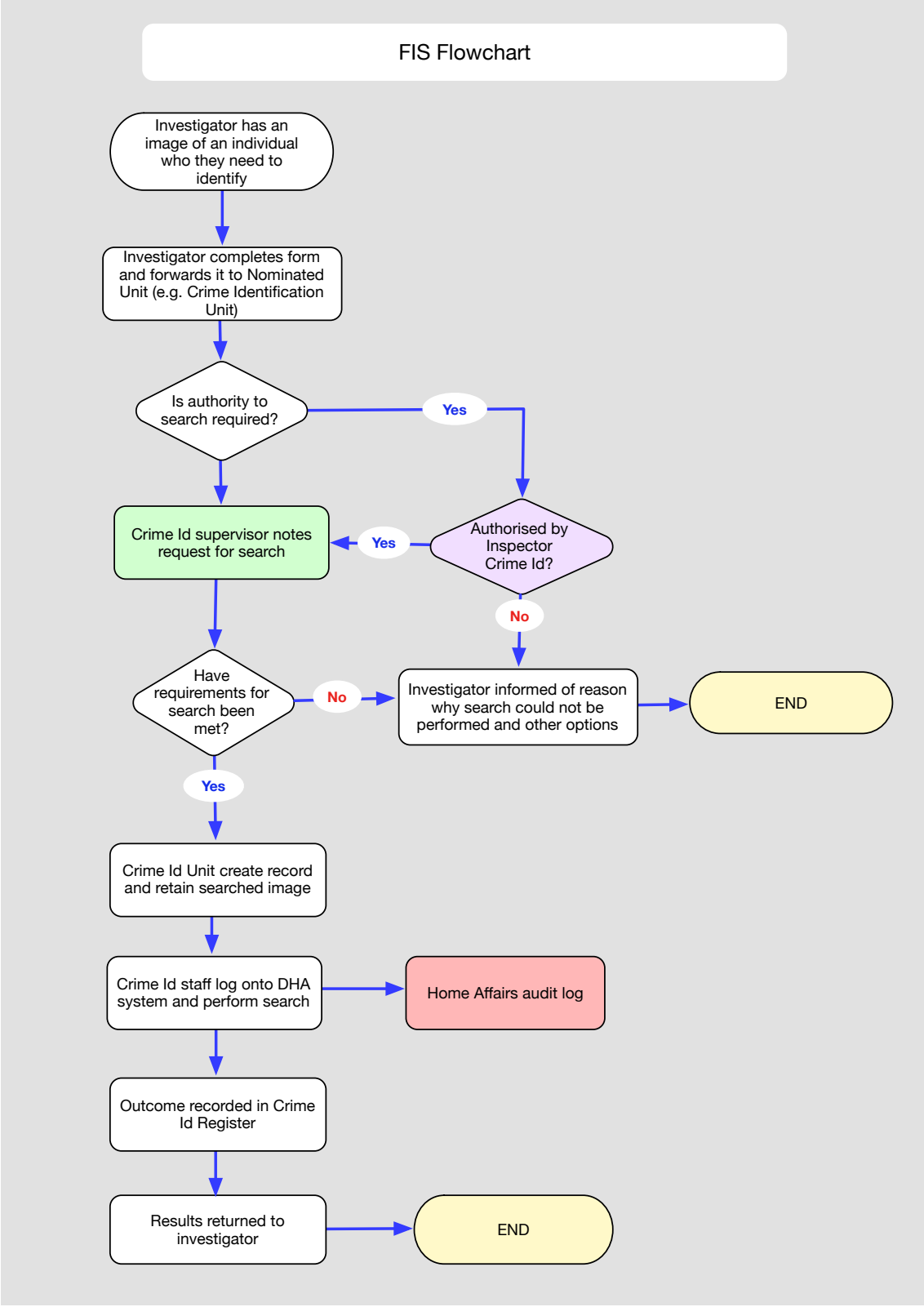


Figure 13 – FIS Request and Authorisation Flowchart

Restriction of the request and authorisation process to a single unit (here, the Crime Identification Unit) minimises the risks of unauthorised access and maximises consistency in terms of practice. In smaller jurisdictions, the 'single unit' may comprise a small group of qualified staff members. This type of triaging approach provides a consistent way for all LECAC agencies to adopt or adapt as relevant.

To the extent that privacy legislation applies, the collection, use and disclosure of FIS information will be 'authorised by law'. Consent is not a basis for collecting information via the FIS.

As with the FVS process, all information transmitted via the Hub is encrypted. Information requests are recorded in an audit log.

The information flows involved in these use cases are considered highly sensitive. They are consistent with legal requirements/authorisation but nevertheless raise privacy concerns because of the nature of the search (i.e. one-to-many, accessing data sources covering a majority of the Australian population. However, if enabling legislation allows Data Holding Agencies to disclose information to Requesting Agencies in this way, privacy legislation – even if it applied – would not override a countervailing legal authority.

Existing information management arrangements would apply to this information. It is considered that suitable processes should be documented in the relevant Police Manual and associated SOPs.

Relevant internal resources capable of supporting effective privacy practice include:

- LECAC agency privacy policy
- LECAC agency governing legislation
- Police Manual – Policy Rules – Professional Standards and Conduct
- Police Manual – Policy Rules – Use and Disclosure of Information
- PSPF/protective security standards or equivalent policy framework
- Australia and New Zealand Police Recommendations for CCTV Systems

6.3 Operationalising Privacy Requirements and Controls

Privacy principles are expressed as high-level requirements, often focused upon an agency taking reasonable steps and observing minimum standards in relation to its collection and handling of personal information. For example:

- Organisations must not collect personal information unless it is reasonably necessary for a function or activity.
- Organisations are required to collect personal information fairly and lawfully.
- Organisations must take such steps as are reasonable to secure personal information from unauthorised access, modification or disclosure.

Principles-based regulation is considered to provide a more flexible framework than rules-based regulation. Privacy principles – whether legislated or voluntary – are designed to provide a flexible framework for managing and protecting personal information. They can be adapted to fit a specific set of circumstances or fact scenario. What they do not do is provide 'off the shelf' answers to questions about how to meet privacy requirements in practice, what is reasonable under specific circumstances and, in particular, how such requirements should be operationalised.

This chapter considers some of the ways in which LECAC agencies may work towards identifying functional equivalence and operationalising privacy controls required under the IGA and FMS Data Sharing Framework, even where they may be exempt from privacy legislation. (Note that there is no suggestion that LECAC agencies should operate inconsistently with their governing legislation or operational requirements.) There are a

number of options available to LECAC agencies to pursue this outcome, including the OAIC's *Privacy Governance Framework and Management Standards*. Some LECAC agencies may already have a privacy governance and management framework in place.

The US National Institute of Standards and Technology (NIST) provides a useful discussion of privacy risk management and privacy controls, enhancement and supplemental guidance.[22] For NIST, information can be protected by:

- categorising the information to determine the impact of loss;
- assessing whether the processing of the information could impact individuals' privacy; and
- *selecting and implementing controls* that are applicable to the system.[23]

A privacy control is defined as an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks from the *authorised and unauthorised* collection and handling of personal information. Different controls are selected to mitigate privacy risks associated with authorised access to personal information (e.g. ensuring employees understand their privacy responsibilities) and unauthorised disclosure (e.g. use of encryption).

NIST publications outline a structured set of controls for protecting privacy (similar to those contained in the FMS Data Sharing Framework), as well as a road map for US federal agencies to use in identifying and implementing privacy controls concerning the entire life cycle of personal information. [24] The notion of a road map is seen as valuable for LECAC agencies as it is capable of providing a bird's eye view of requirements. An adaptation of the NIST approach to FVS/FIS privacy operationalisation is provided at see Appendix F. It may help agencies identify where a relevant control or implementation measure *already exists or could be re-purposed for use in this context*.

It is possible for a version of this approach – revised as necessary to fit the specific requirements of each LECAC agency – to be developed and used to assist in the demonstration of 'functional equivalence' with the privacy law and privacy principle requirements of the FMS Data Sharing Framework. It is not suggested that any work be undertaken that duplicates work required, for example, to complete the PAA template. Nor is it suggested that Appendix F is complete or comprehensive. The purpose of Appendix F is to illustrate an initial approach to demonstrating functional equivalence (i.e. where exemptions apply) in relation to the FMS Data Sharing Framework.

For crime and anti-corruption agencies, information obtained through this process can be documented in a privacy statement format (i.e. consistent with Recommendation 1).

For police agencies, the outputs from this process should be incorporated into their Police Manuals and associated SOPs and policies. Embedding this information in Police Manuals will provide a practical approach to the implementation of FVS and FIS privacy requirements, as well as a more effective outcome, as Police Manuals provide the primary source of operational requirements. This approach will produce better privacy outcomes than, for example, a stand-alone FVS/FIS document or procedure or a reference to privacy legislation. Any information developed should be reviewed by each LECAC agency in line with any relevant exceptions or exemptions. It is not suggested that the following account should override any exceptions/exemptions.

[22] NIST, Privacy Control Catalog, Appendix J, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Revision 4 (April 2013): p.J-1.
[23] NIST, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy NIST SP 800-37, Revision 2 (December 2018), p.xi.
[24] NIST, Privacy Control Catalog, Appendix J, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Revision 4 (April 2013): p.J-1.

6.4 Privacy Management Framework

The FMS Data Sharing Framework identifies (selects) a range of privacy and security controls. LECAC agencies are required to implement them. Another approach to the implementation of privacy controls by LECAC agencies, informed by a Privacy Management Framework, is to highlight commonality across jurisdictional frameworks in order to produce a unified and collaborative approach to privacy management.

A Privacy Management Framework enables organisations and sector-wide initiatives to *operationalise* privacy by embedding the appropriate responsibilities, actions, checks and balances within the legal, policy, process, operations/management, assurance and technology elements that comprise the core of and backdrop to large scale information intensive initiatives.

Like the NIST adaptation provided at Appendix F, use of a Privacy Management Framework can be used to demonstrate operational privacy practice as a form of *provable privacy* across an end-to-end and whole-of-life continuum. As deployed by Bainbridge Associates, the core components of a Privacy Management Framework include:

- Legislation, Regulation and Contract
- Governance and Management
- Information Lifecycle Management
- Risk Assessment and Management
- Systems Design and Management
- Information Access Control and Security Management
- Personnel Management
- Privacy Management
- Compliance/conformance/certification
- Tracking, Audit and Reporting
- Persistence Management

An important practical benefit of the use of a Privacy Management Framework is to understand how factors can be calibrated to create the required privacy *tensile strength* even when an individual factor may not be as robust as may ideally be desired (as is likely to be the case with LECAC agency use of the FVS and FIS. Employed strategically, a privacy management framework can help streamline compliance requirements and ensure a proactive approach to privacy. Specific components within a privacy management framework that may then be developed, amended or revised, include:

- A formal privacy management policy and set of methods
- A set of privacy statements/notices
- Privacy reviews and/or Privacy Impact Assessments at appropriate checkpoints
- Consent protocols

6.5 General Recommendations relating to FVS

Recommendation 4 – Quality of images
It is recommended that recognising that poor quality images will impact on the quality of match results generated, Requesting Agencies should demonstrate how they will: • obtain the highest quality probe images, including where practicable optimising the environmental conditions around capture such as subject pose and lighting;

- apply relevant tools and techniques to pre-process and enhance the images before submitting them for matching, such as normalising the tilt, yaw, pitch and roll of the subject's face; and
- provide periodic reports to the governance group as to progress in implementing this recommendation.

Recommendation 5 – Establish Community of Practice

It is recommended that LECAC agencies should consider establishing a community of practice that can:

- advise authorised users on relevant facial biometrics standards around image quality, storage and image processing techniques;
- share lessons learned and best practice in relation to use of the Face Matching Services; and
- assist in the development of Standard Operating Procedures or equivalent.

6.6 Specific FVS Recommendations

The LECAC PIA Questionnaire process identified the need for law enforcement and anti-corruption agencies that establish a system-to-system connection to the Interoperability Hub to adopt and implement appropriate protective security measures.

Recommendation 6 – LECAC Agency use of the FVS with Consent

It is recommended that where a LECAC agency wishes to access the FVS on the basis of individual consent, the agency should:

- ensure the consent is freely given and fully informed;
- a record is kept of the individual having provided consent; and
- as far as practical, provide a viable alternative method for individuals who do not wish to consent to a FVS check.

Recommendation 7 – System-to-system connection

It is recommended in the event that a law enforcement or anti-corruption agency establishes a system-to-system connection to the Interoperability Hub, the agency must demonstrate how it will:

- adhere to best-practice information and personnel security arrangements in accordance with the Commonwealth's Protective Security Policy Framework and Information Security Manual;
- have documented processes for managing information security risks and responding to incidents, and review these documents annually to ensure they remain relevant to address emerging risks; and
- institute appropriate system access and user management controls in accordance with the Participation Agreement, FVS Access Policy and all other relevant policies as agreed by the National Identity Security Coordination Group.

Recommendation 8 – FVS 'in the field'
It is recommended if a law enforcement or anti-corruption agency deploys FVS access to authorised officers in the field, for example on mobile devices or in-car computers, the agency must demonstrate how it will: • maintain individual role-based access controls so that every transaction can be ascribed to a particular user and there is personal accountability and audit logs; and • ensure that field-based access only comes from agency-issued or approved devices.

6.7 Specific FIS Recommendations

Recommendation 9 – FIS Gallery
It is recommended that where a FIS user has the ability to request more than 20 images from a Holding Agency with approval from the Authorising Officer, these requests should be utilised only where necessary and proportionate to the matter being investigated. FIS users should recognise that such requests: • have a greater net impact on the privacy of individuals; • should only be made in exceptional circumstances; and • may lead to degradation in speed and performance across the whole system.

Recommendation 10 – FIS users to receive minimum access required
It is recommended that authorised users of the FIS should only receive the minimum level of access needed to perform their role, with access maintained only as long as required. LECAC agencies must demonstrate that they have incorporated this requirement into their Standard Operating Procedures (or equivalent).

Recommendation 11 – Gallery download
It is recommended LECAC agencies demonstrate the steps they have taken to ensure that FIS users with the ability to download the image gallery and/or shortlist response: • download the least amount of personal and sensitive information from the FIS; • any information downloaded is stored appropriately and only retained for the minimum period necessary, in accordance with the Participation Agreement and legislative obligations; • the dissemination of information downloaded from the FIS is limited only to those persons within the Requesting Agency with a legitimate 'need to know'; and • that the Requesting Agency retains sufficient tracking and audit information within its internal systems to prove compliance with these privacy safeguards and/or a request from the Holding Agency about the use of personal and sensitive information they disclosed.

Recommendation 12 – Eliminating candidates
Noting that within the gallery response to an FIS query there will be images of people whose face matched the probe image but are not the subject of the request, it is recommended that FIS users should as soon as possible eliminate candidates from the gallery response.

7 Additional Privacy Issues and Risks

This chapter considers some additional issues relating to:

1. *The role of the PIA,* in particular, the deployment of multiple, phased (iterative) PIAs and engagement of 'independent' PIA consultants;
2. *Privacy perception issues* arising during the LECAC PIA that may affect broader stakeholder views of LECAC agencies use of the FMS;
3. *Biometric face recognition systems*, in particular, issues associated with the reliability and accuracy of the biometric software (e.g. the algorithms used to generate the biometric templates); and
4. NFBMC governance arrangements.

These issues are beyond scope but have been documented in the report because they are considered relevant to the LECAC agencies' use of the FVS and FIS. LECAC agency feedback was supportive of this view, noting that the recommendations documented below raise valid issues for consideration, opening up useful lines of communication between participants.

While each of these issues has some capacity to impact upon the use of the FVS and FIS by LECAC agencies, the PIA finds that any response to these issues will need to be coordinated and conducted on a whole-of-NFBMC basis in order to manage risk effectively (i.e. they are broader than LECAC agency access to, and use of, the FVS and FIS). Therefore, recommendations contained in this chapter are directed to Home Affairs rather than LECAC agencies in the first instance.

7.1 Role of the PIA

7.1.1 Iterative PIA process

The Commonwealth is to be commended for its commitment to 'privacy by design', including its incorporation as a guiding principle within the IGA and the commissioning of PIAs as a key risk management tool during the build of the various components of the NFBMC. However, while this 'privacy by design' approach was clearly intended to embed privacy within the NFBMC, the decision to commission multiple PIAs in alignment with the iterative build process has proved to be increasingly problematic over time.

Rather than producing an *iterative* or *cumulative* view of privacy risk, this approach has increased privacy visibility at the micro or individual component level at the expense of potential privacy impacts at the macro or whole-of-NFBMC level. That is, while the iterative PIA process has enabled privacy issues to be assessed on a PIA-by-PIA or component-by-component basis, this is insufficient – and potentially misleading – both in terms of: (i) the identification of whole-of-NFBMC issues; and (ii) important issues that lie beyond the scope of the NFBMC (such as the potential relationship between the NFBMC and jurisdictional or private sector biometric systems).

Under this approach, each individual PIA focused upon a specific NFBMC component: the Hub (technical); the FMS and NDFLRS (services); and legislation (IMSB). But, as the 'privacy by design' PIA process progressed, each PIA also began to focus on a different aspect of design. For example:

- the NDFLRS PIA examined the architecture and technical underpinnings of the FMS;
- the IMSB PIA examined the legislative framework required for the Commonwealth to operate the Hub and the NDFLRS; and

- the LECAC FMS PIA focused upon the framework supporting access and use of the FMS by LECAC agencies.

A tight focus upon 'in scope' issues – e.g. the LECAC PIA excluded consideration of technical, governance and IMSB issues – may meet the requirements of a specific PIA process but does not necessarily deliver 'privacy by design'. The LECAC PIA finds that the approach taken to the NFBMC PIA process overall – in particular, restrictions placed upon the scope of later PIA processes and the fact that the IMSB PIA report was not available to inform the LECAC PIA – has prevented consideration of a full set of privacy issues and risks, including the need to 'circle back' at key points to re-visit aspects of earlier PIA processes. This includes the NFBMC's technical, governance and/or legislative 'underpinnings'.

In order to execute an iterative PIA process effectively – i.e. to produce a cumulative view of privacy risk – these underpinnings need to be considered in context and on an ongoing basis. While these issues are particularly acute for the LECAC PIA, it was noted as a potential risk from the beginning of the PIA processes and is presented in every previous PIA report available to Bainbridge Associates (i.e. excluding the IMSB PIA report). For example, IIS emphasised that the privacy impacts of the NFBMC as a whole could be greater than the individual risks identified by each individual PIA:

> The incremental approach could mean that the privacy impacts of the system as a whole are not sufficiently considered. This could mean that the opportunity to identify and manage potentially significant risks created by the system as a whole is lost.[25]

The LECAC PIA finds that the specific approach taken to the execution of multiple, iterative PIAs as a means of embedding privacy by design – while not deliberate – has not produced the full (intended) set of proactive privacy outcomes. If anything, this approach impeded the ability of Bainbridge Associates to assess privacy risk holistically and may have obscured wider, and potentially more significant, privacy risks posed by a biometric face matching capability. In this context, it is difficult for a PIA consultant to make 'whole-of-information-lifecycle' findings and recommendations.

While it is expected that the final 'whole of NFBMC' PIA will consider all relevant issues end-to-end and from a 'whole-of-information-lifecycle' perspective, it is noted that, by the time it is commissioned, it may no longer be possible to revisit key aspects of the NFBMC as a whole.

The PIA finds that it will be very important for the final NFBMC PIA to be commissioned in a timely manner. PIA requirements, particularly those expressed in any Approach to Market (ATM) documentation, should be expressed in terms of undertaking the full NFBMC PIA 'end to-end' and on a 'whole-of-information-lifecycle' basis. Further, the PIA process should not be subject to restrictions in scope unless there is explicit agreement between Home Affairs and the PIA consultant that specific aspects of the NFBMC do not require analysis from a 'whole-of-capability' perspective.

7.1.2 'Non-independent' PIA processes

As identified earlier in the PIA report (section 1.4.2), Home Affairs commissioned external, independent PIA consultants to undertake each of the NFBMC PIAs. While this may be useful where a project involves significant privacy risk or controversy and there is a need to commit to an independent process, it should not be seen as the only way to conduct a PIA. Sometimes a better outcome can be achieved by engaging an external privacy consultant or a suitably qualified internal resource to work alongside the project team, particularly as part of the development process.

[25] IIS, *NDFLRS PIA Report* (November 2017): p.7.

This is particularly useful where it may not be clear how the PIA should be undertaken, whether a planned approach will produce the desired outcome, what resources are required, what the key questions are, where the focus should be placed or what information is required to support the PIA. While it will not be possible to claim that this type of PIA process is independent, it is potentially far more valuable in terms of getting to the bottom of difficult privacy issues and risks. Enabling a closer relationship between the PIA consultant and the project team can also help with privacy and project knowledge transfer.

Home Affairs is encouraged to consider a variety of approaches to conducting a PIA, recognising that there is no 'one-size-fits-all' PIA process. This includes involving PIA experts in the development of any Approach to Market in the future (consistent with procurement requirements).

Recommendation 4 – Full NFBMC PIA
It is recommended that the proposed, full NFBMC PIA: • be commissioned in a timely manner and supported by appropriate documentation; • be expressed as requiring an 'end to-end' and 'whole-of-information-lifecycle' PIA process; • not be subject to restrictions in scope unless there is agreement between the Commonwealth and the PIA consultant that there is no privacy benefit in revisiting certain aspects of the NFBMC; and • should encompass consideration of all relevant design components, including legislation, governance and information governance arrangements, protective security and privacy frameworks and associated fairness, accountability and transparency measures.

Recommendation 5 – Commissioning a PIA Process
It is recommended that Home Affairs take a strategic approach to the commissioning of PIA processes, recognising that there is no 'one size fits all' PIA process. At time engaging an 'independent' PIA consultant may be best option while, at other times, it may be preferable to engage a PIA consultant to assist in the development of Approach to Market documentation or to conduct a PIA process in collaboration with a project team.

7.2 Privacy Perceptions

7.2.1 *Identity-Matching Services Bill 2018* (Cth)

Privacy perception issues were raised by the introduction into the Commonwealth parliament on 7 February 2018 of the *Identity-matching Services Bill 2018* (IMSB) and the *Australian Passports Amendment (Identity-Matching Services) Bill 2018 (*Australian Passports Amendment Bill). Both bills were developed in response to the requirement in the IMS IGA that Parties use their best endeavours to preserve or introduce legislation to enable participation in the NFBMC (see clause 8.1).

The main purpose of the IMSB is to confer the legal authority for Home Affairs (as a Commonwealth agency) to operate the Hub, to collect and handle NDFLRS data, and to provide for associated safeguards. In effect, it ensures that new Commonwealth functions (i.e. role of Hub Operator) and activities (e.g. the collection, use and disclosure of NDFLRS data) are authorised by law.

Reflecting its sensitive nature, three parliamentary committees have considered the IMSB:

- The Senate Standing Committee for the Scrutiny of Bills considered the IMSB on 14 February 2018 and a report was provided in the Committee's Scrutiny Digest No. 5 of 2018.
- The Parliamentary Joint Committee on Human Rights considered the IMSB in 2018 and a report was provided in the Committee's Scrutiny Digest of 2018.
- On 2 March 2018, the IMSB was referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS). It held public hearings in Melbourne on 3 May 2018. As at the date of this PIA, the PJCIS had not published its report.

The main purpose of the Australian Passports Amendment Bill is to provide a clear legal basis for the automation of the sharing of passport data for the purposes of national security. The bill authorises the participation of DFAT as a DHA as well as DFAT's disclosure of personal information via the FMS. It is not known when the PJCIS report will be published, or when the IMSB and/or Australian Passports Amendment Bill will be likely to receive passage.

The IMSB and Australian Passports Amendment Bill do not apply to state and territory LECAC agencies, which are expected to participate in the FMS under their own pre-existing or enhanced (amended) legislative authority. Queensland's *Police and Other Legislation (Identity and Biometric Capability) Act 2018* was enacted for this purpose.

The IMSB, in particular, produced a number of legal and privacy perception issues. For example, many of the submissions about the IMSB made to the various parliamentary committees were critical of the way the IMSB was drafted, in particular, the bill's failure to mirror requirements contained in the IMS IGA (such as restrictions on the types of general law enforcement covered by the scheme) and recommended that the bill not proceed in its current format.

But equally, negative privacy perceptions have arisen because stakeholders and the broader community are not currently well placed to understand how each of the components or 'iterative bits' of the NFBMC will come together to operate as a comprehensive information-sharing scheme. For example, in response to Bainbridge Associates' LECAC PIA consultation process with Australian privacy commissioners, there was an overwhelming focus upon the IMSB, at the expense of the issues raised by the LECAC PIA. In the academic sphere, a recent paper published in the *UNSW Law Review,* stated that 'the NFBMC is being introduced through administrative processes and is occurring outside of a legislative framework, and the increased scrutiny that entails.'[26]

While the iterative project development process made it difficult to form a comprehensive view of the NFBMC, this is no longer the case. Recognising that it is just as important to address privacy perceptions, as it is to ensure that NFBMC legislation is appropriate, will require action.

The PIA finds that it is necessary, feasible and desirable for a consolidated and comprehensive picture of the NFBMC to be developed. This should illustrate how the

[26] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight, *University of New South Wales Law Journal* (2017) 40 (1) at p. 7.

NFBMC is being implemented as a scheme within a federal system, how the FMS Data Sharing Framework will operate, the various measures and mechanisms that will ensure core legal, governance and administrative requirements are met and how privacy, security, fairness, accountability and transparency will be supported. This overview should be published online so that it is readily available to a wide range of interested parties (individuals, agencies, organisations, civil society, academia).

This approach should help to ameliorate misunderstandings. Alternatively, it may help to identify where privacy perceptions are actually privacy risks requiring changes to policy and/or legislation. If possible, this recommendation should be actioned prior to the full NFBMC PIA process so that it can provide an input to the PIA process. This will help to ensure that the PIA consultant has relevant 'foundational' information available at the commencement of the PIA process.

7.2.2 Transfer of Responsibility for the NFBMC from AGD to Home Affairs

At the time that work on the NFBMC was initiated and up until December 2017, AGD was responsible for the design, development and operation of the NFBMC on behalf of the Commonwealth, States and Territories. However, under Administrative Arrangements Orders made on 20 December 2017, the relevant functions were transferred from AGD to the newly formed Commonwealth Department of Home Affairs (Home Affairs).[27] From that date, Home Affairs has been the Commonwealth agency responsible for developing, implementing and operating the NFBMC.

This change of arrangements affected public and media perceptions relating to NFBMC operations and privacy governance. In particular, the 'privacy optics' of one agency (Home Affairs) being responsible for the management and operation of the NFBMC (as Framework Administrator) as well as occupying the roles of Hub Controller, Data Holding Agency and Requesting Agency, raises issues about the degree to which Home Affairs can maintain and be seen to maintain a 'separation of functions' (which is viewed as a crucial accountability measure). Under previous arrangements, AGD occupied the roles of Framework Administrator and Hub Controller. As AGD was neither a Requesting Agency nor a Data Holding Agency, this ensured that there was organisational separation between control of, and access to, the NFBMC. Any powers to extend or change the NFBMC were also expected to reside with AGD, which would occupy an 'honest broker' role.

The LECAC PIA finds that the transfer of responsibility from AGD to Home Affairs raises genuine privacy perception issues that require active management. While Home Affairs is already required to develop a whole-of-Home-Affairs privacy policy under the Privacy Act, it is recommended that specific attention be paid to NFBMC privacy and legal issues. In particular, Home Affairs should consider how to account for potential and/or perceived conflicts of interest arising from the fact that agencies within Home Affairs occupy a number of different NFBMC roles (e.g. Data Holding Agency, Hub Controller, Framework Administrator, Requesting Agency). This could include explaining that the Australian Border Force is an operationally independent body under the Home Affairs portfolio, etc.

Recommendation 6 – Transfer of NFBMC from AGD to Home Affairs
It is recommended that Home Affairs address privacy perception issues arising from the transfer of responsibility for the NFBMC from AGD to Home Affairs. It is considered desirable for Home Affairs to develop and publish information outlining how the separation of various NFBMC roles and responsibilities (System Administrator, Data

[27] See Administrative Arrangements Orders, 20 December 2017, at https://www.pmc.gov.au/resource-centre/government/aao-amendment-made-20-dec-2017.

Holding Agency, Requesting Agency) will be maintained within a single organisation (Home Affairs).

7.2.3 Publication of NFBMC PIA Reports

As part of its commitment to undertaking PIAs, Home Affairs intends to publish NFBMC PIA reports (in full or in summary), subject to the need to protect operational secrecy. Where publication is not considered appropriate on operational grounds, Home Affairs is committed to providing summaries of the PIA recommendations and Home Affairs' response to them.

As at October 2018, only one of the NFBMC PIAs has been published online in full (Interoperability Hub PIA report), while a summary of a second series of PIA reports (Lockstep PIAs) is available via the Home Affairs website. At least one of the latter reports – *AFP Access to DIBP FVS (Match & Search Functions) for Citizenship & Visa Images PIA Report* – is available online, having been released under FOI legislation. However, it is not published via the Home Affairs website on the grounds of operational secrecy.

The failure to publish NFBMC PIA reports, contrary to a stated policy preference for publication (full or summary), risks negative perceptions arising. The PIA finds that while operational secrecy may justify withholding some of the information contained in PIA reports, efforts should be made nevertheless to provide the maximum amount of information online, including PIA findings and recommendations.

Recommendation 7 – Publication of PIA Reports
It is recommended that, where the full publication of a PIA report is withheld on the grounds of operational secrecy, the Commonwealth investigate all appropriate options for publishing as much of the content of a PIA report as is possible. At a minimum, a PIA report's key findings and recommendations should be published online.

7.3 Algorithms, Biometrics and the Public Sector

The increasing use of automated and semi-automated decision-making systems has been accompanied by calls to assess the degree to which their application is appropriate, to investigate the reliability of the algorithms that drive these systems, and to ensure public accountability.[28] Two public policy issues that overlap with considerations of NFBMC privacy requirements have been identified from a range of possible current and emerging approaches. They have been chosen because they have the capacity to increase confidence and trust in the adoption of biometric face recognition systems.

7.3.1 Algorithmic Impact Assessment

Internationally, there is a discernible shift towards increasing the degree of transparency associated with automated and semi-automated decision-making systems. This has included legal instruments like the EU's General Data Protection Regulation (GDPR), which requires that individuals be notified when an automated decision-making system processes their personal information.

There have also been calls for public sector agencies to implement a practical framework to address potential issues raised by such systems. In the United States, this has included the development of *Algorithmic Impact Assessments: A Practical Framework for Public*

[28] This is not to suggest that similar issues are not arising in the private sector (they are), but rather to focus upon the largely public sector nature of the NFBMC.

Sector Accountability,[29] which notes that there is a lack of information about and access to the systems under consideration because 'many such systems operate as "black boxes" – opaque software tools working outside the scope of meaningful scrutiny and accountability.'[30] In this context, the implementation of an Algorithmic Impact Assessment (AIA) provides a necessary first step to ensuring that the short and long term impacts of such systems can be monitored and that their use is subject to governmental and legal requirements relating to fairness, accountability, transparency, natural justice and privacy.

These issues are equally relevant in Australia and would benefit from further public policy consideration. These issues are also likely to be relevant to the full NFBMC PIA.

7.3.2 NIST Face Recognition Vendor Tests

Undertaken by the US National Institute of Standards and Technology (NIST), Face Recognition Vendor Tests (FRVT) provide independent government evaluations of commercially available and prototype face recognition technologies.[31] These evaluations are designed to provide US Government and law enforcement agencies with information to assist them in determining where and how facial recognition technology can be deployed best. FRVT results also help to identify future research directions for the face recognition community. In addition to its work on biometric standards, NIST provides guidance on how biometric systems should be tested and how results should be calculated and reported so that the performance of one system can be compared to the performance of another system. It also defines methods for assessing the quality of the biometrics that are collected.

Like Australia, the US views biometrics as a 'key enabling technology' to support improved homeland security. In this context, NIST 'supports the government-wide effort to increase the collection of good quality biometrics, to see that the data collected is appropriately shared with other agencies, and to make sure biometric systems are accurate and interoperable.'[32]

It is recommended that the Commonwealth consider ways of providing greater technical information about the NFBMC, including:

- how the NFBMC biometric face recognition system compares to other, similar systems; and
- how to implement relevant metrics relating to the accuracy of the NFBMC.

The latter point should be considered within the context of the Commonwealth's proposed benefits realisation project, which is currently under development and will be applied to the NFBMC.

Recommendation 8 – Enhanced Technical Accountability Measures
It is recommended that Home Affairs should consider publishing an account of the technical and other steps it has taken and will continue to take to: a) benchmark the NFBMC biometric face recognition system against other like

[29] Dillon Reisman, Jason Schultz, Kate Crawford, Meredith Whittaker, *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability* (April 2018) AI Now: https://ainowinstitute.org/aiareport2018.pdf
[30] See, for example, Frank Pasquale, *The Black Box Society: the Secret Algorithms that Control Money and Information* (Harvard University Press, 2015).
[31] NIST, Face Projects: *Face Recognition Vendor Tests (FVRT)*: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt
[32] NIST, Biometrics: https://www.nist.gov/programs-projects/biometrics

	systems;
b)	ensure the accuracy of the NFBMC biometric face recognition system; and
c)	undertake a NFBMC benefits realisation project

7.4 NFBMC Governance

During the PIA process, a high-level assessment of FMS governance arrangements was undertaken to determine whether or not they were capable of supporting the FMS Data Sharing Framework. From the perspective of the LECAC PIA, effective and appropriate governance arrangements will be crucial to the successful implementation of the FVS and FIS. However, as a whole, proper governance of the NFBMC, including the FVS and FIS, is essential if the NFBMC is to achieve the objectives that have been established for it and to manage risks that arise in the course of its operations. The governance bodies that have a role in the oversight of the FMS are:

- COAG (IGA)
- The Ministerial Council on Police and Emergency Management (MCPEM) (in consultation with the Transport Infrastructure Council, if required), which consists of relevant Ministers from each jurisdiction (IGA)
- The National Identity Security Coordination Group (Coordination Group), which consists of senior officials from each jurisdiction's lead agency as well as observers from Austroads, Commonwealth, State and Territory Privacy Commissioners and the ACIC
- The Face Matching Services Advisory Board, which consists of officials from data holding agencies as well as observers from Austroads, Commonwealth, State and Territory Privacy Commissioners and the ACIC
- Supporting working groups, including Policy and Legal and Business and Technical working groups.

Figure 11, below, provides an overview of the governance structure of the NFBMC, including the FMS within the IMS.

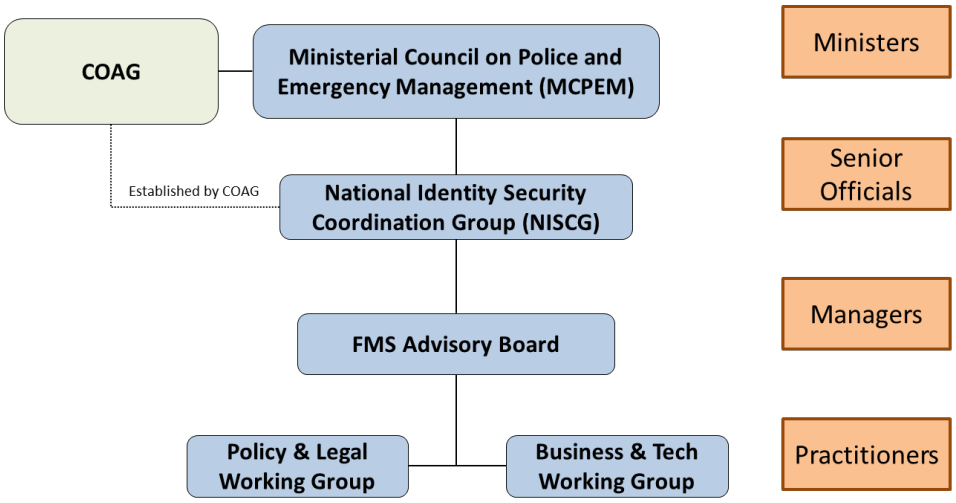


Figure 14 – FMS Governance Framework

The FMS is an information system. In broad terms, it consists of hardware, software, technical capabilities and operational processes and procedures.

Governance of an information system does not occur in a vacuum. It needs to align with overall organisational governance and support, and be supported by it. Good governance must be 'fit for purpose' so that 'the right people have the right access to the right information and functionality at the right time.' Successful governance of the FMS will require sustained and responsible collaboration between the Commonwealth, states and territories and their relevant agencies.[33] Its corporate and information governance must reflect this reality. The fact that LECAC agencies are either partially or wholly exempt from privacy legislation and are likely to embody their privacy approach within a privacy statement, as per clause 45.2(p) of the Participation Agreement, raises the question of whether there is a role for the NISCG to undertake some of the monitoring, oversight and complaint handling functions usually performed by privacy regulators.

7.4.1 Assessment of FMS Governance Arrangements vis-à-vis LECAC Agencies

The PIA finds that there is a discrepancy between the privacy objectives that have been developed for the FMS (and the NFBMC) and its (their) governance. Although the importance of privacy is embedded and underlined in the IGA, the Participation Agreement (including the FVS and FIS access policies, compliance policies and Participation Access Arrangements), that importance is not reflected in governance arrangements, i.e. the place where a culture of privacy should be set and affirmed. While the OAIC will attend Coordination Group meetings as an observer, it is more important that group members (as opposed to observers) take responsibility for privacy governance.

Equally, there are numerous other skills – not just privacy skills – such as ICT and protective security skills that may be considered lacking from the composition of the governance arrangements.

Despite the existence of the MCPEM, it is the Coordination Group that will shoulder the governance burden for the FMS. It is a group whose membership is drawn from Home Affairs and each of the first Minister's departments of the states and territories. Although this composition of membership reflects the desire to include representatives of all the major stakeholders in the governance of the FMS, it overlooks the necessity of including members who bring to the governance table the broad spectrum of skills that are fundamental to the successful discharge of the governance activities that have been assigned to it and which are set out in detail earlier in this section.

Moreover, none of the members are independent. Each member will be a senior government official from the Commonwealth, the states and territories and subject to the direction of their respective departments.

The PIA finds that the lack of independence and absence of diversity of skills within the Coordination Group has the potential to undermine the governance arrangements for the FMS and should be subject to review at a suitable point in time. In particular, it is considered both necessary and desirable that the Coordination Group includes members with relevant privacy and protective security expertise.

[33] It is acknowledged that the need for collaboration will in future extend to foreign partners and the private sector.

Finding 2 – Enhancing Privacy Governance
It is considered important that a review of the approach taken to privacy governance within the FMS Data Sharing Framework be undertaken at an appropriate point in time, e.g. review of the IGA on Identity Matching Services. This will help to balance the high degree of privacy protections offered through the IGA, Participation Agreement and associated policies and procedures with those provided via the Coordination Group.

Finding 3 – Enhancing Governance Independence and Skills
As part of the review of the IGA on Identity Matching Services, consideration should be given to appointing independent members to the Coordination Group. This could include individuals with specific protective security, legal or privacy skills.

Appendix A – LECAC Agency Privacy Requirements & Controls,

A.1 Intergovernmental Agreement on Identity Matching Services

Intergovernmental Agreement on Identity Matching Services

General

- The IGA will help to promote privacy by strengthening the integrity and security of Australia's identity infrastructure and preventing identity crime
- Parties to the IGA acknowledge the importance of protecting the privacy of individuals
- Coordination Group to oversee the development, implementation and ongoing operation of multifaceted privacy and security safeguards, including Participation Agreement, Access Policies and PAA, which will outline privacy safeguards for RAs
- IMS to be informed by guiding principles including:
  - *Privacy by Design*: aims to balance privacy impacts against the broader benefits to the community from sharing and matching identity information (PIAs, consultation with federal, state and territory privacy commissioners)
  - *Best practice security*: adoption of best practice security arrangements in accordance with the PSPF and the ISM; participating agencies to implement appropriate security and access controls, including audit and compliance mechanisms
- Parties to maintain accessible and effective mechanisms for responding to any public complaints re: use of identity matching services (including FMS)

Legislative Authority

- Parties will only collect, use or disclose personal information through FMS as permitted or required by law, including privacy law
- Parties agree to use best endeavours to preserve or introduce legislation that enables the exchange (collection, use and disclosure) of facial images and identity information for the purposes of:
  - preventing identity crime
  - general law enforcement
  - national security
  - protective security
  - road safety
  - identity verification
- Legislation to cover facial images and related identity information used in:
  a) an Australian passport
  b) an Australian driver licence
  c) an ImmiCard or visa issued under the *Migration Act 1958* (Cth)
  d) a certificate of Australian citizenship issued under the *Australian Citizenship Act 2007* (Cth)
  e) any other type of identity document with a facial image that a state or territory wishes to include in the NDLFRS

Privacy & Security

- Sharing of identity information involves the collection and disclosure of personal information, including sensitive information, and requires robust privacy and security safeguards
- Parties to ensure collection, use or disclosure of personal information is reasonable, necessary and proportionate to their functions or activities
- Participation to be subject to privacy and regulatory oversight, including OAIC, state and territory privacy commissioners or equivalent
- Parties to adopt best practice security and access arrangements
- Interoperability Hub and NDFLRS to be subject to independent penetration and vulnerability tests and security reviews
- Participation Agreement to stipulate further security requirements, with regular audits ensuring protections are functioning appropriately
- Provision of training in relation to privacy and security obligations and security awareness
- Parties responsible for additional resourcing of privacy regulators and other oversight bodies

A.2 FMS Participation Agreement

Participation Agreement

Summary of Security, Privacy and Legislative Requirements Relevant to FMS

The Participation Agreement (PA) provides the framework within which LECAC agencies will negotiate details of data sharing arrangements so that these meet minimum privacy and security safeguards necessary to support information sharing across jurisdictions

Security

Participants must comply with security requirements, including:

- preventing access to information subject to a Security Classification unless the user has a security clearance to an appropriate level (no less than Baseline Security Clearance - PSPF) and a need to know, or to users whose security clearance has lapsed, been revoked or who no longer require access;
- ensuring all security classified information and resources meet the minimum standards set by the Commonwealth for the relevant Security Classification level (PSPF);
- acknowledging that all personal information used in connection with the FMS is "Unclassified - *Sensitive Personal*" and all audit data relating too the FMS, Hub or the PA is "Unclassified - *For Official Use Only*" (PSPF)

Privacy and FOI

Participants must:

- comply with the relevant privacy legislation that applies to it by law or where no privacy law is in place with the APPs in Schedule 1 of the Privacy Act as if the Participant or user were an APP entity within the meaning of the Privacy Act (noting that some Participants are exempt from the requirement to comply with the APPs)
- comply with FOI legislation within their jurisdiction
- ensure that they address any requests from an individual made under applicable privacy or FOI legislation
- develop and/or amend as necessary their Privacy Governance Framework and Management Standards to ensure they are adequate and reflect the management of flows of information through the FMS (Privacy Management Framework)
- submit Compliance Statements on an annual basis confirming privacy and security safeguards operating effectively
- provide training to users and authorising officers in privacy obligations and security awareness
- take steps to assure and protect identity information - compliance with all applicable legislation relevant to a PAA, including record keeping, identity information protection, privacy and protection of personal information
- not disclose identity information to third parties unless legally required to do so or legally authorised to do so and it is for an authorised disclosure purpose, the DHA agrees in writing, the RA has obtained informed consent in writing from the individual to whom the information relates

Legal Authority

LECAC agencies

- may not enter into PAA unless independently satisfied on its own behalf that all aspects of the PAA will be lawful
- must ensure that each PAA to which it is a party contains a Statement of Legislative Authority detailing the legislative provision and other relevant information that the agency believes establishes that its access to and use of facial images and identity information via the FMS will be lawful

Default Position under Participation Agreement

Security — *Protective Security Policy Framework (PSPF) (Cth)* and *Information Security Manual (ISM) (Cth)*

Privacy — APPs in Schedule 1 of the *Privacy Act 1988* (Cth)

Privacy Governance Framework and Management Standards — OAIC's Privacy Management Framework

A.3 FVS Access Policy

FVS Access Policy

Legal, Privacy and Security Requirements

FVS Access Criteria

FVS access is predicated upon agencies meeting the following access criteria:

- Participation Agreement & Participant Access Agreement (PAA) in place
- Statement of Legislative Authority referencing the legislation that provides the legal basis for collecting, using and/or disclosing identity information via the FVS/FIS documented in PAA
- Completion of PIA process or development of privacy statement (where exempt from privacy legislation)
- Scope of information sharing defined, includes type of data, characteristics (for individual, e.g. security clearance) or accreditation (for system) relating to agreed categories of Users (role) and access permissions associated with each role
- Protection of personal information, including retention & destruction of data, any disclosure of information
- Management of nominated users, including no concurrent access to FVS and FIS, maintenance of register of nominated users, timely termination of access when it is no longer needed
- Provision of appropriate privacy and security training to users
- Auditing and accountability: all data sharing must be audited independently; relevant data must be maintained to support audits, including, e.g. detection of anomalous or potentially suspicious transactions or patterns of transactions
- Any system-to-system connection must include Security Risk Management Plan and System Security Plan or Security Accreditation Certificate; portal only must conduct a security risk assessment process
- Transparency measures, including publication of relevant information about FMS, legal authority, privacy and security

LECAC agencies' responsibilities as documented under a PAA must be consistent with the FVS Access policy and ensure adequate privacy and security safeguards

A.4 FIS Access Policy

FIS Access Policy

Legal, Privacy and Security Requirements

FIS access is subject to the same access criteria as provided for in the FVS Access Policy, this includes providing a Statement of Legislative Authority, conducting PIAs or preparing privacy statements, defining the scope of data sharing, training and transparency.

Additionally, **FIS access** is underpinned by following principles:

a) promote privacy and compliance with legal provisions: confidence must be maintained by ensuring FIS access is subject to legal basis for data sharing and anticipated impacts upon individuals are outweighed by the public benefit of the service, which dictates the way in which permitted uses are framed and how supervision and authorisation requirements and other access controls are applied

b) s37(2)(b)

c) non-evidentiary system

d) promote information sharing to the maximum extent permitted by law and in accordance with the FIS principles

e) FIS access controls based on a risk-based approach that takes account of privacy and security safeguards and usability and timeliness of FIS

f) approved agencies: access limited to agencies with law enforcement or national security functions, eligibility to access subject to approval by the Coordination Group

g) permitted purposes: FIS access for permitted purposes only, as set out in IGA and Part 4 of the FIS policy

h) FIS nominated users limited to specific 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 to ensure privacy-respecting, efficient and effective use of the FIS capabilities

i) supervised access: user access to FIS to be subject to supervision by more senior officer

j) additional authorisation for more delicate information: FIS queries re: more delicate or restricted information to be managed as exceptions requiring an additional authorisation step in most cases

k) controlled access to biographic information: FIS designed to limit access to biographic information, such as name and date of birth, of persons who are not the subject of the query; to help maintain anonymity of these individuals, biographic details only to be made available after the FIS user shortlists an image from the return gallery

l) control of download and export of returned images: DHAs may impose conditions under which RAs may download or export images. RA responsible and held accountable for secure management of any images downloaded through the FIS

m) auditing to ensure compliance and enable risk management: sufficient transaction data to be captured by Hub to support audits of RAs for compliance purposes

Permitted purposes

As per IGA, FIS access subject to meeting permitted purpose(s):

- preventing identity crime
- general law enforcement (maximum penalty of not less than 3 years imprisonment
- national security
- protective security
- community safety

RA responsibilities

RAs are responsible for ensuring PAAs are consistent with Access Policy and ensuring adequate FIS privacy safeguards are in place

Appendix B – List of Documents Reviewed

B.1 PIA Reports

- *National Facial Biometric Matching Capability, Privacy Impact Assessment – Interoperability Hub*, Information Integrity Solutions (August 2015)
- *National Facial Biometric Matching Capability, Privacy Impact Assessment: DFAT Access to DIBP FVS (Match & Search Functions) for Citizenship & Visa Images*, Version 1.0.2, Lockstep Consulting (August 2016)
- *National Facial Biometric Matching Capability, Privacy Impact Assessment: AFP Access to DIBP FVS (Match & Search Functions) for Citizenship & Visa Images*, Version 1.0.2, Lockstep Consulting (August 2016)
- *National Facial Biometric Matching Capability, Privacy Impact Assessment: AFP Access to DIBP Face Verification Service (Retrieve Function) for Citizenship & Visa Images*, Version 1.2.2, Lockstep Consulting (August 2016)
- *National Facial Biometric Matching Capability, Privacy Impact Assessment: DFAT Access to DIBP Face Verification Service (Retrieve Function) for Citizenship & Visa Images*, Version 1.4.2, Lockstep Consulting (August 2016)
- *National Facial Biometric Matching Capability PIA – Use of Face Identification Service by specified agencies,* Information Integrity Solutions (March 2017)
- *National Driver Licence Facial Recognition Solution, Privacy Impact Assessment Report*, Information Integrity Solutions (November 2017)

B.2 Other Documents

- *NFBMC – Interoperability Hub User Scenarios*, Attorney General's Department, Version 0.6 (April 2015)
- *NFBMC – Portal Demo – User Scenarios: Interoperability Hub Project,* Attorney-General's Department (October 2015)
- *Benefits to State and Territory Law Enforcement & Related Agencies – NFBMC*, Attorney General's Department, Version 2.0 (April 2016)
- *FMS Training Policy: NFBMC,* Department of Home Affairs, Version 2.3 (undated)
- *FMS Compliance Policy: NFBMC,* Department of Home Affairs, Version 1.5 (December 2017)
- *LECAC Agencies – Legal Basis and Protective Security Policy*, Attorney General's Department (undated)
- *Comparative Protective Security Policy Frameworks*, Attorney General's Department (July 2016)
- *NFBMC FMS Memorandum of Understanding – Services*, Department of Home Affairs, Version 0.8 (January 2018)
- *NFBMC FMS Memorandum of Understanding – Services*, Between the Department of Home Affairs and the Queensland Police Service, Version 0.8 (January 2018)
- *Overview of security arrangements: National Driver Licence Facial Recognition Solution (NDFLRS),* Attorney General's Department (February 2018)
- *FIS Standard Offer – Five Role Types*, Attorney General's Department (undated)

- *FMS Participant Access Arrangement Template*, Department of Home Affairs (March 2018)
- *Face Verification Service (FVS) Access Policy – NFBMC*, Department of Home Affairs, Version 3.2 (March 2018)
- *Face Identification Service (FIS) Access Policy – NFBMC*, Department of Home Affairs, Version 2.4 (May 2018)
- *Face Matching Services (FMS) Participation Agreement*, Department of Home Affairs (June 2018)
- *Face Verification Service (FVS), Face Identification Service (FIS) and One Person One Licence Service (OPOLS): Data Flow Diagrams: NDFLRS Project*, Department of Home Affairs (September 2018)
- *FMS Governance Agreements Overview* diagram, Department of Home Affairs (September 2018)
- *MoU between AGD and OAIC for the provision of PIAs in relation to the NFBMC: https://www.oaic.gov.au/about-us/corporate-information/mous/mou-between-agd-and-oaic-for-the-provision-of-privacy-assessments-in-relation-to-the-national-facial-biometric-matching-capability#s2-commencement-and-term*

Appendix C – LECAC PIA Background Material

Readers of the LECAC PIA report are expected to be familiar with the following background material and context.

C.1 Identity Security Policy Framework

Governments across Australia have been concerned with the need to establish better ways to preserve and protect the identity of individuals for more than a decade. Formal work on addressing these policy concerns began in April 2005 when the Commonwealth announced plans to develop a national strategy to combat identity theft and the fraudulent use of stolen and assumed identities as a matter of national priority.[34] In particular, this provides the broader context for the FVS. Between 2005 and 2017, a significant amount of identity security work was undertaken, leading to the establishment of the NFBMC in 2017.

C.2 Identity Matching Services IGA

On 5 October 2017, the Commonwealth, states and territories agreed to the NFBMC and entered into the Identity Matching Services (IMS) IGA,[35] which is intended to:

> … promote the sharing and matching of identity information to prevent identity crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service delivery, while maintaining robust privacy and security safeguards.[36]

Relevantly, the IMS IGA presents *a continuum of purposes* for the NFBMC. These range from national security and law enforcement through to improved service delivery. Thus, the IMS IGA covers:

a broader group of participants than LECAC agencies; and

a broader range of services than the FVS and FIS. [37]

When reading this report, it is important to remember that the LECAC PIA is focused upon a subset of parties (LECAC agencies) and information flows (FVS, FIS). It is a piece of the NFBMC puzzle, rather than a stand-alone assessment.

C.3 NFBMC legal framework

The IMS IGA incorporates a commitment by all jurisdictions to ensure that the NFBMC is subject to an interoperable legal framework. As participation in the NFBMC is predicated upon an agency's ability to comply with all relevant legislative requirements, this is a key threshold issue for the LECAC PIA. Further, the ability to identify the broader legal environment is a pre-requisite to any privacy analysis. If the broader legal environment is not clear, there is a risk that the PIA may fail to identify or present a full and/or accurate set of issues. At the point the LECAC PIA was undertaken, legislative support remained under development.

Except as relevant and summarised throughout this report, limited information is provided about recent law reform efforts designed to ensure an interoperable legal

[34] See https://www.ag.gov.au/rightsandprotections/identitysecurity/pages/nationalidentitysecuritystrategy.aspx
[35] Special Meeting of the Council of Australian Governments (COAG) on Counter-Terrorism (Canberra: 5 October 2018) Communiqué: https://www.coag.gov.au/sites/default/files/communique/special-communique-20171005.pdf.
[36] See Recital A, IMS IGA.
[37] These are the Document Verification Service (DVS), FVS, FIS, One Person One Licence Service (OPOLS), Face Recognition Analysis Utility Service (FRAUS) and the Identity Data Sharing Service (IDSS) as well as any other identity matching or data sharing services to be developed under the IGA. See clause 1.3, IMS IGA.

framework. At a minimum, it is assumed that readers are familiar with the Commonwealth's *Identity-matching Services Bill 2018* (IMSB) and the *Australian Passports Amendment (Identity-Matching Services) Bill 2018 (*Australian Passports Amendment Bill) and related consideration by parliamentary committees.

C.4 Legislative frameworks in a federal system

Australia's federal system divides responsibility for passport, visa and citizenship information and images, and driver licence information and images between Commonwealth and state/territory agencies respectively. These data sources are subject to different Commonwealth, state and territory legislative regimes, each containing different purposes, requirements and/or exceptions and some of which may impose impediments to information sharing for NFBMC purposes.

So too, 'law enforcement' is largely undertaken as a state/territory responsibility by the relevant state/territory police forces, with the Commonwealth responsible for policing Commonwealth criminal laws, national security and border control. Each jurisdiction has its own law enforcement, crime and/or anti-corruption legislation.

The LECAC PIA assumes that readers are broadly aware of the diverse legislative frameworks applicable to passports, visa and citizenship arrangements and driver licence databases, as well as those applicable to law enforcement and national security in Australia.

C.5 Best practice governance

Governance will be key to the NFBMC's success. The NFBMC consists of hardware, software, technical capabilities and operational processes and procedures. The FVS and FIS operate within an information system. Governance of an information system does not occur in a vacuum. It needs to align with organisational governance overall, and be supported by, it. Good governance must be 'fit for purpose' so that 'the right people have the right access to the right information and functionality at the right time.' Successful governance of the FMS will require sustained and responsible collaboration between the Commonwealth, states and territories and their relevant agencies, with corporate and information governance reflecting this reality.[38]

The LECAC PIA is focused upon a specific aspect or component of governance, information governance, including associated operational policies, procedures and processes. This report assumes that readers have an understanding of best practice governance and information governance principles.

C.6 Privacy by Design

Privacy by Design was developed in the 1990s in response to the significant growth of ICT and networked data systems.[39] *Privacy by Design* seeks to entrench a more integrated approach to privacy in which privacy operates by default rather than as an exception. It introduced *7 Foundational Principles of Privacy by Design.* While *Privacy by Design* incorporates foundational 'principles', these are not intended to replace the privacy principles contained in privacy legislation. Instead, they provide a broader framework

[38] It is acknowledged that the need for collaboration will in future extend to foreign partners and the private sector.
[39] *Privacy by Design – The 7 Foundational Principles*, p.1. www.privacybydesign.ca. Ann Cavoukian, Onterio's Information and Privacy Commissioner, developed *Privacy by Design*. It has been an extremely successful concept, endorsed by the International Association of Data Protection Authorities and Privacy Commissioners, the US Federal Trade Commission, the European Union and privacy professionals across the world. See, Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* (December 2012): https://gpsbydesign.org/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/.

within which to consider and apply the privacy principles. They are particularly helpful in the context of developing information systems.

'Privacy by design' has been incorporated as a design feature of the NFBMC. It has been used to help develop a positive and proactive NFBMC privacy framework, including relevant components of the IMS IGA, the FMS data sharing framework and the iterative PIA process. When the OAIC or the Commonwealth refer to 'privacy by design', it incorporates reference to Privacy by Design and the 7 Foundational Principles.[40]

This report assumes that readers have a reasonable understanding of the meaning and application of *Privacy by Design.*

[40] See also, OAIC, *Privacy Management Framework* (May 2015), p.3: 'adopt a "privacy by design" approach. Ensure you consider the seven foundational principles of privacy by design in all your business projects and decisions that involve personal information': https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

Appendix D – State/Territory Collated Questionnaire Responses

D.1 Legislative Authority

Legislative Authority	
Under the *Intergovernmental Agreement on Identity Matching Services* (IGA (October 2017), the Commonwealth, States and Territories agreed to preserve or introduce legislation to support the collection, use and disclosure of facial images and related identity information between the parties using the FMS and interoperability hub. The purpose of this section of the questionnaire is to obtain complete and up-to-date information about existing and any proposed state and territory legislation authorising law enforcement, crime and anti-corruption (LECAC) agencies to participate in the FMS.	
1.1 What existing legal authority will authorise LECAC agencies in your jurisdiction to participate in the FMS? Please list relevant laws, including specific sections within those laws, below. Include hyperlinks to current versions of any legislation listed. Where different laws/provisions apply to different LECAC agencies, please list these separately.	
Respondent	Response
NSWPF	There is no legislative framework expressly authorizing the NSWPF to collect, use or disclose information for the purposes of using face matching information. An express legal authority is not a pre-requisite for the lawful use of the Capability.
NSW CC	In the absence of any legislation impeding access to the Capability, the NSWCC is inherently authorised to access information, including information from the Capability, in the performance of its investigation functions as specified in the *Crime Commission Act 2012.* The laws that authorise the NSWCC to pursue and access information, including information from the Capability, are all contained within the *Crime Commission Act 2012.* Specific provisions are as follows: • Section 10 (1)(a) • Section 10 (1)(1a) • Section 10 (1)(d) • Section 10 (1)(f) • Section 10 (1)(g) • Section 11 • Section 11A (7) • Section 14 https://www.legislation.nsw.gov.au/#/view/act/2012/66/full
NSW LECC	Section 161 of the LECC Act enables the LECC to provide information to State and Commonwealth agencies and bodies for the purpose of its investigations. This would include the provision of names, addresses, photos etc. for the purpose of making requests to the Commonwealth for face verification or face identification. The secrecy obligations contained in s 180 of the LECC Act impose a strict regime on LECC officers for handling such confidential information obtained from the Commonwealth. https://legislation.nsw.gov.au/#/view/act/2016/61/full
NSW ICAC	Independent Commission Against Corruption Act 1988 (NSW) *s. 16(3) and s. 111* Privacy and Personal Information Protection Act 1998 *s.8, s. 17 and s. 27* Law Enforcement and National Security (Assumed Identities) Act 2010 *(NSW) s. 27(2)* https://legislation.nsw.gov.au/#/view/act/1988/35/full

QLD Police Service (QPS)	Part 10, Division 1AA 'National identity matching services' of the *Police Service Administration Act 1990.* *https://www.legislation.qld.gov.au/view/pdf/inforce/2018-03-16/act-1990-004* Key sections include: Section 10.2FC 'Disclosure of identity information by commissioner' which authorises the commissioner to disclose identity information to the host agency or a participating entity in the service. Section 10.2FD 'Collection and use of identify information by commissioner', which authorises the commissioner to collect and use identity information provided through the operation of the service by the host agency or a participating entity. Section 10.2FF 'Disclosure, use or collection must be for permitted purpose' which provides that the collection, use and disclosure of identity information must be for a permitted purpose.
SA Police Agency	*Public Sector (Data Sharing) Act 2016* (SA) – s13 and s8
SA ICAC	*Independent Commissioner Against Corruption Act 2012* (SA) – s50 and s52
ACT Policing	s.37 *Road Transport (Driver Licensing) Act 1999* *http://www.legislation.act.gov.au/a/1999-78/default.asp* *Crimes (Assumed Identities) Act 2009* *http://www.legislation.act.gov.au/a/2009-33/default.asp* *s230(3) Crimes Act 1900* *http://www.legislation.act.gov.au/a/1900-40/default.asp* *Privacy Act (Cth)* *Information Privacy Act 2014 (ACT)*
TAS	Vehicle and Traffic (Driver Licensing & Vehicle Regulation) Amendment (Identity Matching Services) Regulations 2017 was enacted to sharing as per the IGA https://www.legislation.tas.gov.au/view/html/inforce/current/sr-2017-113 Personal Information Protection Act 2004 https://www.legislation.tas.gov.au/view/html/inforce/current/act-2004-046 personal information means any information or opinion in any recorded format about an individual – (a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and (b) who is alive or has not been dead for more than 25 years; Schedule 1 contains Personal Information Protection Provisions however section 9 contains a Law Enforcement Exemption – which includes various parts Schedule 1. LE use covered by: (g) the personal information custodian reasonably believes that the use or disclosure is reasonably necessary for any of the following purposes by or on behalf of a law enforcement agency: (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; (iii) the protection of the public revenue; (iv) the prevention, detection, investigation or remedying of conduct that is in the opinion of the personal information custodian seriously improper conduct; (v) the preparation for, or conduct of, proceedings before any court or tribunal or

	implementation of any order of a court or tribunal; (vi) the investigation of missing persons; (vii) the investigation of a matter under the Coroners Act 1995 ; Disclosure interstate is also covered by: A personal information custodian may disclose personal information about an individual to another person or other body who is outside Tasmania only if – (a) the personal information custodian reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that has principles for fair handling of the information that are substantially similar to the personal information protection principles; or (b) the individual consents to the disclosure; or (c) the disclosure is necessary for – (i) the performance of a contract between the individual and the personal information custodian; or (ii) the conclusion or performance of a contract concluded in the interest of the individual between the personal information custodian and a third party; or (d) the personal information custodian has taken reasonable steps to ensure that the information which it has disclosed is not to be held, used or disclosed by the recipient of the information inconsistently with the personal information protection principles; or (e) the disclosure is authorised or required by any other law.
WA Police	*Police Act 1892* and subsidiary legislation, specifically s 607 *Police Force Regulations 1979*. https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a615.html
WA CCC	Protection of Commission Assumed Identities: The Corruption, Crime and Misconduct Act 2013 provides that the ability for the Commission to grant approval for the acquisition and use of an assumed identity by an officer of the Commission. Access to and use of the FMS will provide the Commission the capacity to protect authorized Commission assumed Identities. MDL Photograph Access: The Road Traffic Act 1974 provides the Director General with the permission of the Commission of Police the power to provide access to photographs which are required for the purposes for the performance of the law enforcements official's function under a written law. The CCM Act confers a number of functions upon the Corruption and Crime Commission. Its primary purpose is to combat and reduce the incidence of organized crime and to improve continuously the integrity of, and to reduce the incidence of misconduct in, the public sector. https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a6503.html https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_27379.pdf/$FILE/Road%20Traffic%20Act%201974%20-%20%5B12-e0-00%5D.pdf?OpenElement
VIC Police Agency	**Refer** Statement of Legislative Compliance
1.2 Do any LECAC agencies in your jurisdiction require additional authorising legislation to enable them to participate fully in the FMS?	
Respondent	Response
NSW	No
QLD	No
SA	No

ACT	Maybe
TAS	No
WA Police	No
WA CCC	No
VIC	No

1.3 If yes, please provide a reference below to the enabling legislation (e.g. *Police and Other Legislation (Identify and Biometrics Capability) Act 2018* (Qld)) or provide an outline of the legislative proposal and current timetable for introduction. If your jurisdiction has not yet undertaken a legislative analysis on this issue, please indicate when such an analysis may be completed.	
Respondent	Response
NSW	**Road Transport Act 2013** Transport for NSW advised that a Bill is being put before Parliament to amend the Road Transport Act 2013. If approved, the amendment will allow RMS to disclose driver license images to the Commonwealth for storage in the NDLFRS. NSWPF has advised a legislative amendment should be considered. This would give express authorisation for NSWPF to collect, use and disclose information through the Capability. NSWPF noted that QLD has recently passed legislation authorising access to the Capability.
QLD	No response
SA	N/A
ACT	ACT as a jurisdiction has not yet undertaken legislative analysis on this issue. It is anticipated that this analysis will commence in July 2018 and be finalized in early 2019.
TAS	N/A
WA Police	No response
WA CCC	No response
VIC	N/A

1.4 Do you have any specific concerns about legal authority that need to be considered during the PIA process? For example, limitations or conditions on legal authority that need to be satisfied?	
Respondent	Response
NSW	No
QLD	No
SA	No
ACT	Yes
TAS	No
WA Police	No
WA CCC	No
VIC	No

1.5 If yes, please outline these concerns below (and provide contact details for any follow up required)	
Respondent	Response
NSW	N/A
QLD	No response
SA	No response
ACT	Application of *Human Rights Act 2004* (ACT)
TAS	N/A
WA Police	No response
WA CCC	No response
VIC	N/A

D.2 Privacy

Privacy
The *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs) provide the applicable privacy law framework for Commonwealth agencies participating in the FMS. At the State and Territory level, some LECAC agencies are subject to State/Territory privacy legislation (to varying degrees) while other LECAC agencies are exempt from privacy legislation altogether. Under the FMS Participation Agreement, certain LECACs in jurisdictions without privacy laws will be obliged to comply with the APPs. The purpose of this section of the questionnaire is to obtain complete and up-to-date information about state and territory privacy legislation, in particular, the degree to which - if at all - State/Territory privacy legislation is applicable to the participation of LECAC agencies in the FMS.

2.1 Does your jurisdiction have privacy/information privacy/data protection laws?	
Respondent	
NSW	Yes
QLD	Yes
SA	No
ACT	Yes
TAS	Yes
WA Police	No
WA CCC	No
VIC	Yes

2.2 Does your jurisdiction have alternative arrangements for the protection of information privacy? (For example, administrative arrangements)	
NSW	Yes
QLD	Yes
SA	Yes
ACT	No
TAS	Yes

WA Police	Yes
WA CCC	Yes
VIC	No
2.3 If yes, please list the title of relevant privacy legislation/administrative arrangements as well as hyperlink(s) to current versions	
NSW	Privacy and Personal Information Protection Act 1998 Health Records and Information Privacy Act 2002. Information Protection Principles All documents can be found on the Information Privacy Commission website - https://www.ipc.nsw.gov.au/privacy
QLD	The QPS are subject to all 11 Information Privacy Principles (IPP) contained within the *Information Privacy Act 2009* (Qld) (IP Act), with QPS IPPs mirroring Commonwealth APP framework. https://www.legislation.qld.gov.au/view/pdf/inforce/current/act-2009-014
SA	Title: Information Privacy Principles Instruction – more information can be found on the State Records website. Under the FMS Participation Agreement, SA agencies will also be obliged to comply with the Australian Privacy Principles.
ACT	*Information Privacy Act 2014* http://www.legislation.act.gov.au/a/2014-24/default.asp
TAS	Title: Personal Information Protection Act 2004 https://www.legislation.tas.gov.au/view/html/inforce/current/act-2004-046 Schedule 1 contains Personal Information Protection Provisions however section 9 contains a Law Enforcement Exemption. Title: Police Service Act 2003 (Code of Conduct) – Division 1 https://www.legislation.tas.gov.au/view/html/inforce/current/act-2003-075 Administrative arrangements e.g. Code of Ethics contained in the Tasmania Police Manual mirror the Police Service Act.
WA Police	The WA Government has administrative arrangements through a Public Sector Commissioner's Circular requiring public sector agencies to comply with the Australian Privacy Principles. See Public Sector Commissioner's Circular 2014-02 (Policy Framework and Standards for Information Sharing between Government Agencies). https://publicsector.wa.gov.au/document/public-sector-commissioners-circular-2014-02-policy-framework-and-standards-information-sharing-between-government-agencies WA Police Force Policy on Information Release and Sharing and WA Police Force Privacy Statement which requires compliance with the Public Sector Commissioner's Circular (AD 85.00)
WA CCC	The WA Government has administrative arrangements through a Public Sector Commissioner's Circular requiring public sector agencies to comply with the Australian Privacy Principles. See Public Sector Commissioner's Circular 2014-02 (Policy Framework and Standards for Information Sharing between Government Agencies). https://publicsector.wa.gov.au/document/public-sector-commissioners-circular-2014-02-policy-framework-and-standards-information-sharing-between-

	government-agencies The CCM Act provides the requirement for officers of the Commission disclose official information unless under or for the purposes of the Act; otherwise in connection with the performance of the persons functions under the Act. https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a6503.html
VIC	*Privacy and Data Protection Act 2014* *Health Records Act 2001*
2.4 Are LECAC agencies subject to your jurisdiction's privacy legislation/administrative arrangements?	
NSWPF	Privacy Code of Practice NSW Police Service
NSW CC	Yes, the *Privacy and Personal Information Protection Act 1988* ('the Act') which broadly reflects the Commonwealth *Privacy Act 1988* in that it provides a list of Information Privacy Principles ('IPPs') for the collection, storage, accuracy, access and use of 'personal information', which would include biometric information.
NSW LECC	Privacy and Personal Information Protection Act 1998 and Health Records and Information Privacy Act 2002.
NSW ICAC	Privacy and Personal Information Protection Act 1998
QLD Police	Yes
SA Police agency	Yes
SA Anti-corruption agency	No
ACT Police agency	Yes
TAS Police agency	Yes
WA Anti-corruption Agency	Yes
WA Police Agency	Yes
WA CCC	Yes
VIC Police agency	Yes
VIC IBAC	Yes
2.5 If a partial exemption applies, please provide relevant section references within the privacy legislation/administrative arrangements?	
NSWPF	The NSWPF is exempt from compliance with the information protection principles in the Privacy and Personal Information Protection Act 1998, except in relation to the NSWPF's 'administrative and educative functions' (see sections 27 (1)-(2) of the

	Act).
NSW CC	Section 27 of the Act provides that the NSW Crime Commission is not required to comply with the IPPs unless in connection with the exercise of its 'administrative or educative functions'.
NSW LECC	Exemptions are included in sections 23, 27 and 27A of the Privacy and Personal Information Protection Act 1998.
NSW ICAC	Privacy and Personal Information Protection Act 1998 s. 27
QLD Police Service	IP Act: Section 29 'Special provision for law enforcement agencies' Schedule 1 'Documents to which the privacy principles do not apply' QPS is exempt from Schedule 3 Information Privacy Principles 2, 3, 9, 10 and 11 as outlined below: IPP 2: provide a collection notice; IPP 3: only collect relevant, complete and up to date personal information, and do not intrude unreasonably on an individual's personal affairs; IPP 9: only use relevant personal information; IPP 10: only use personal information for the purpose for which is was collected, unless an exception applies; and IPP 11: do not disclose personal information to anyone but the individual it is about, unless an exception applies. https://www.legislation.qld.gov.au/view/whole/html/inforce/current/act-2009-014
SA Police agency	Not applicable
SA ICAC	Schedule: Clause 2, Information Privacy Principles Instruction
ACT	No response
TAS Police Agency	Exemption in Section 9
WA Police	No response
WA CCC	No response
VIC Police Agency	*Privacy and Data Protection Act 2014* – Section 15. This section would only be used where an Information Privacy Principle may not be applicable.
VIC IBAC	*Privacy and Data Protection Act 2014* – *Section 15*
2.6 Has your jurisdiction conducted any PIA processes for participation in the FMS?	
NSW	No
QLD	Yes
SA	No
ACT	No
TAS	No
WA Police	No
WA CCC	No

VIC	No
2.7 Do you have any specific concerns about privacy that need to be addressed during the PIA process?	
NSW	No
QLD	No
SA	No
ACT	No
TAS	No
WA Police	No
WA CCC	No
VIC	No
2.8 If yes, please outline these concerns below (and provide contact details for any follow up required)	
NSW	No response
QLD	No response
SA	No response
ACT	No response
TAS	N/A
WA Police	No response
WA CCC	No response
VIC	No response

D.3 Protective Security

3. Protective Security
The Commonwealth Protective Security Policy Framework (PSPF) is the applicable protective security framework for Commonwealth agencies participating in the FMS, including Home Affairs' role as Hub Controller and Framework Administrator. The PSPF will provide the *default* protective security framework for the FMS in relation to State/Territory Law Enforcement, Crime and Anti-Corruption Agencies (LECAC) — as Requesting Agencies — unless State/Territory jurisdictions have an equivalent protective security framework in place (equivalent includes both the level of protection and the degree of coverage). The purpose of this section of the questionnaire is to obtain complete and up-to-date information about state and territory protective security arrangements and associated policy documents.

3.1 Will your jurisdictional protective security framework provide the basis for your jurisdiction's LECAC agencies to participate in the FMS?	
NSW	Yes
QLD	Yes
SA	Yes
ACT	Yes

TAS	No (We will use the Commonwealth PSPF.)
WA Police	No
WA CCC	No
VIC	Yes
3.2 If yes, please list the title of the relevant protective security policy and provide a hyperlink to the current version of your protective security policy	
NSW	Commonwealth Protective Security Framework NSW Digital Information Security Policy https://www.finance.nsw.gov.au/ict/sites/default/files/Digital%20Information%20Security%20Policy%202015.pdf
QLD	The Queensland Government Chief Information Officer (QGCIO) remains responsible for establishing information security requirements and monitoring compliance for all Queensland government agencies. These requirements are detailed in the Queensland Government information security classification framework (QGISCF), Information Standard 18 (IS18:2018), which covers all types of information, including facial biometric information. https://www.qgcio.qld.gov.au/__data/assets/pdf_file/0019/4258/QGISCF_v3_1_0.pdf https://www.qgcio.qld.gov.au/documents/information-security-is18-information-standard In addition to these arrangements, Queensland is currently considering implementation of a *Queensland Protective Security Framework* to give more jurisdictionally-specific effect to the Commonwealth Protective Security Policy Framework.
SA	Title: PC030 – Protective Security Policy Framework
ACT	ACT Policing is subject to the AFP protective security policy framework as set by the Commonwealth Government.
TAS	N/A
WA Police	No response
WA CCC	No response
VIC	Title: Victorian Protective Data Security Standards (VPDSS)
3.3 What is the authority for your jurisdiction's protective security framework? For example, is it a law/a policy/set of rules?	
NSW PF	Applies the NSW Digital Information Security Policy and are certified against ISO27002:2013. Further, the NSW Digital Information Security Policy underpins the NSWPF Information Security Manual (2017). NSWPF also recognises the Commonwealth Protective Security Framework and applies most of its requirements. There is also the Information Security Policy Statement (2015).
NSW CC	The Commission recognises the Commonwealth Protective Security Policy Framework (PSPF). This is a feature of the emerging Security Framework for the Commission. The Security Framework for the Commission is an overarching security framework which is being developed to integrate three

	major tranches, including: a) Tranche 1 — Personnel Security (Security Vetting and Clearances) b) Tranche 2 — Physical Security (Personal and Physical Security) c) Tranche 3 — Information Security (ICT and Information Security) As appropriate the Commission applies the PSPF, the Australian Government Information Security Management (AGISM), Business Continuity Management and Planning; and is currently developing the IS027001:2015 Information Security Management Systems for accreditation later this calendar year. Other policies and manuals include: a) NSW Digital Information Security Policy (DISP), August 2015 b) NSW Security Guidelines, August 2017 c) NSW Government Information, Classification, Labelling and Handling Policy, July 2015 d) Protective Security Policy Framework (PSPF) — Commonwealth e) Australian Government Information Security Management (AGISM) — Commonwealth f) Australian Government Personnel Security Management (AGISM) — Commonwealth g) Australian Government Physical Security Management (AGISM) — Commonwealth
NSW LECC	The LECC's Physical Security (Personnel and Premise) Policy and Procedure framework seeks to apply the security principles outlined in the Australian Government's Protective Security Policy Framework (PSPF), which includes reference to the Security Construction and Equipment Committee (SCEC) and ASIO T4 Protective Security (ASIO T4) standards. The LECC is currently undertaking a review and upgrade of its ISMS polices in line with the NSW Digital Information Security Policy.
NSW ICAC	Recognises the Commonwealth Protective Security Framework and NSW Digital Information Security Policy. It also operates Information Security Management System framework based on ISO27001:2013.
QLD	IS18:2018 is governed by policy.
SA	It is a policy that must be complied with by all South Australian government agencies and contains specific requirements and responsibilities for Chief Executives.
ACT	It is established under the Commonwealth Protective Security Policy Framework (PSPF)
TAS	N/A Tasmania will use the PSPF.
WA Police	Policy Information Systems and Security (AD – 71.00) Restricted Access to Information on the Police Computer System (LO-01.06)
WA CCC	The CCM Act provides the requirement for officers of the Commission disclose official information unless under or for the purposes of the Act; otherwise in connection with the performance of the persons functions under the Act. https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a6503.html
VIC	VPDSS

3.4 How is compliance with the protective security framework assured? Who is responsible for reviewing compliance?	
NSW Police agency	NSWPF has developed a self-assessment maturity model to identify risk in relation to Framework strategies. A Protective Security and Governance Committee has been established to steer the implementation and ongoing governance of protective security within the NSWPF. The objective of the committee is to ensure that a security culture is embedded through the NSW PF to safeguard its people, information and assets. An Agency Security Executive and an Agency Security Advisor have also been appointed to enhance the security culture within the NSWPF.
NSW Crime Commission	The Commission operates a security framework steering group which has responsibility for the framework and implementation, integration and compliance as appropriate with the PSPF and other aspects. Compliance responsibility is with the Executive Director, Corporate Services. Key elements of the security framework tranches are subject to internal audits which report to the Chief Audit Executive of the Commission and the Independent Audit and Risk Committee. The Commission also undertakes internal audits of some areas as part of established Memorandum's of Understanding with Commonwealth and State Agencies which provide the Commission with access to information and information management systems.
NSW LECC	The LECC has various audit controls relating to physical and information security at the Commission. The controls are coordinated by the Manager Risk and Security who reports directly to the Chief Executive Officer. The Manager Risk and Security has the policy remit to conduct investigations into breaches of security at the Commission.
NSW ICAC	Audits are completed by Sai Global.
QLD	Third party service delivery agreements must comply fully with IS18:2018; Third party service delivery agreements must be periodically reviewed and updated to ensure they address changes in business requirements, but remain compliant with IS18:2018; and Third party service operating agreements must specifically address third party governance policies and processes. A threat and risk assessment must be conducted for all ICT assets that create, store, process or transmit security classified information at least annually, or after any significant change has occurred, such as machinery-of-Government. The policy provides for all information security compliance activities relating to information security policies and standards. Reporting obligations relating to information security must be complied with and managed appropriately. An information security compliance checklist must be submitted annually to the ICT Policy and Coordination Office in line with IS18:2018 reporting requirements.
SA	Under section 4 of the framework, Ministers are responsible for the security of assets in their portfolios. This section also creates specific obligations on Chief Executives in implementing and administering the Protective Security Policy Framework. Including the establishment of an Agency Security Executive which oversees a compliance program. The Chief Executive must also appoint an Agency Security Adviser and an Information Technology Security Adviser, which report to the Agency Security Executive. The Agency Security Executive overseas the compliance program with the Protective Security Policy Framework in each Agency. The Auditor General may review an agency's protective security compliance program and assess it in the context of the Protective Security Policy Framework.

ACT	AFP ensures compliance with the protective security framework through inclusion in the Commissioner's Order on Security (CO9). AFP Security are responsible for reviewing compliance. If there are any instances of non-compliance, these are referred to AFP Professional Standards for investigation and action.
TAS	Tasmanian Auditor General Audit 3Rd Party Audit Internal Audit Manager Information Security Department of Police, Fire and Emergency Management e-mail:Information.Security@dpfem.tas.gov.au phone: 03 61732480
WA Police	As a participant in the FMS, WA Police Force will comply with the Cth PSPF. Access to, and use of information in the FMS will be monitored by WA Police Force Intelligence Portfolio, State Intelligence, Specialist Support Unit (SSU) Internal Guidelines will be developed to ensure compliance with the PSPF The WA Police Specialist Support Unit (SSU) WA Police Force Internal Affairs Unit (IAU)
WA CCC	As a participant in the FMS, WA Police Force will comply with the Cth PSPF. Access to, and use of information in the FMS will be monitored and audited by Commission auditors and processes Internal Policy and procedures will be development to ensure compliance with the PSPF. Director Operations, Corruption and Crime Commission Parliamentary Inspector
VIC	An organisation must perform an annual assessment of their implementation of the VPDSS and report their level of compliance to the Commissioner for Privacy and Data Protection. Commissioner for Privacy and Data Protection
3.5 Please describe the breadth and depth of your framework, including: a. whether the framework covers physical, information and personnel security, b. whether it applies to all potential Users of the FMS, and c. any other relevant information, so that a high-level 'equivalency' assessment can be undertaken as part of the PIA process.	
NSWPF	The Protective Policy Security Framework covers the protection of people, information and assets; it includes four key tiers – governance security, physical security, personnel security, and information security; and applies to all NSW employees.
NSWCC	The Commission's security framework's individual components and the overarching framework in development cover all aspects of physical, information and personnel security. It provides effective cover to all Commission staff, contractors and consultants to the Commission and this would be extended to the new Biometrics capability.
NSW LECC	All potential users with access to the system will have a minimum AGSVA Negative Vetting 1 clearance level. The system will be located within a secure area of the Commission with appropriate physical and information controls in place to support

	its operation.
NSW ICAC	Yes. The framework covers physical, information and personnel security, it applies to all commission staff and contractors.
QLD	a. QGISCF, IS18:2018, includes information assets.
	b. Yes, QGISCF, IS18:2018 applies to all potential FMS users.
SA	a. The framework covers Information Security; Personnel Security; Physical Security; Procurement Security; Security Incidents and Investigation; Security When Working Away from the Office
	b. All Users of FMS will be covered by PC030 – Protective Security Policy Framework.
	c. PC030 may be amended as a result of changes to the Commonwealth PSPF.
ACT	a. The protective security framework covers physical, information and personnel security.
	b. It applies to all AFP personnel, therefore will apply to all users of FMS.
	c. To fulfil the expectations of the Cth Protective Security Framework, the AFP: • applies a risk-based approach to protecting its information and ICT systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability • has adopted its own security principles • supports the guiding principles and strategic priorities outlined in the Australian Government Cyber Security Strategy • has adopted its own minimum physical security standards for planning, selecting, designing and modifying AFP facilities • builds security into AFP culture, its practices and operational plans • establishes protective security measures to ensure the safety and security of its personnel • manages security risks to prevent harm to personnel, official resources and disruption to business objectives • maintains high standard vetting principles and applies the character standards of honesty, maturity, trustworthiness, loyalty, tolerance and resilience.
TAS	N/A Tasmania will be using the PSPF.
WA Police	a. This document is still under development by WA Police, which is being modeled on the PSPF.
	b. As above
	c. As above
WA CCC	a. This document is to be developed the CCC, which will align with the requirements within the PSPF.
	b. As above
	c. As above
VIC	a. Yes, the VPDSS covers physical, information & personnel security
	b. Yes, the VPDSS covers users of the FMS
	c. See Statement of Legislative Compliance (Victoria Police-Department of Home Affairs

Appendix E – Law Enforcement, Biometrics, Privacy Risks

E.1 General Law Enforcement, Biometrics and Privacy Risks

A high-level literature review undertaken during the PIA process revealed a common set of privacy risks associated with the use of biometric face matching systems by law enforcement agencies.[41] These common or general privacy risks are summarised below.

- Biometric face matching deployed against large, government-held databases of facial images has the capacity to facilitate the monitoring or surveillance of citizens by law enforcement agencies and, by extension, government, raising concerns about individual autonomy and privacy and a potential 'dampening' effect upon democracy
- Law enforcement agencies' use of biometric face recognition systems is viewed as a form of surveillance by stakeholders and the general public, resulting in a lack of support for, or opposition to, their deployment
- Law enforcement agencies' adoption of biometric face recognition systems may be implemented in a legal, regulatory or policy vacuum without adequate oversight
- The use of biometric facial recognition systems by law enforcement agencies for identification purposes may cause disadvantage or harm to people who have not committed any offence, e.g. an 'innocent' person becomes a person of interest as a result of a false positive match and may be required to bear responsibility for establishing that an error has occurred
- The return of 'galleries' of potential persons of interest (suspects or witnesses) may result in the permanent retention of personal information in law enforcement databases about individuals who have not committed any offence
- The benefits of the biometric system must outweigh the degree of privacy intrusion posed by the system. If relevant metrics have not been collected/are not available for a benefits realisation analysis, it is not possible to measure whether or not the system is meeting expectations in terms of outcomes, accuracy and utility, thereby preventing an assessment of whether or not the degree of privacy intrusion is justified
- Limitations on the further use or disclosure of biometric information are difficult to enforce once the information has been disclosed
- Facial recognition systems and the algorithms that enable them to function are not sufficiently transparent
- Facial recognition systems and the algorithms that enable them to function have greater difficulty identifying women and non-Caucasian males
- The potential for secondary use or function creep is significant, for example, a system designed to help identify perpetrators of serious criminal offences may subsequently be extended to the administration of parking offences

[41] International Justice and Public Safety Network (NIets), *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field (2011);* Robee Krishan, Reza Mostafavi, 'Biometric technology, security and privacy concerns' *Journal of Internet Law (*July 2018) 19-23; Tim Ring, 'Privacy in peril: is facial recognition going too far too fast? *Biometric Technology Today* (July-August 2016) 7-11; Clare Garvie and Jonathan Frankle, 'Facial-Recognition Software Might Have a Racial Bias Problem' *The Atlantic* (7 April 2016); Jessica Gabel Cino, 'Facial Recognition is increasingly common, but how does it work? *The Conversation,* (5 April 2017).

- Information privacy law does not apply to personal information when it is collected, used and/or disclosed for law enforcement purposes as law enforcement agencies are subject to complete or partial exemptions from privacy legislation

E.2 Surveillance' as a Key Privacy Perception Risk

'Surveillance' is *routinely identified as a privacy risk* arising from the deployment of biometric systems. Many organisations deploying biometric systems balk at the label 'surveillance' being applied to their activities, not least because of its negative connotations. However, avoidance of this term altogether may result in it functioning as a 'shadow' to any privacy analysis of the NFBMC, because journalists, civil society and individuals are likely to categorise the NFBMC (including the FVS and FIS) as a form of (actual or prospective) surveillance.[42] This approach rapidly results in an impasse, with both 'sides' convinced of the validity of their respective arguments. In order to move beyond this impasse, the connection between 'surveillance' and privacy is considered in relation to personal information and, therefore, privacy.

Until recently, 'surveillance' was defined primarily as 'close observation, especially of a suspected spy or criminal' (Oxford English Dictionary). As a result, historically, 'surveillance' carries an association with illegal behaviour, especially when coupled with law enforcement or national security activities.

However, for many contemporary commentators, 'new surveillance technologies' are not restricted to the identification of a suspect or criminal but rather comprise 'the use of technical means to extract or create personal data … taken from individuals or contexts' and applied categorically (e.g. to a specific group or an entire population), rather than to an individual 'person of interest' (POI) alone. This broadens the applicability of the term 'surveillance' beyond a government and law enforcement context to a wide range of information services voluntarily adopted by individuals, including social media networks, online search engines, epidemiological programs and supermarket loyalty programs.

While personal information has always provided a link between privacy and surveillance, in a networked society, fuelled by the collection and dissemination of personal information, enables the widespread tracking of individuals' digital footprints without their full knowledge or consent. This is viewed as a new form of surveillance (e.g. 'surveillance capitalism', 'surveillance platforms') that both extends existing privacy issues and risks, and produces new privacy issues and legal policy problems. The definition of 'surveillance' is changing in line with technological and social changes.

It is not possible to avoid a discussion of 'surveillance' issues in a biometrics context. Even if the NFBMC (FVS, FIS) is described as a form of surveillance – because it uses biometric face matching technology to extract personal information for verification and identification purposes – this raises questions about the degree to which the specific privacy risks arising from the deployment of the FVS and FIS are 'new' or 'different' and how these risks can and should be mitigated.

[42] See, for example, Nigel Gladstone, 'Surveillance State: NSW intensifies citizen tracking', SMH (4 November 2018): https://www.smh.com.au/national/nsw/surveillance-state-nsw-intensifies-citizen-tracking-20181019-p50atw.html.

Appendix F – Adaptation of NIST Framework for FVS/FIS Privacy Operationalisation

No.	Privacy Control	Implementation	Status
1	**Transparency**		
1.1	NFBMC website	Confirm development of NFBMC website by Home Affairs (or alternative means) to provide more detailed and good quality information to interested parties and the general public; LECAC agencies provide link to website	
1.2	Privacy Policy	Confirm development of NFBMC privacy policy by Home Affairs; LECAC agencies to adopt relevant text/ensure consistent text is included in local/jurisdictional privacy policy	
1.3	Privacy Notice	Confirm that DHAs have included an appropriate privacy notice in relation to relevant data holdings; LECAC agencies provide notice (unless it is not appropriate to do so on operational grounds)	
2	**Authority and Purpose**		
2.1	Authority to Collect	Authority to collect is core to participation in the NFBMC, including the FVS and FIS; identify relevant authority and document in Police Manual/related policies and procedures. Note overlap with PAA process	
2.2	Purpose Specification	Purposes outlined in IGA and FMS Data Sharing Framework; document purposes in Police Manual/related policies and procedures. Note overlap with PAA process	
3	**Accountability, Audit and Risk Management**	**Document approach to each category**	
3.1	Governance and privacy program	Ensure appropriate privacy governance arrangements (e.g. as per LECAC PIA recommendations); this includes assigning responsibility for privacy governance to the Coordination Group Ensure privacy training and information is provided to staff members	
3.2	Privacy impact and Risk Assessment	Commit to/undertake PIAs and related risk assessments for any changes to the collection and/or handling of FVS/FIS data; document in Police Manual/related policies and procedures as/if relevant	

3.4	Privacy monitoring and auditing	Outline how prescribed monitoring/auditing under the FMS Data Sharing Framework will be delivered and the roles responsible for reviewing reports and/or actioning recommendations arising from audit reports; document in Police Manual/related policies and procedures	
3.5	Privacy reporting	Consider the role of benefits realisation/collection of relevant metrics to assess whether or not the intrusion into individuals' privacy is justified in terms of public benefit	
3.6	Privacy-enhanced system design and development	Not directly applicable to LECAC agencies; however, retain support for Privacy-by-Design for future releases and developments or any local system development	
4	**Data Quality and Integrity**		
4.1	Data Quality	Identify how the quality of data obtained from the FVS/FIS will be checked, e.g. additional investigations undertaken to confirm or verify identity; document in Police Manual/related policies and procedures as/if relevant, ongoing monitoring for false positives and false negatives	
4.2	Data Integrity	Identify how the integrity of data retained from the FVS/FIS will be ensured; refer to local protective security framework; document in Police Manual/related policies and procedures as/if relevant	
5	**Data Minimisation and Retention**		
5.1	Minimisation of personal information	Not applicable to LECAC agencies, except in relation to the retention of FIS galleries, which should be guided by the degree to which the gallery assists an approved investigation. Home Affairs has minimised the collection, use and disclosure of personal information via the FVS and FIS in line with privacy principles and a Privacy-by-Design approach to system development. Data Holding Agencies will also seek to provide the minimum amount of data when negotiating PAAs	
5.2	Data retention and disposal	Confirm time limits for data retention (e.g. permanent retention) and, if appropriate, its disposal (in line with public records requirements)	
5.3	Minimisation of personal information used in testing, training	Ensure that testing and training are subject to privacy assessment to ensure that any risks have	

	and research	been ameliorated	
6	**Individual Participation and Redress**		
6.1	Consent	Confirm that any consent-based use of the FVS has an appropriate consent mechanism; aim to ensure consistency across LECAC agencies; document in Police Manual/related policies and procedures	
6.2	Individual Access	Confirm any arrangements under FOI and identify where information may be withheld; document in Police Manual/related policies and procedures	
6.3	Complaint Management	Confirm/ensure that existing complaint management processes can be leveraged for privacy complaints. Ensure that an appropriate regulator (e.g. privacy commissioner, Ombudsman) is able to receive privacy complaints	
7	**Security**		
7.1	Inventory of personal information	Confirm/ensure that local protective security arrangements are fit for purpose; where no protective security arrangements are in place, refer to the Commonwealth's PSPF and ISM; document in Police Manual/related policies and procedures	
7.2	Privacy incident response	Leverage existing approach to privacy incidents (base response upon security incident response where no privacy incident response exists). Ensure that there is no duplication. Document in Police Manual/related policies and procedures; agreed approach to data breach notification	
8	**Use and Disclosure Limitation**		
8.1	Internal use	Limit use of FVS/FIS data to that which is permitted under the IGA, FMS Data Sharing Framework, etc. Document in Police Manual/related policies and procedures. Minimise the number of roles with authorised access. Restrict access to FIS to a single unit or group with specialist skills	
8.2	Disclosure/information sharing	The FVS/FIS enable information sharing to take place. The technical and policy framework developed for the FVS/FIS incorporates privacy measures. Document in Police Manual/related policies and procedures	