Privacy Impact Assessment – VicRoads participation in the National Driver Licence Facial Recognition Solution

For: VicRoads

Date: December 2018 - Commercial-in-Confidence

INFORMATION
INTEGRITY
SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Table of Contents

Glossary

Abbreviation or term	Expansion or definition
Austroads	Austroads Ltd
BAU	Business as usual
Data Holding Agency	Agency that contributes identity information used in the FMS to provide responses to queries from Requesting Agencies
DLIS	Drivers Licence Identification System
DLS	The Drivers Licence System
DPC	Department of Premier and Cabinet
DXC	VicRoads IT service provider for the NDLFRS project
FIS	Face Identification Service
FMS	Collective term for the Identity Matching Services that involve facial biometric matching including the FIS, the FVS and OPOLS
Framework administrator	The Commonwealth, or any replacement entity appointed by the Governing Body, administering the FMS Participation Framework
FRAUS	Facial Recognition Analysis Utility Service
FVS	Face Verification Service
Governance Framework	The NDLFRS Governance Framework for this PIA is taken to include the IGA and related agreements, policies and data sharing arrangements described in Appendix A
Governing Body	The National Identity Security Coordination Group, which, under the IGA, is accountable to the MCPEM for the efficient and effective delivery and management of the Identity Matching Services
HA	Department of Home Affairs (Cth) (formerly Attorney Generals Department – AGD)
IGA	Intergovernmental Agreement on Identity Matching Services
IIS	Information Integrity Solutions Pty Ltd
IPPs	Information Privacy Principles
MCPEM	The Ministerial Council for Police and Emergency Management, which under the IGA will exercise ministerial oversight of the Identity Matching Services.
NDLFRS	National Driver Licence Facial Recognition Solution
NFBMC	National Facial Biometric Matching Capability

Abbreviation or term	Expansion or definition
NISCG	The National Identity Security Coordination Group
OPOLS	One Person One Licence Service
OVIC	Office of the Victorian Information Commissioner
PA	Participation Agreement
PAA	Participant Access Arrangement
Participant	Participant means a party to the PA from time to time and any person who has agreed to become a party to this Agreement by executing the Deed of Accession. Participants include the Framework Administrator, Hub Controller (initially HA), Data Holding Agencies and Requesting Agencies
PDPA	*Privacy and Data Protection Act 2014* (Vic)
PIA	Privacy Impact Assessment
PRA	*Public Records Act 1973* (Vic)
Requesting Agency	Agency that submits a query to a Data Holding Agency, through the FMS
RSA	*Road Safety Act 1986* (Vic)
The Charter	*Charter of Human Rights and Responsibilities Act 2006* (Vic)
The Hub	Interoperability Hub
VPDSF	The Victorian Protective Data Security Framework established under Part 4 of the PDPA

1. Executive Summary

VicRoads engaged Information Integrity Solution Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) to help VicRoads in managing its privacy obligations when participating in the National Drivers Licence Facial Recognition Solution (NDLFRS).

The NDLFRS It will bring together driver licence images and biographic information from each of the states and territories in a system hosted by the Commonwealth. It will make driver licence facial images available to agencies participating the Face Matching Services (FMS) facilitated by the National Facial Recognition Solution (NFBMC).

VicRoads is now in the process of designing and building its solution and processes for the transfer of images and related information from its driver licence systems to the NDLFRS.

1.1 IIS's overall view – issues and risks

In undertaking the PIA IIS has considered the inherent privacy and security risks in the project, taking account in particular of VicRoads' obligations under the privacy principles. For this project, factors affecting inherent risk include:

- The involvement of biometric data, which is generally considered inherently sensitive
- The very large size of the dataset
- The fact that it covers a significant portion of the Victorian population
- The richness of the data (notwithstanding that VicRoads is only planning to upload the 'minimum dataset')
- The fact that the NFBMC, the FMS and the NDLFRS are still in the early stages of implementation with potential for as yet unknown privacy or security risks to arise.

IIS considers that VicRoads' participation in the NDLFRS has high inherent risks, but these are likely to be reasonably controlled. In making this assessment, IIS has taken account of:

- The NDLFRS governance framework, which VicRoads must work within, and which provides comprehensive, if high-level, requirements aimed at consistency and rigour in protecting privacy and security
- VicRoads' close involvement in the development of the NDLFRS governance framework where it has achieved changes including requirements to accommodate its legislative obligations and to ensure strong protections apply, even in jurisdictions without privacy law, by making the NDLFRS agreements legally binding
- VicRoads' approach to the project, which IIS observes to be systematic and thorough
- The project design, which builds in privacy and security features and which involves a fairly automatic process with limited room for human error or misuse of data
- The attention being paid to security assessment and monitoring

- Proposed testing of processes and willingness to hold off the bulk data upload if problems are identified.

IIS has not identified significant privacy gaps or risks. It has identified some areas where it considers priority attention is need or where additional steps are needed. These include:

- Monitoring the upload process and the use of VicRoads data in the FMS to identify and manage system or other errors
- Managing the data store and associated audit logs
- Considering the period for which data or audit logs should be retained
- Ensuring data breach response plans are in place and ready to go should there be breach during the bulk upload process.

IIS also considers that particular attention will be needed as the project is handed over to BAU. In this phase it will be critical to ensure processes are in place to identify and manage system issues that could affect privacy or security and to manage for risks including improper access to data, failure to identify impact on individuals or to manage privacy questions or issues, including because staff are not sufficiently aware of VicRoads' participation the NDLFRS or how to respond to privacy queries.

IIS has made 13 recommendations to address the issues identified.

1.2 Recommendations

Recommendation 1 – Monitoring NDLFRS bulk upload and daily updates to identify and manage accuracy issues

IIS recommends that VicRoads ensure it has in place a well-resourced error management process to identify accuracy issues as the NDLFRS implementation proceeds and until all processes, including the daily updates, are well established. The process should include specific 'caretaker' arrangements with HA.

Recommendation 2 – Minimising impact of NDLFRS data accuracy issues

IIS recommends that VicRoads make sure that where data accuracy issues are identified, it ensures it understands the impact on individuals, or particular groups of individuals, and take steps to minimise the impact. These steps could include system or process changes or providing more information or resources to assist individuals.

Recommendation 3 – Content and management of NDLFRS audit logs

IIS recommends that VicRoads ensure that its upload metadata and upload metadata audit logs, and Hub audit data provided to it from HA in relation to use of VicRoads data within the NDLFRS, contain only the minimum information needed to achieve their objectives. IIS also recommends that VicRoads implement all additional steps possible to minimise the risk of misuse; for example, if possible personal details and document details in VicRoads' audit logs should masked unless there is a specific and approved need to view these details.

IIS recommends that VicRoads develop a formal policy on the management of audit logs, including who can access the logs, for what purposes. There should then be systems in place to ensure that the policy is adhered to.

Recommendation 4 – Retention of upload metadata and upload metadata audit log

IIS recommends that VicRoads review its disposal schedules under the *Public Records Act 1973* to ensure there is a relevant schedule for the NDLFRS upload metadata and upload metadata audit log. If there is no applicable schedule, VicRoads should take steps to ensure there is one in place.

Recommendation 5 – Data breach plans ready for bulk upload

IIS recommends that VicRoads has a data breach response plan in place prior to the bulk upload, with relevant staff trained in it, so that there can be a swift response in the event that anything goes wrong.

Recommendation 6 – NDLFRS BAU governance

IIS recommends that VicRoads ensure that to the extent possible its NDLFRS BAU governance arrangements are in place before handover to BAU. The arrangements should include:

- A senior executive with carriage of the ongoing protection of privacy as VicRoads participates in the NDLFRS
- Documented policy and procedures for key aspects of VicRoads' NDLFRS participation, including its:
  - Service catalogue
  - Processes for approving PAAs
  - Processes for monitoring VicRoads' compliance with its privacy and NDLFRS governance requirements for NDLFRS participation
  - Processes for monitoring Requesting Agency compliance with the NDLFRS governance requirements and for ensuring VicRoads data is being used only for authorised purposes
- A formal process to consider and make decisions about expansions to VicRoads' NDLFRS participation
- Privacy issues, such as system issues with potential to affect privacy, privacy complaints or data breaches, included in risk management and performance monitoring processes and reports to Audit and Risk Committee.

Recommendation 7 – Process to approve PAAs

IIS recommends that VicRoads develop a formal process for approving PAAs from Requesting Agencies that includes:

- A Senior executive responsible
- Involvement of VicRoads experts on privacy, security and auditing
- Consideration of:
  - Any requirements arising from VicRoads' governing law

  - Overall consistency with the PDPA
  - The extent of ‘due diligence’ VicRoads would undertake in considering Requesting Agency material
  - Risk factors for the Requesting Agency
  - Whether and when, as permitted under the Participation Agreement, VicRoads should place additional requirements before granting access.

Recommendation 8 – Processes to manage PAAs, including review of compliance, audit reports

IIS recommends that VicRoads, particularly in first few years of NDLFRS participation, undertake a regular program to review each of its PAAs. Matters that VicRoads should particularly check for when reviewing annual audits include:

- The seriousness of any breaches or non-compliance
- Any instances of ‘repeat offences’ where a Requesting Agency has breached the PAA or its privacy and security obligations in the same way for a second year running
- Evidence of implementation of audit recommendations or a plan for implementation
- Any indication that Requesting Agency actions may cause VicRoads to, itself, breach a law
- Ongoing liaison with the NDLFRS governing body to ensure VicRoads has a good understanding of any issues arising in the system overall or with respect to particular Requesting Agencies.

Recommendation 9 – Collection notices

IIS supports VicRoads intention to amend its privacy statements to advise of use and disclosure of personal information for biometric facial matching.

IIS recommends that VicRoads undertake research to test its proposed statements to assess the extent to which they help make individuals aware of use and disclosure of personal information for biometric facial matching and to identify what additional information might be needed. VicRoads should also consider how to make such additional information readily available at the point at which personal information is collected.

Recommendation 10 – image quality and impact on customers

IIS recommends that VicRoads actively monitor its NDLFRS activities, including error reports, trends in the success or otherwise of the bulk and daily uploads and reports from the governing body and other road agencies, so that it is well informed on any data accuracy or image quality issues that are coming to light. In particular, VicRoads should watch and manage for any undue negative impact on individuals or groups of individuals, for example, matching difficulties involving VicRoads data leading to increased need to attend service centre to resolve issues.

IIS also recommends that VicRoads ensure it has in place procedures to that it can respond quickly to requests for access or to correct information. VicRoads should also establish clear communication channels with other road agencies to facilitate the resolution of accuracy issues or access or correction requests involving more than one jurisdiction.

Recommendation 11 – Staff awareness of VicRoads NDLFRS obligations and procedures

IIS recommends that VicRoads take steps to ensure its frontline staff are aware of VicRoads' role in the NDLFRS and know how to support customers who ask questions, seek access or correction or have been referred to a service centre because of a match failure.

Recommendation 12 – Data breach management and notification

IIS recommends that before VicRoads goes live with NDLFRS participation it should review its current data breach and incident management processes to ensure they:

- Meet the Hosting Agreement and OVIC requirements
- Have been tested with realistic scenarios to ensure they work appropriately for the NDLFRS. Testing should assess matter such as:
    - Roles and responsibilities
    - Decision making and speed of response
    - Notification processes
    - Communications.

Recommendation 13 – Transparency and public communications about the NDLFRS

IIS supports VicRoads intention to amend its privacy policy to provide information about its participation in the NDLFRS and about the FMS.

IIS recommends that VicRoads make its website privacy information more prominent and more easily discoverable.

IIS also recommends that, subject to steps taken by HA, VicRoads assess if additional community awareness activities are needed to ensure transparency.

2. Introduction

The Victorian Government is a signatory to the *Intergovernmental Agreement on Identity Matching Services* (IGA) that sets the framework enabling:

- State and territory participation in the Face Matching Services (FMS) facilitated by the National Facial Biometric Matching Capability (NFBMC)
- The establishment of the NDLFRS.

The NDLFRS will bring together driver licence images and biographic information from each of the states and territories, in a system hosted by the Commonwealth. It will make driver licence facial images available to agencies participating in the FMS.

An overview of the NFBMC, the FMS and the governance arrangements for the NDLFRS is at Appendix A.

VicRoads is now in the process of designing and building its systems and processes for the transfer of images and related information from its driver licence systems to the NDLFRS. The purpose of this PIA is to assist VicRoads in managing its privacy obligations in relation to its initial participation in the NDLFRS.

2.1 Scope

The PIA is focussed on VicRoads' role as a Data Holding agency, rather than as a Requesting Agency/user of the NDLFRS. VicRoads has specifically identified that it is not currently considering as part of its solution:

- Resolution of existing risks and issues (technical and operational) that have gained focus or been reinforced with the NDLFRS Project (e.g. data quality/integrity/cleansing)
- VicRoads designing the systems architecture, or making systems-related changes, that will assist future use of the facial image data and technology
- Agencies seeking access to VicRoads data for facial recognition aside from Law enforcement or road transport agencies.

These activities could be considered once VicRoads has bedded down its role as a Data Holding agency.

VicRoads asked for the PIA to cover the privacy considerations of the project, including specific analysis of:

- Upload process of VicRoads data to the NDLFRS, including an assessment of the physical transfer and attendant security
- Auditing of Requesting Agencies' use of VicRoads data
- VicRoads staff access to the Face Matching Services
- VicRoads internal process of approving template Participation Access Arrangements from Requesting Agencies

- VicRoads current privacy policy
- Process for access and correction of Victorian driver licence data held in the NDLFRS
- Security classification differences between VicRoads database and the NDLFRS
- Impact of data quality of VicRoads licence photos on the operation of the NDLFRS.

It was out of scope for the PIA to cover information flows already assessed, or being assessed, in other PIAs related to VicRoads participation the NDLFRS. These are:

- The Commonwealth commissioned PIA on the NDLFRS – finalised November 2017
- The Austroads PIA – Road Agencies' use of the NDLFRS – commenced in March 2018 and soon to be finalised.[1]

The PIA considered possible security or technical issues for the solution, but it was also out of scope for IIS to undertake detailed investigations or reviews of the solution's technical or security features.

2.2 Methodology

Following a planning phase where IIS confirmed its PIA approach with VicRoads, IIS carried out its work by:

- Gathering information by reading documents (see Appendix B) and meeting with VicRoads staff
- Analysing the information against Victoria's privacy legislation, in particular the IPPs in the PDPA, the more specific security requirements in Part 4 of the PDPA, the Charter, broader privacy issues and analysing privacy implications in the specific matters listed in Section 2.1
- Drafting a PIA report and allowing VicRoads staff to comment on the report
- Addressing VicRoads staff feedback and finalising the report.

The advice in this report is intended as strategic privacy advice. IIS does not provide legal advice.

[1] IIS was engaged to conduct both of these PIAs. The reports are not yet in the public domain but are expected to be published in the future.

3. About the project

VicRoads holds drivers licence information in two systems, which are managed on its behalf by its service provider DXC. The systems are:

- The Drivers Licence System (DLS), which holds biographic information
- The Drivers Licence Identification System (DLIS), which holds biometric information including face images.

These systems will not change in this project.

VicRoads will bulk upload 15 years' worth of DLS and DLIS data to the NDLFRS. This period will cover currently issued licences and a margin to allow for assessments of image quality.

The data transferred to the NDLFRS will be a mirror copy of the data held in the DLS and DLIS. Following the bulk data upload, VicRoads will move to business as usual (BAU) upkeep of its NDLFRS data, with daily updates to allow corrections and changes arising from everyday transactions (such as address updates).

On the current schedule, VicRoads' bulk upload is expected to occur in April 2019. During May and June 2019, law enforcement will conduct sanitisation works on the data (to protect legally assumed identities). From July 2019, the data will be fully functional in NDLFRS and VicRoads will begin accepting applications from 'Requesting Agencies' to access VicRoads data via the FMS.

VicRoads has told IIS that they will do the bulk upload by secure FTP while the daily updates will occur by XML file via TLS encryption.

3.1 Relevant legislation

VicRoads participation in the NDLFRS will be subject to its legislative obligations in the following:

- *Privacy and Data Protection Act 2014* (Vic) (PDPA), in particular the Information Privacy Principles (IPPs) and the Protective Data Security requirements in Part 4 of the PDPA
- *Public Records Act 1973* (Vic) (PRA)
- *Road Safety Act 1986* (Vic) (RSA)
- *The Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter).

3.2 Types of personal information involved

VicRoads will be disclosing personal information to the NDLFRS under its existing powers in the RSA.[2] This limits the information VicRoads will be able to disclose and the organisations which it would permit to access Victorian data via the FMS. At this point VicRoads is not authorised under the

[2] The RSA: Part 7B regulates use and disclosure of information; s 90K(a)(vi) allows disclosure in relation to an intergovernmental agreement; s 90K(g) allows disclosure for law enforcement purposes.

IGA to provide, for example, information from maritime licences, working with children cards or firearm cards to the NDLFRS.

VicRoads will be providing facial images and biographic data of a person with at least one of a road or motor bike licence or a learner permit. The biographic data to be provided is the specified minimum data set for participation in the NDLFRS and is as follows:

- Licence number (Customer_ID)
- Date of birth
- Alive or deceased
- Last name
- First name
- Gender (including undetermined)
- Address
- Suburb
- State
- Postcode
- Country
- Licence code (for example, learner, full etc).

IIS notes that the information provided will include the licence number field. IIS understands that driver licence numbers are important within the NDLFRS for two reasons:

- They allow VicRoads to identify with certainty records which have been replicated and transferred to the Commonwealth for the NDLFRS. For example, if a record needs to be deleted at a future date because it has been identified as duplicate or fraudulent, the licence number will allow VicRoads and the Commonwealth to identify the correct record with certainty.
- They will assist in achieving one of the purposes of the FVS, which is to prevent and detect identity crime. If a person seeks to (fraudulently) verify their identity with the licence of another person onto which they have added their own photograph, the FVS will not return a match because the licence number will not match that person’s photograph.

VicRoads has a lawful basis for disclosing information to the NDLRS under s 90K(a)(vi) of the RSA.

3.3 Project design and information flows

DXC will be building the solution that will extract and process images and transfer them to the NDLFRS (hosted and operated by the Department of Home Affairs (HA)). The bulk upload will be a once-off activity. Subsequent uploads are part of the daily update process.

The process will include qualification rules that will interrogate the DLS and DLIS once a day looking for three types of transactions:

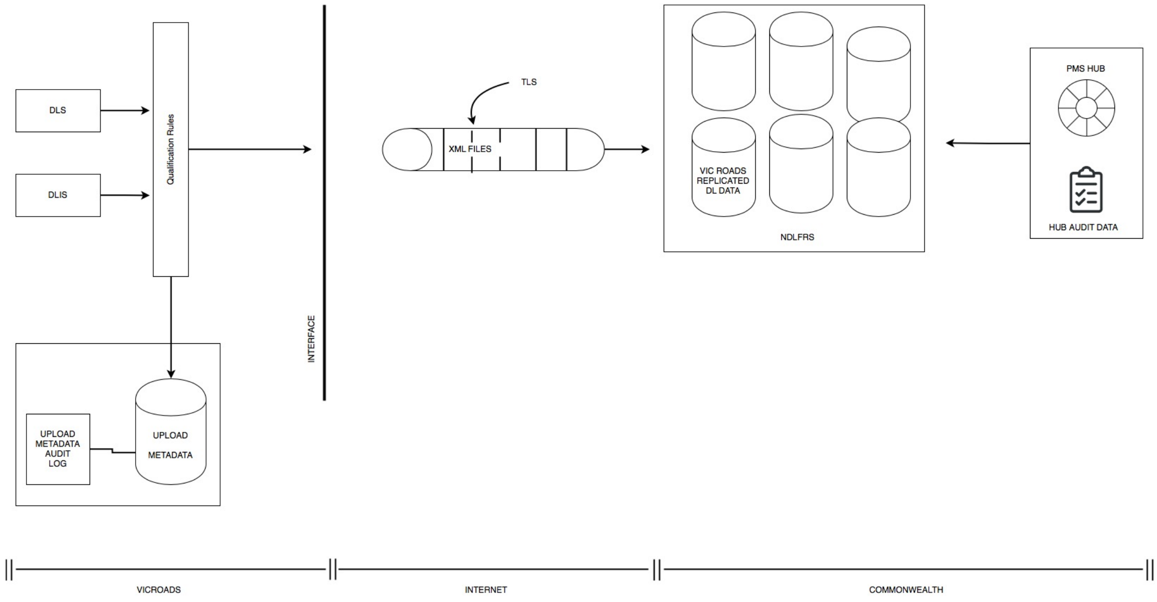
- New records for inclusion – this may be a brand-new record, or it could be an existing record that was not included, but something has changed that makes it now includable
- Changed records – for example, an address or name change
- Records for exclusion – for example, a record is discovered to be fraudulent and is reversed out of the NDLFRS.

The VicRoads Driver Licence Image System contains current and historical images, and data associated with these images. Where a record meets the above qualification criteria, only the most recent facial image, defined by the system, and data associated to this image, is required to be included in the transaction. This will ensure that:

- A record can have no more than one facial image attached to it
- Only the most recent Person details are included
- Only one transaction is generated for each Permit/Licence Number for loading into the NDLFRS databases.

Figure 1 below provides an overview of the existing DLS and DLIS (in black in the diagram) and the solution to extract and process the data and transfer it to the NDLFRS (in blue).

Figure 1: NDLFRS bulk and incremental upload process



At this stage, VicRoads intends to keep metadata about the records uploaded (**upload metadata**), which will include:

- Biographic information as outlined above
- Document information, including document IDs and type
- VicRoads identifiers and record details

- Information about the image, for example compression algorithm used when capturing the image, time/date of the image capture, location of the image capture, the unique identifier for the image and coordinates for aspects of the image, but not the image itself
- Details of transactions that qualify for processing (regardless of whether the transaction was then sent for processing) and the outcome of processing
- Transactions times, dates and status
- Data returned from HA that defines the outcome of HA receiving and processing the transaction.

VicRoads advises the upload metadata is needed for NDLFRS data synchronisation, investigation, and auditing purposes. Other than automated services, this data store will have strict access controls and will only be available for VicRoads' or other NDLFRS participants' investigation purposes.

The upload metadata will be accessible only to specified VicRoads staff, with access provided by user ID and password on a view only basis for. There will be an audit log which will identify:

- Staff that have accessed the upload metadata, by User ID
- Reports that have been generated by staff using the upload metadata
- Changes made by staff when using the upload metadata, such as requesting a Refresh transaction.

VicRoads notes that, separately, the Commonwealth is in the process of building an audit log system in relation to Requesting Agencies' use of Data Holding Agencies' data with the Face Matching Services (**Hub audit data**). This will assist VicRoads to be satisfied that use of Victorian data is in accordance with Participant Access Arrangements with Requesting Agencies.

3.3.1 Privacy and security features

Privacy and security features that have been designed into the solution and into VicRoads' processes include:

- A 'security be design' approach, and advice and assessments from security specialists to ensure the solution meets security standards for participation in the NDLFRS and to identify the potential for compromise of VicRoads systems
- Images are assessed on enrolment to ensure they meet quality thresholds; only successfully validated images are uploaded
- The system is designed one-directionally – data can only be updated in the DLS and DLIS, with updates then fed up into the NDLFRS. No updates occur in the other direction. That is, the NDLFRS cannot be updated directly with those changes flowing backwards to the DLS and DLIS
- VicRoads will be uploading only the minimum data needed to meet HA's specifications and VicRoads requirement – the dataset being uploaded will not include the current status of the card, that is whether the card is valid or not, or (apart from image testing) data about the location at which the image was taken

- The NDLFRS only stores the current image (plus a backup of the previous image in an archive); VicRoads notes it will not be using the backup of the previous image stored in the NDLFRS
- System tests will involve the minimum data possible, for example when testing images, the images will be submitted with only a small amount of metadata (including location data)
- The processes will be largely automated with limited human interaction other than testing and resolving issues.

3.3.2 Next steps in the project

VicRoads is well advanced with its system design and development.

Its next steps will include testing 6000 images to identify trends where images do not satisfy the quality provisions (possibly because of local conditions, nature of camera, age of the images etc). If a large percentage of images fail VicRoads advises it would need to reassess whether they should test a larger batch (>6000) or indeed consider whether participation is feasible at all. However, based on similar tests in Tasmania, which resulted in a 95% match rate, VicRoads is confident its results will be the same or better.

Other aspects of the project which will be dealt with prior to the bulk load include:

- Developing processes to manage Customer Enquiries
- NDLFRS Driver Licence Enrolment (automated)
- Systems Management (IT Support)
- Annual Audit and Compliance Statement process
- Incident Management and Escalation Processes
- NDLFRS Service Management
- VicRoads NDLFRS product catalogue services governance and maintenance
- NDLFRS VicRoads Governance.

.

4. Key privacy issues and recommendations

4.1 IIS approach to risk assessment

Victoria has already agreed to participate in the NDLFRS and has signed the IGA. As expected under the IGA, VicRoads is approaching the NDLFRS with the intention of sharing its data to the greatest extent possible, consistent with the IGA However it is also mindful of its obligations under privacy law and the Charter to protect personal information and privacy, including from unlawful or arbitrary interference with privacy.

In undertaking the PIA IIS has considered the inherent privacy and security risks in the project, taking account in particular VicRoads' obligations under IPP 4 which requires it to take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure. What is 'reasonable' usually depends on the data and the circumstances. In this case, those reasonable steps will need to be comprehensive and rigorous given:

- The involvement of biometric data, which is generally considered inherently sensitive
- The very large size of the dataset
- The fact that it covers a significant portion of the Victorian population
- The richness of the data (notwithstanding that VicRoads is only planning to upload the 'minimum dataset')
- The fact that the NFBMC, the FMS and the NDLFRS are still in the early stages of implementation with potential for as yet unknown privacy or security risks to arise.

4.2 IIS's overall opinion

IIS considers that the VicRoads' participation in the NDLFRS has high inherent risks but these are likely to be reasonably controlled. In making this assessment, IIS has taken account of:

- The NDLFRS governance framework, which VicRoads must work within, and which provides comprehensive, if high-level, requirements aimed at consistency and rigour in protecting privacy and security
- VicRoads' close involvement in the development of the NDLFRS governance framework where it has achieved changes including requirements to accommodate its legislative obligations and to ensure strong protections apply, even in jurisdictions without privacy law, by making the NDLFRS agreements legally binding
- VicRoads' approach to the project, which IIS observes to be systematic and thorough
- The Project design, which as noted above, builds in privacy and security features and which involves a fairly automatic process with limited room for human error or misuse of data
- The attention being paid to security design and assessment
- Proposed testing processes and willingness to hold off the bulk data upload if problems are identified.

IIS has not identified significant privacy gaps or risks. It has identified some areas where it considers priority attention is need or where additional steps are needed. IIS also considers that particular attention will be needed as the project is handed over to BAU. The issues identified are discussed below.

4.3 Design and build – privacy and security considerations for data upload to the NDLFRS

The issues discussed here have been identified following a high-level assessment against the IPPs at Appendix C or they cover broader issues that IIS has identified or on which VicRoads has requested specific advice.

4.3.1 IPP 3 – accuracy and data quality

IPP 3 requires agencies to take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

In discussions, VicRoads noted that its existing DLS and DLIS may have a range of data accuracy and quality issues. These could involve duplicate licences or incorrect biographical details resulting from process or data entry issues or fraud. VicRoads has commenced scoping a piece of work to assess data quality in the DLS and DLIS and will develop a data quality improvement plan if required. It is out of scope for this PIA to consider this aspect of the accuracy of VicRoads data. VicRoads emphasised in its discussions with IIS that the NDLFRS overall is being built on the understanding that state and territory data will be submitted as is; there is no expectation that the data will be cleansed before upload. Rather, the expectation is road agencies will continue to work on data accuracy and that FMS services, such as the One Person One Licence Service (OPOLS) and the Facial Recognition Analysis Utility Service (FRAUS) will, over time, help improve the quality of road agency data. Whether the project could still compound the impact of inaccurate on individuals is considered further at Section 4.4.2.2.

The focus here is on image quality and on the importance of having a watching brief as the solution is implemented to understand and deal with the impact of these issues. In this regard, VicRoads asked IIS to consider the impact of data quality of VicRoads photos on the NDLFRS.

IIS notes that data accuracy has been a consideration in the design and development of the NDLFRS solution. For example, the Functional Specification for the solution includes amongst its objectives 'Review & maintain quality in the way biometric and biographic details are managed by VicRoads'.

In this regard, as noted in Section 3.3.2 above, VicRoads will soon begin testing of 6000 images to ensure they can be uploaded to the systems and can be used effectively in facial recognition systems. Knowingly incorrect records won't be shared.

Subject to the image quality testing, VicRoads will be proceeding with the implementation of the bulk upload and then daily update processes. It does not expect huge volumes of problems in the upload process; Victoria is the 2nd cab off the rank and expects that problems would be identified and resolved as Tasmania uploads its data. However, it is considering implementing a caretaker period with HA to make sure any issues in its bulk upload, or daily increments, are identified early and dealt with.

VicRoads does not anticipate that the NDLFRS process will affect individuals' ability to deal with data accuracy problems if they arise but it appreciates there should be an approach ready to go to assist individuals in case there are issues.

IIS considers that in the circumstances VicRoads is taking reasonable steps with respect to data quality and accuracy in its project implementation.

However, IIS also considers that there should be a strong and continued focus on monitoring accuracy or other errors until the bulk upload is complete and daily update is established. IIS supports the idea of a caretaker period. It also considers VicRoads should make sure there are procedures and resources available to assist individuals unduly affected by the NDLFRS implementation. IIS discusses this issue further in Section 4.3.2.2 below.

Recommendation 1 – Monitoring NDLFRS bulk upload and daily updates to identify and manage accuracy issues

IIS recommends that VicRoads ensure it has in place a well-resourced error management process to identify accuracy issues as the NDLFRS implementation proceeds and until all processes, including the daily updates, are well established. The process should include specific 'caretaker' arrangements with HA.

Recommendation 2 – Minimising impact of NDLFRS data accuracy issues

IIS recommends that VicRoads make sure that where data accuracy issues are identified, it ensures it understands the impact on individuals, or particular groups of individuals, and take steps to minimise the impact. These steps could include system or process changes or providing more information or resources to assist individuals.

4.3.2 IPP 4 and Part 4 of the PDPA – security issues

VicRoads is obligated to consider the privacy and security safeguards for the bulk upload and the daily updates.

Aside from the security obligations in the FMS Participation Agreement and policy documents, VicRoads also has security obligations under IPP 4. These, as noted earlier, require it to take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure. What is 'reasonable' usually depends on the data and the circumstances. VicRoads also has obligations under Part 4 of the PDPA. The 2016 Victorian Protective Data Security Framework (VPDSS) established under this part provides direction to Victorian public sector agencies or bodies on their data security obligations.

VicRoads is engaging a specialist information security firm to ensure that its implementation of the NDLFRS solution meets these obligations and the Commonwealth's compliance requirements and to ascertain the extent the supporting VicRoads NDLFRS system environment and associated internet facing infrastructure and information are susceptible to compromise.

It is envisaged that the security assessment will cover the following topics:

- Management practices review of the operation of the proposed solution
- Review of processes to support access control and privilege user management
- Risk assessment of proposed solution and mitigation controls/strategies
- VicRoads integration solution security architecture/design review
- Penetration testing of the VicRoads integration solution (align to Industry standards such as NIST 800-115, OWASP)
- Reporting and risk rating (use VicRoads risk matrix)
- VicRoads integration solution Information Security Manual (ISM) compliance review
- Development of RACI matrix (between AGD and VicRoads)[3]
- Development of RACI (between VicRoads and DXC)
- Review security artefacts delivered by the Commonwealth.

From its review of the material provided it appears to IIS that the security aspects of the project are being given due consideration. IIS has not identified specific additional actions.

VicRoads asked IIS to consider whether security classification differences between VicRoads database and the NDLFRS would have implications from a privacy perspective.

IIS understands that the Commonwealth's environment is certified to PROTECTED level with accreditation issued to Unclassified DLM of Sensitive: Personal. VicRoads' records for NDLFRS, as a whole, are classified as CONFIDENTIAL. However, the CONFIDENTIAL classification is due to a small number of records, which VicRoads manage at the direction of Law Enforcement Agencies. Subsets of the whole data are classified as PROTECTED. Those small number of records will be separately managed by the relevant Law Enforcement Agencies and Home Affairs within the NDLFRS, allowing the remaining records to exist within the Commonwealth's PROTECTED environment.

Based on the information provided, IIS considers the approach is reasonable and there does not appear to be undue impact in a change to the named security classification.

4.3.2.1 Upload metadata

VicRoads will be keeping detailed records of information provided to the NDLFRS and advice from HA about the success or otherwise of the records uploaded. As outlined at Section 3.3 above, the upload metadata will include all biographic details uploaded, document details, information about the image

[3] Matrix mapping out every task, milestone or key decision involved in completing a project and assigns which roles are Responsible for each action item, which personnel are Accountable, and, where appropriate, who needs to be Consulted or Informed.

(but not the image itself) and associated metadata (time, date of transactions, etc). Both the bulk upload and the daily updates will be largely automated, with no human interactions needed. However, some VicRoads' staff will have view-only access to the system to help resolve issues and facilitate audits and investigations. There will be an audit log of access to the upload metadata (**upload metadata audit log**), so that the following information can be retrieved:

- Staff that have accessed the facial imaging data store, by User ID
- Reports that have been generated by staff using the data store
- Changes made by staff when using the data store, such as requesting a Refresh transaction.

VicRoads asked IIS to consider if there were any particular types of data included in the upload metadata that would raise particular privacy risks.

As far as IIS understands, the content of the audit logs of staff accesses is fairly limited and the information included has the clear purpose of having a record of staff actions in relation to the data store. Nevertheless, there should be clear documentation on the nature and purpose of the audit logs and how they will be managed and used. If possible, the logs should be capable of being regularly reviewed, or of producing reports flagging unusual behaviour.

The upload metadata itself does appear to carry more risks. It contains quite detailed information, including biographic information although no biometric information as such. If, as IIS understands, the information in the upload metadata could be retained for long periods, IIS considers that VicRoads should take additional steps to minimise the risk of misuse; for example, could personal details and document details be masked unless there is a specific and approved need to view these details. In any event, there should be detailed documentation on how the information in the data store can be used and how its use will be managed and monitored.

The hub audit logs could be more problematic. IIS understands these logs would not contain personal information or enough information to allow a person to be identified or for transactions about a person to be re-created from the audit logs alone. However, there should be clear documentation on how the Hub audit data can be used – are they a passive source to assist in investigations of possible misbehaviour or misuse of data by staff from other agencies, or, a tool that VicRoads should monitor as part of 'being in control' of its NDLFRS data. There should also be clear policies on who can access the Hub audit data for what purposes and processes to ensure rules are adhered to.

4.3.2.2 Data retention

IPP 4 provides that information that is no longer required for any purpose must be deleted or de-identified. IIS understands that at this point VicRoads has not considered data retention periods for either the data store or audit logs. IIS also understands that VicRoads is inclined to keep the upload metadata for a long period, possibly permanently, because data will be stored in the NDLFRS for long periods.

VicRoads noted that there is likely to be a PRA destruction schedule that would apply and will be following up on this. It acknowledges that holding data when it is no longer needed increases the risk of misuse or breach and that appropriate retention periods and an applicable destruction schedule should be in place.

4.3.2.3 Data breach management

In discussions, VicRoads noted that there it has incident management procedures, including data breach procedures, which it presumes would apply to the NDLFRS solution, but these have not been reviewed for the project. IIS consider this should be undertaken; there is for significant potential for damage to VicRoads' reputation as well as harm to individuals if things go wrong, particularly for the bulk upload. IIS also encourages VicRoads to ensure the procedures are relevant to the NDLFRS context and that they work in practice.

Recommendation 3 – Content and management of NDLFRS audit logs

IIS recommends that VicRoads ensure that its upload metadata and upload metadata audit logs, and Hub audit data provided to it from HA in relation to use of VicRoads data within the NDLFRS, contain only the minimum information needed to achieve their objectives. IIS also recommends that VicRoads implement all additional steps possible to minimise the risk of misuse; for example, if possible personal details and document details in VicRoads' audit logs should masked unless there is a specific and approved need to view these details.

IIS recommends that VicRoads develop a formal policy on the management of audit logs, including who can access the logs, for what purposes. There should then be systems in place to ensure that the policy is adhered to.

Recommendation 4 – Retention of upload metadata and upload metadata audit log

IIS recommends that VicRoads review its disposal schedules under the *Public Records Act 1973* to ensure there is a relevant schedule for the NDLFRS upload metadata and upload metadata audit log. If there is no applicable schedule, VicRoads should take steps to ensure there is one in place.

Recommendation 5 – Data breach plans ready for bulk upload

IIS recommends that VicRoads has a data breach response plan in place prior to the bulk upload, with relevant staff trained in it, so that there can be a swift response in the event that anything goes wrong.

4.4 NDLFRS participation – BAU including governance

The issues discussed here have been identified following a high-level assessment against the IPPs at Appendix C or they cover broader issues that IIS has identified or on which VicRoads has requested specific advice.

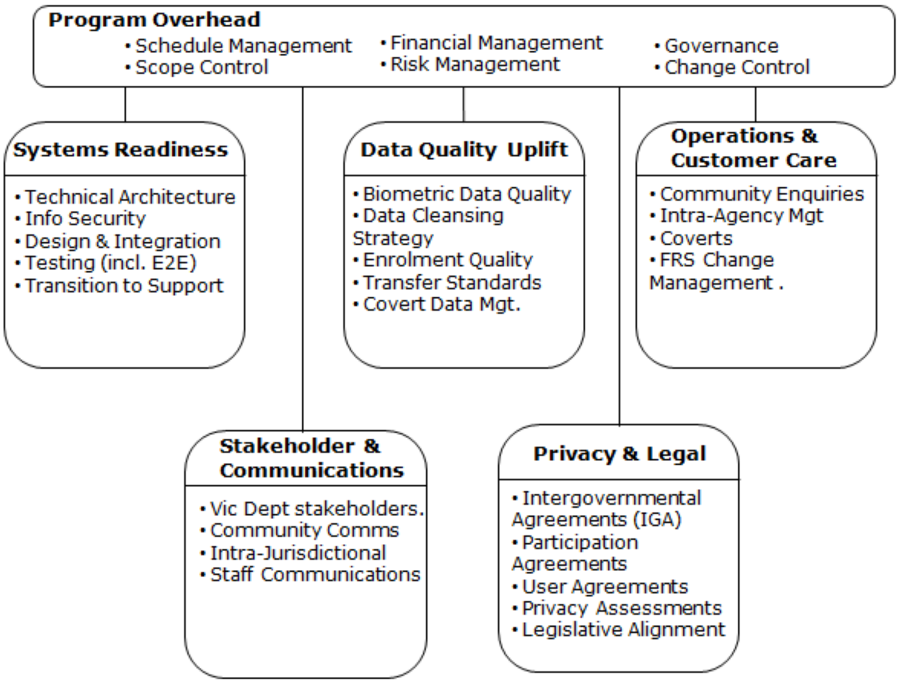
4.4.1 BAU governance

The VicRoads NDLFRS Functional Specifications anticipate that VicRoads will:

- Create business readiness for launch of the NDLFRS Project by creating awareness of what the project is, what it means, and what impacts it will have on the business.
- Prepare for handover to BAU by consulting existing operational teams either directly or indirectly impacted by the NDLFRS Project, assist with determining the level of impact, and ensure the required level of knowledge and resource is available to minimise impact of the NDLFRS Project on current support operations and SLAs.

For project phase, governance has involved:

- Face Matching Service Policy and Legal Working Group and Face Matching Services Advisory Board (both chaired by Commonwealth
- Joint Steering Committee (monthly meeting) of senior executives from VicRoads, the Department of Premier and Cabinet (DPC), the Department of Justice and Victoria Police
- Project Authority (sponsor, legal, policy, customer operations centre, IT) – Director level (monthly meeting)
- Program management as outlined in the following diagram



VicRoads has also established a Policy & legal Working Group with the DPC to ensure the solution and ongoing implementation is informed by DPC's policy thinking and guidance. The group will include representatives from the Department of Justice and Regulation, Victoria Police, Department of Premier and Cabinet and, Service Victoria. VicRoads will also participate in a new group being created by HA – the Business Technical Working Group. This group will provide a forum to discuss operational matters such as biometric template thresholds and match thresholds (how they are set and what levels they are set).

VicRoads' advised that BAU governance has still to be set up. IIS considers the arrangements should be in place to the extent possible before handover to BAU. In the course of this PIA IIS has identified areas which it considers would assist VicRoads to continue its proactive approach to privacy for its participation in the NDLFRS. These are outlined in the following recommendation.

Recommendation 6 – NDLFRS BAU governance

IIS recommends that VicRoads ensure that to the extent possible its NDLFRS BAU governance arrangements are in place before handover to BAU. The arrangements should include:

- A senior executive with carriage of the ongoing protection of privacy as VicRoads participates in the NDLFRS
- Documented policy and procedures for key aspects of VicRoads' NDLFRS participation, including its:
    - Service catalogue
    - Processes for approving PAAs
    - Processes for monitoring VicRoads' compliance with its privacy and NDLFRS governance requirements for NDLFRS participation
    - Processes for monitoring Requesting Agency compliance with the NDLFRS governance requirements and for ensuring VicRoads data is being used only for authorised purposes
- A formal process to consider and make decisions about expansions to VicRoads' NDLFRS participation
- Privacy issues, such as system issues with potential to affect privacy, privacy complaints or data breaches, included in risk management and performance monitoring processes and reports to Audit and Risk committee.

4.4.1.1 Approving Participant Access Arrangements

VicRoads NDLFRS Functional Specification includes amongst its objectives 'Maintain control on access to the Face Verification Servicer (FVS) and Face Identification Service (FIS), for use by Inter-agency products and services'.[4]

The PAAs, which form part of the FMS Participation Agreement, are a key mechanism to ensure NDLFRS participants are in control of their data. PAAs are made between the Hub Controller, a Requesting Agency and one or more Data Holding Agencies. Their purpose is to set out the level of services being offered or requested and the way in which an agency will access the service via a 'Service Catalogue'.

[4] The FIS (Face Identification Service) and FVS (Face Verification Service) are described in Appendix A

An Agency's Service Catalogue could, for example, provide a full service for FIS but might limit FVS responses to a basic match/no-match (yes/no) response and not return associated biographical data.

At this point in the development of the FMS there is a limited set of agencies that can request access. VicRoads anticipates there would be a maximum of 20 agencies submitting PAAs requesting access to its data. Initial participants are likely to be law enforcement agencies and road agencies.

The Participation Agreement sets out matters including for privacy and security which Requesting Agencies must have in place. The requirements include having a privacy governance framework and undertaking or participating in a PIA for the information flows (see Appendix A for a more detailed overview of the requirements).

<u>VicRoads approach to approving PAA templates</u>

VicRoads indicates it will be setting up a process to approve PAA Templates. VicRoads will use its process as the starting point when deciding whether to support a Requesting Agency's request for access. It intends to create a form that appropriately skilled staff can use when they assess PAAs when they come in. It anticipates a 'user friendly' checklist, informed by legal advice, on relevant considerations to take into account.

VicRoads' initial thinking on an appropriate PAA approval process is that it is likely to include:

- A case-by-case assessment and decision under its BAU governance arrangement – VicRoads would not, as is possible under the Participation Agreement, be delegating approval of PAAs to HA as the Hosting Agency
- Restricting the Requesting Agency from using the data for purposes that VicRoads would not want them to use it for.

<u>Factors VicRoads could consider in formalising its PAA approval approach</u>

IIS has identified the following questions as raising relevant considerations for the approval process and provides initial views on how these could be reflected.

Any requirements arising from VicRoads' governing law

- VicRoads notes that it is limited to certain uses of the data by its existing legislative authority which includes permitting disclosure in relation to an intergovernmental agreement. Under current arrangements, VicRoads cannot approve requests from organisations not encompassed in the current IGA, for example, local councils, or to allow approved Requesting Agencies to pass information to third parties outside of the IGA[5]
- Any other limiting factors should be identified and reflected in the PAA approval process.

Any specific obligations in the PDPA

- VicRoads disclosures to the NDLFRS will already be 'authorised by law' under the RSA and therefore consistent with IPP 2. IPP 9 would come into play as VicRoads will be transferring

[5] RSA s 90K(a)(vi) allows disclosure in relation to an intergovernmental agreement

information outside of Victoria. As noted in Appendix C it's likely that the NDLFRS governance framework would mean that information transferred would be protected in ways that are substantially similar to the PDPA protections.

- While not identifying specific IPP obligations that would need to be checked off, IIS considers it would be consistent with the spirit of the IPPs for VicRoads to be satisfied that its data is used only for authorised purposes and that it will be protected by appropriate privacy and security safeguards.

The extent of 'due diligence' VicRoads should undertake in considering Requesting Agency material

- The question here is can VicRoads rely on a Requesting Agency's assurances that policies or processes are in place or should it seek copies of relevant documents and review them and or should it seek additional assurance or evidence.
- IIS considers that a reasonable level of active review, at least for an initial set of PAAs, would be more consistent with VicRoads' overall obligations under the PDPA to protect Personal information. The fact that the material is available could also leave VicRoads open to criticism if something goes wrong and there was no review in the PAA process. IIS suggests VicRoads build its check list taking account of matters in the Participation Agreements, as listed in Appendix B, and also the Compliance Statement that is included in the PAA template (Appendix E to the template). Where the requirements involve documents, VicRoads should seek copies of, and review the documents. Preferably such review would be undertaken by experienced staff who could identify gaps or possible inconsistencies with VicRoads' expectations.

Risk assessment

- IIS considers it would be worth identifying factors that could mean a Requesting Agency should be subject to additional scrutiny or conditions. Such factors could include:
    - Nature of agency, its size and experience with face matching
    - Whether disclosures to third parties are contemplated
    - Whether the Agency is new to the FMS and has not yet prepared compliance statements or been subject to audits
    - Significant past data breaches
    - The conditions under which, if at all, VicRoads would be willing to agree to a non-independent auditor
    - That the agency is from a jurisdiction that does not have a formal privacy law.

Whether and when, as permitted under the Participation Agreement, VicRoads should place additional requirements before granting access.

- IIS in discussions with VicRoads has not identified specific circumstances when VicRoads would seek to impose additional requirements. These might come out of VicRoads' review of material supporting a PAA or an assessment that there are particular risk factors for the Requesting Agency.

Other points to consider

In addition to the points outlined above, IIS suggests that a sound PAA approach would be characterised by:

- Documenting the approach into a formal policy and set of procedures
- Senior staff member to approve PAAs
- The involvement of relevant VicRoads experts, for example, in privacy, security or auditing.

Recommendation 7 – Process to approve PAAs

IIS recommends that VicRoads develop a formal process for approving PAAs from Requesting Agencies that includes:

- A Senior executive responsible
- Involvement of VicRoads experts on privacy, security and auditing
- Consideration of:
  - Any requirements arising from VicRoads' governing law
  - Overall consistency with the PDPA
  - The extent of 'due diligence' VicRoads would undertake in considering Requesting Agency material
  - Risk factors for the Requesting Agency
  - Whether and when, as permitted under the Participation Agreement, VicRoads should place additional requirements before granting access.

4.4.1.2 Ensuring Requesting Agencies' use VicRoads data appropriately

VicRoads is also considering the steps it might take to satisfy itself that its data is being used properly by Requesting Agencies.

In addition, as set out in Appendix A, the Participation Agreement has built in a level of assurance, which includes requirements for participants to undertake annual audits and prepare annual compliance statements within specific timeframes. The NDLFRS governance framework also provides for governing body oversight. This includes reviews of compliance statements, audits, data breaches and privacy complaints to identify the need for remedial action. This might involve truncating or removing a participant's access to the NDLFRS or to the FMS.

The draft FMS Compliance Policy states that decisions to modify, suspend, or terminate a Requesting Agency's access to the FMS for non-compliance are matters for the Governing Body.[6] This indicates that, while Data Holding Agencies (like VicRoads) have the power to direct the Commonwealth to

[6] See paragraph 4.1, *Compliance Policy – Face Matching Services – Draft version 1.7.*

suspend a Requesting Agency's access rights, generally, it will be the Governing Body that acts on non-compliance.

Given the ongoing monitoring built into NDLFRs governance framework VicRoads could rely on those processes to provide a level of assurance that VicRoads data is being used appropriately. However, as in the discussion in the previous section, it would be more in keeping with VicRoads' PDPA obligations, and probably with sound risk management, for VicRoads to take a more proactive approach.

Putting in place a process to review audits and compliance statements would help VicRoads to keep track and not lose control of its data. Matters that VicRoads should particularly check for when reviewing annual audits include:

- The seriousness of any breaches or non-compliance
- Any instances of 'repeat offences' where a Requesting Agency has breached the PAA or its privacy and security obligations in the same way for a second year running
- Evidence of implementation of audit recommendations or a plan for implementation
- Any indication that Requesting Agency actions may cause VicRoads to, itself, breach a law
- Ongoing liaison with the NDLFRS governing body to ensure VicRoads has a good understanding of any issues arising in the system overall or with respect to particular Requesting Agencies.

Recommendation 8 – Processes to manage PAAs, including review of compliance, audit reports

IIS recommends that VicRoads, particularly in first few years of NDLFRS participation, undertake a regular program to review each of its PAAs. Matters that VicRoads should particularly check for when reviewing annual audits include:

- The seriousness of any breaches or non-compliance
- Any instances of 'repeat offences' where a Requesting Agency has breached the PAA or its privacy and security obligations in the same way for a second year running
- Evidence of implementation of audit recommendations or a plan for implementation
- Any indication that Requesting Agency actions may cause VicRoads to, itself, breach a law
- Ongoing liaison with the NDLFRS governing body to ensure VicRoads has a good understanding of any issues arising in the system overall or with respect to particular Requesting Agencies.

4.4.2 IPP issues

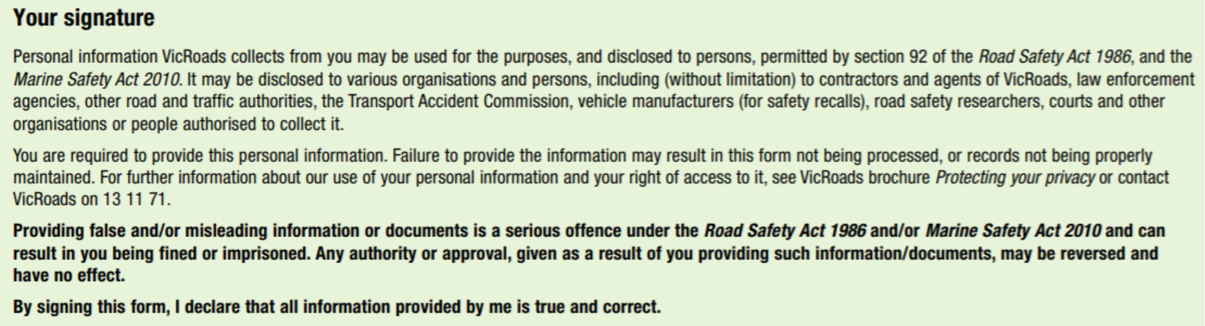
4.4.2.1 IPP 1 – Collection statements

IPP 1 requires organisations to take reasonable steps to ensure individuals are aware of matters including the purposes for which the information is collected and to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind.

The principle aims to help individuals make informed choices and to understand how their personal information will be used and handled. The steps needed will vary with the circumstances. IIS considers that VicRoads' participation in the NDLFRS is a significant change and that VicRoads will need to give thought as what 'reasonable steps' would be in this case.

IIS appreciates that in practice, it can be difficult to provide comprehensive, and understandable, information on forms or other channels used to collect personal information. Organisations also face challenges in terms the amount of space on forms to cover all matters, cost of changing forms to reflect current circumstances and so on.

VicRoads advises that its current practice is for notices to be fairly broadly worded, for example as in the following notice:



Your signature

Personal information VicRoads collects from you may be used for the purposes, and disclosed to persons, permitted by section 92 of the *Road Safety Act 1986*, and the *Marine Safety Act 2010*. It may be disclosed to various organisations and persons, including (without limitation) to contractors and agents of VicRoads, law enforcement agencies, other road and traffic authorities, the Transport Accident Commission, vehicle manufacturers (for safety recalls), road safety researchers, courts and other organisations or people authorised to collect it.

You are required to provide this personal information. Failure to provide the information may result in this form not being processed, or records not being properly maintained. For further information about our use of your personal information and your right of access to it, see VicRoads brochure *Protecting your privacy* or contact VicRoads on 13 11 71.

Providing false and/or misleading information or documents is a serious offence under the *Road Safety Act 1986* and/or *Marine Safety Act 2010* and can result in you being fined or imprisoned. Any authority or approval, given as a result of you providing such information/documents, may be reversed and have no effect.

By signing this form, I declare that all information provided by me is true and correct.

Other information is provided via privacy brochures, the VicRoads website and its privacy policy.

VicRoads also advised that it intends to update its notices to specifically name biometric facial matching as a usage of the data. To make sure it is meeting IPP 1 to the best effect, IIS encourages VicRoads to test its statements with individuals to identify the extent to which they are sufficiently 'aware' and to identify what further information might be helpful. It would be good practice to encourage individuals to go to the more detailed information. The approaches would vary with the channels used (hard copy forms, service centres, online). Particularly for online channels it should be possible to include links or buttons in an engaging manner.

Recommendation 9 – Collection notices

IIS supports VicRoads intention to amend its privacy statements to advise of use and disclosure of personal information for biometric facial matching.

IIS recommends that VicRoads undertake research to test its proposed statements to assess the extent to which they help make individuals aware of use and disclosure of personal information for biometric facial matching and to identify what additional information might be needed. VicRoads should also consider how to make such additional information readily available at the point at which personal information is collected.

4.4.2.2 IPP 3 – Data quality and IPP 6 – Access and Correction

IIS considered data quality in relation to the design and build of VicRoads' NDLFRS solution in Section 4.3.1.

The focus here is on whether the introduction of the NDLFRS will compound the impact of inaccurate data on individuals or introduce new sources of error, for example, in the face matching process. The potential for the multi-jurisdictional nature of the NDLFRS and FMS to make it difficult for individuals to track down the source of inaccurate records and have them resolved has also been raised in previous NFBMC and NDLFRS PIAs. These issues involve both IPP 3 and IPP 6 and these principles are therefore considered together.

IPP 6 gives individuals a right to access personal information about themselves and have it corrected if it is wrong. These access and correction rights are underlined by provisions in the draft FMS Participation Agreement.

The Agreement points out that it is the responsibility of Data Holding Agencies to address access and correction requests by individuals relating to the Agency's data held in the NDLFRS.[7] The draft FMS Participation Agreement also requires Data Holding Agencies to:

- Process access and correction requests made by an individual to another participant where that participant refers the request to the Data Holding Agency
- Tell another participant that personal information it holds in the NDLFRS is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, in the event that the Data Holding Agency becomes aware of any such deficiency.[8]

VicRoads noted in discussions its view that there might be less risk from inaccurate driver licence data than anticipated. The issue of problems with the data is already faced by the agency and the process for rectification would be the same for facial data.

Individuals can only have a valid licence in one jurisdiction, and so should know which jurisdiction to approach if alerted to a failure involving one of the face matching services. Moreover, in Victoria, citizens have a legal responsibility to keep driver licence details up-to-date and must, for example, notify VicRoads that they have changed address. It's also the case that the information on a Victorian driver licence should mirror the information in VicRoads' DLS and DLIS. If, for example, the image on the card was not of them, the person would be expected to contact VicRoads and then there is a business process to ask them to come in to have their picture re-taken. Any changes to the source will be carried across to the NDLFRS system – it is a mirror. In the NDLFRS the record would be marked as invalid (therefore excluded), once the new image is attached, the record would be marked as a new record for inclusion.

[7] See clause 16.2, *Draft FMS Participation Agreement (AGS Draft 26 June).*

[8] See clause 16.2, *Draft FMS Participation Agreement (AGS Draft 26 June).*

Potentially issues might come up for individuals in the operation of the facial recognition engine, for example, because a face constantly comes up in a gallery as a witness to a crime or for some reason facial verification does not work.

In addition, as with any new system, there might be unexpected sources of error in the handling of information. VicRoads also identified that its obligations under the NDLFRS governance framework to assist individuals in relation to access requests and complaints means there will be a need to ensure frontline staff are well across the NDLFRS.

IIS therefore considers that VicRoads should put in place a close watching brief so that it can identify and respond to any emerging NDLFRS data quality issues. It should also ensure it has in place procedures to that it can respond quickly to requests for access or to correct information. VicRoads should also ensure it establishes clear communication channels with other road agencies to facilitate the resolution of accuracy issues or access or correction requests involving more than one jurisdiction. Particular attention should be given to ensuring VicRoads frontline staff are aware of the NDLFRS and what should be done to assist where problems are raised.

Recommendation 10 – image quality and impact on customers

IIS recommends that VicRoads actively monitor its NDLFRS activities, including error reports, trends in the success or otherwise of the bulk and daily uploads and reports from the governing body and other road agencies, so that it is well informed on any data accuracy or image quality issues that are coming to light. In particular, VicRoads should watch and manage for any undue negative impact on individuals or groups of individuals, for example, matching difficulties involving VicRoads data leading to increased need to attend service centre to resolve issues.

IIS also recommends that VicRoads ensure it has in place procedures to that it can respond quickly to requests for access or to correct information. VicRoads should also establish clear communication channels with other road agencies to facilitate the resolution of accuracy issues or access or correction requests involving more than one jurisdiction.

Recommendation 11 – Staff awareness of VicRoads NDLFRS obligations and procedures

IIS recommends that VicRoads take steps to ensure its frontline staff are aware of VicRoads' role in the NDLFRS and know how to support customers who ask questions, seek access or correction or have been referred to a service centre because of a match failure.

4.4.2.3 IPP 4, and Part 4 of the PDPA – Security and VicRoads staff access to the Face Matching Services

IIS has, in the earlier parts of the PIA, noted VicRoads' approach to security and has considered particular issues with respect to the content and management of audit logs (Section 4.3.2). This work will extend to the BAU phase and will include the development of access matrices, review of security manuals and security assessments.

VicRoads asked IIS to consider the impacts of VicRoads staff access to the Face Matching Services.

From the information available to it, IIS considers that VicRoads' approach is mindful of issues such the need to ensure there is a continued high focus security as VicRoads moves into the BAU phases of its participation in the NDLFRS and FMS and for tight controls on, and auditing of, access to ensure systems such as OPOLS and FRAUS are used appropriately and that practices such as password sharing are avoided. IIS has not identified additional actions needed. As noted earlier, this phase of VicRoads' participation in the NDLFRS involves processes that once established are fairly automatic. Risks such as those flagged are perhaps more likely to emerge if the future if and when VicRoads moves to use the FMS.

4.4.2.4 IPP 4 – Data breach notification

IIS identified the need for an effective data breach handling process in the project design and build phase. It also considers VicRoads should ensure its data breach processes are appropriate as it moves to NDLFRS participation and BAU.

This will be needed to allow VicRoads to meet its specific obligation under the NDLFRS Hosting Agreement (clause 13.3) in relation to data breaches (called Information breaches in the Hosting Agreement).[9] These include:

- Notifying the Hosting Agency and other relevant participants in the event of a breach
- Taking immediate steps to mitigate risks
- Cooperating in the management and investigation of breaches
- Notifying affected individuals in Victoria about the breach (whether or not the breach arises in Victoria or at the Hosting Agency).

In addition, OVIC encourages agencies to report data breaches to it on a voluntary basis.[10]

As noted, VicRoads has a process in place. However, this has not yet been assessed to see if changes are needed to address the specific NDLFRS risks and requirements. IIS considers this should happen prior to live participation in the NDLFRS.

Recommendation 12 – Data breach management and notification

IIS recommends that before VicRoads goes live with NDLFRS participation it should review its current data breach and incident management processes to ensure they:

- Meet the Hosting Agreement and OVIC requirements
- Have been tested with realistic scenarios to ensure they work appropriately for the NDLFRS. Testing should assess matter such as:
  - Roles and responsibilities

[9] Agreement Relating to the Hosting of the National Driver Licence Facial Recognition Solution, which implements and sets out the operation of the NDLFRS and enables the NDLFRS Products to be provided by the Data Hosting Agency to each NDLFRS Contributor. HA at this point is the Hosting Agency.

[10] https://ovic.vic.gov.au/privacy/for-agencies/responding-to-data-breaches/

- Decision making and speed of response
- Notification processes
- Communications.

4.4.2.5 Privacy policy – IPP 5

IPP 5 in the PDPA requires organisations to have a privacy policy. Specifically, it states that ‘an organisation must set out in a document clearly expressed policies on its management of personal information’ and ‘make the document available to anyone who asks for it.’ IPP 5 further states: ‘On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.’

IIS also notes the governance framework includes ‘transparency requirements’, in particular, agencies’ participation in the FMS should be **transparent** by ensuring that information relating to their participation in the FMS is made publicly available in accordance with the FMS Participation Agreement.

Earlier in this PIA, IIS made comments in relation to VicRoads privacy notices, encouraging it to take some additional steps to ensure individuals are aware of the use and disclosure of information for facial biometric matching.

IIS understands that VicRoads will make changes to its privacy policy as well as its privacy notices. VicRoads also advises that it will provide links from its website to the HA website. IIS understands this will include information for individuals about the system and will also act as a central point for privacy inquiries and complaints. VicRoads also anticipates that HA will be centrally coordinating some community awareness activities.

IIS considers that an initiative such as the NDLFRS, which makes a significant change in the handling of personal information, does warrant a strong effort to build community awareness and support. IIS encourages VicRoads to assess the extent of information available from HA and to reassess the need for additional action closer to the NDLFRS go live.

IIS also makes the following observations about VicRoads’ privacy policy and some additional steps it might take for greater transparency.

VicRoads privacy policy is in the form of a brochure titled ‘Protecting your privacy.’ It summarises how VicRoads handles personal information and explains how to get in touch with a privacy query or complaint. VicRoads also offers an internet privacy policy on its website.

As already noted, VicRoads will update it privacy policy with information about NDLFRS and would provide a link to more information. IIS also encourages VicRoads to make the policy easier to find on website by:

- Having a direct link to privacy in the footer of the homepage (as is standard practice) – currently a user has to click ‘Website terms’ in the footer and then scroll down and click ‘privacy’
- Having the link to the privacy policy (the brochure) at the top of the privacy webpage, rather than right at the bottom after the internet privacy policy.

VicRoads could also consider having a dedicated webpage on the VicRoads website for information about the NDLFRS (this could contain content that is standard across road agencies or could also hold additional content that VicRoads develops).

Recommendation 13 – Transparency and public communications about the NDLFRS

IIS supports VicRoads intention to amend its privacy policy to provide information about its participation in the NDLFRS and about the FMS.

IIS recommends that VicRoads make its website privacy information more prominent and more easily discoverable.

IIS also recommends that, subject to steps taken by HA, VicRoads assess if additional community awareness activities are needed to ensure transparency.

5. Appendix A – About the NFBMC and NDLFRS

5.1 NFBMC, NDLFRS and FMS

The NFBMC is a key measure under the National Identity Security Strategy endorsed by the Council of Australian Governments (COAG) in 2007. The NFBMC comprises the infrastructure, legislative arrangements and governance arrangements that enable the sharing and matching of identity information by participants.

Technical infrastructure of the NFBMC includes the **Interoperability Hub** (the Hub) and the **NDLFRS**.

The Hub transmits image matching requests and responses between agencies participating in the NFBMC. It commenced operation in October 2016 with participating Commonwealth agencies.

The NDLFRS will make driver licence facial images available to agencies participating in the NFBMC. It will bring together driver licence images and biographic information from each of the states and territories, in a system hosted by the Commonwealth. Drivers licence information and image matching will occur via FMS. FMS is the collective name for services that will be offered by the NDLFRS. Services include:

- Face Identification Service (FIS), which enables a facial image to be compared against multiple images held on a database of government records. Its purpose is to **establish** an individual's identity.
- Face Verification Service (FVS), which enables a facial image of an individual to be compared against the facial image held on a specific government record associated with that same individual. Its purpose is to **confirm** an individual's identity.
- One Person One Licence Service (OPOLS), which enables a facial Image to be compared, on a constrained one-to-many basis, to other images hosted to identify whether a person holds multiple licences in the same or a different identity across jurisdictions
- The Facial Recognition Analysis Utility Service (FRAUS), which is designed specifically for road agencies which don't already have this capacity via their own face matching systems to analyse their own data and to undertake analysis/deduplication/investigation of their own data holdings.

The NDLFRS involves road agencies like VicRoads uploading drivers licence information and images to the system and keeping that information up to date. Road agencies are referred to as 'Data Holding Agencies'. Other agencies ('Requesting Agencies') may then establish access arrangements with the road agencies to query their data using the FMS. Access arrangements are to be strictly specified and limited.

A Data Holding Agency may also be a Requesting Agency. In some of the documentation, road agencies are also referred to as 'NDLFRS Contributors'. The Commonwealth plays the role of Hub Operator and Data Hosting Agency.

5.2 Governance arrangements for the NDLFRS

A range of agreements and policies govern the operation of the NDLFRS. At the top is the *Intergovernmental Agreement on Identity Matching Services* (IGA) that established the framework enabling state and territory participation in the FMS and the establishment of the NDLFRS. Under the IGA sit the:

- **FMS Participation Agreement,** which is an agreement made between the Commonwealth of Australia (represented by the Department of Home Affairs (HA) and each NDLFRS participant.
- **Participant Access Arrangement** (PAA) forms part of the FMS Participation Agreement. It is made between the Hub Controller, a Requesting Agency and one or more Data Holding Agencies. Its purpose is to set out the level of services being offered or requested and the way in which an agency will access the service.
- **NDLFRS Hosting Agreement** formed between the Data Hosting Agency and road agency (called an NDLFRS Contributor), in relation to that the road agency's provision of driver licence information to the NDLFRS and its use of NDLFRS 'products'.

The two agreements and PAA are currently in draft.

Accompanying the FMS Participation Agreement and the PAA are a number of policies (also in draft) including the:

- FMS Compliance Policy
- FMS Training Policy
- Access policies for each FMS.[11]

The Governance arrangements also include the Ministerial Council for Police and Emergency Management, which provides ministerial oversight, as well as the National Identity Security Coordination Group, which under the IGA is the governing body for the Identity Matching Services, and other advisory bodies.

5.3 VicRoads control of its data in the NDLFRS

The IGA and other elements of the NDLFRS governance framework emphasise that each jurisdiction providing information to the NDLFRs remains in control of the information. Ultimately, jurisdictions can seek to deny access to their data; clause 9.15 of the IGA allows a state or territory to direct the Commonwealth (as Hub Operator) to suspend an entity's access to the state or territory's data were there are concerns about the entity's compliance with privacy and security safeguards.

[11] IIS has only viewed the draft FVS Access Policy.

The Framework also sets a range of requirements for use of the FMS, to ensure information is appropriately protected and to give Data Holding mechanisms to satisfy themselves or to be satisfied that the requirements and standards are met.

5.3.1 Material VicRoads can consider when deciding on PAAs

The starting point would usually be the establishment of PAA.

There is a range of documents and evidence that Requesting Agencies must submit before they can access the FMS. The draft FMS PAA requires Requesting Agencies to:[12]

- adopt a privacy governance framework (clause 16.4 of the FMS Participation Agreement)
- demonstrate their legislative basis for dealing with personal information via the FMS in Statements of Legislative Authority (clause 46.1 of the FMS Participation Agreement)
- undertake or contribute to a privacy impact assessment on the proposed information flows between participating agencies (clause 46.2 of the FMS Participation Agreement)
- enter into agreements (PAAs) setting out the scope of information sharing via the FMS within the legislative confines (Part 4 of the FMS Participation Agreement)
- document arrangements for the retention and destruction of personal information obtained via the FMS; and circumstances where disclosure of that personal information may be made to third parties (clauses 34 and 35 of the FMS Participation Agreement)
- ensure users have the requisite training in accordance with the FMS Training Policy (clause 24 of the FMS Participation Agreement); and
- maintain appropriate security accreditation as informed by a Security Risk Management Plan (clause 22.1 of the FMS Participation Agreement).

5.3.2 Ongoing compliance with privacy and security safeguards

The draft FMS Compliance Policy (the draft policy) lists ways of assessing compliance, or non-compliance with privacy and security safeguards.[13] These include:

- Annual audits by Requesting Agencies
- Annual compliance statements (by Requesting Agencies and Data Holding Agencies)[14]
- Regular review of query data reports by the Hub Controller or the Data Hosting Agency or by an agency's internal reviewers
- Notification by another agency, the OAIC, a state or territory privacy regulator or a complaint by a member of the public.

[12] This summary appears at paragraph 3.5 of *Compliance Policy – Face Matching Services – Draft version 1.7.*

[13] See paragraph 4.7, *Face Matching Services Compliance Policy*, draft version 1.7.

[14] Clause 17.1 of the *Draft FMS Participation Agreement (AGS Draft 26 June)* provides that the Data Hosting Agency will prepare compliance statements on behalf of Data Holding agencies

5.3.2.1 Requesting Agency annual audits

Clause 38 of the FMS Participation Agreement requires Requesting Agencies to do an annual audit and explains what it should cover. Specifically, clause 38 requires the following:

- The annual audit must confirm the Requesting Agency's compliance with its PAA.
- The annual audit must make recommendations to address any non-compliance with the PAA.
- An auditor must conduct the annual audit.
- The auditor must inspect the Requesting Agency's systems, processes, record keeping and overall use of the relevant Services under the Participant Access Arrangement.
- The Requesting Agency must inform the Data Holding Agency of the selection of the Auditor to be engaged.
- The auditor must be independent of the Requesting Agency if feasible (if not feasible, the Requesting Agency must get the agreement of the Data Holding Agency to use an auditor that is not independent).
- The Requesting Agency and Data Holding Agency must provide any relevant information to help the auditor conduct the audit (including all information related to the PAA)
- The Requesting Agency must give a copy of the annual audit report to the Data Holding Agency, as soon as practicable after the end of the relevant calendar year, (and no later than 5 months after the end of that year).

According to the FMS Participation Agreement, the annual audit must contain the following:

- Any times the Requesting Agency breached their stated legislative authority in their handling of NDLFRS data
- Details of any security breaches or notifiable data breaches
- Details of any instances where the Requesting Agency received a complaint about its use of the FMS and NDLFRS data obtained under the relevant PAA, and action the Requesting Agency took in response
- The size and composition of the random samples used in the Annual Audit and a statement explaining how the samples are appropriate to support the conclusions of the Annual Audit Report
- The Requesting Agency's handling and storage of information accessed via the FMS and whether the Requesting Agency complied with its information destruction obligations
- Other service-specific annual audit report requirements detailed in the Requesting Agency's PAA(s)

The FMS Participation Agreement sets out extra matters the annual audit must include for Requesting Agencies that use the FIS.[15]

5.3.3 Compliance statements

In addition to annual audits, participants must submit annual 'Compliance Statements' which provide a regular check that participants are meeting their PAA obligations. Clause 17 of the draft FMS Participation Agreement sets out the matters Compliance Statements must cover.

Participants submit the statements to the Hub Controller which provides them to the Governing Body. The Data Hosting Agency prepares an annual Compliance Statement on behalf of Data Holding Agencies.

5.3.4 Governing Body review of annual audits and compliance statements

Annual audits and Compliance Statements are given to the Governing Body annually for their consideration. According to the draft FMS Compliance Policy, where these reports contain recommendations, the Governing body will oversee the implementation of recommendations, as appropriate.

[15] See clause 38.5, *Draft FMS Participation Agreement (AGS Draft 26 June).*

6. Appendix B – List of documents reviewed

Documents Reviewed
NDLFRS Governance Documents
Draft NDLFRS Hosting Agreement (AGS draft 26 June 2018)
Draft FMS Participation Agreement (AGS draft 26 June 2018)
Draft FMS Participation Agreement (AGS draft 26 June 2018)
Draft NDLFRS Hosting Agreement (AGS draft 26 June 2018)
COMPLIANCE POLICY - Face Matching Services - Draft version 1.7
TRAINING POLICY - Face Matching Services - Draft Version 2.3
Face Identification Service Access Policy v2.4
OPOLS ACCESS POLICY - Face Matching Services - Draft version 3.1
FVS ACCESS POLICY - Face Matching Services - Draft 3.3
VicRoads documents
NDLFRS Bulk File - File Specifications v1.2
NDLFRS Change Request CR-4 (Location)
NDLFRS Change Request CR-6 Business Requirements
NDLFRS Change Request CR-7 Business Requirements Options Summary
NDLFRS Change Request CR-8 Business Requirements
NDLFRS Functional Specifications v1.1
NDLFRS Incremental File - File Specifications v1.3
Privacy and Collection Statements – examples

7. Appendix C – Analysis against Victoria's Privacy Principles

Appendix C sets out the IPPs in the PDPA and assess explains how they apply to VicRoads and the NDLFRS. Where relevant, IIS has identified matters for further consideration and these are discussed in Section 4 above.

Privacy Principle	Assessment – design & build	Assessment - BAU
IPP 1 Collection Must not collect personal information unless necessary for functions or activities, must collect personal information by lawful and fair means and not in overly obtrusive way, must give privacy notice at point of collection	No risks identified – collection limited, feedback from HA about record uploads and audit log information (which is unlikely to involve personal information).	As per design and build, collection consistent with principle. VicRoads advises it will be amending its privacy notices to provide high-level advice about use/disclosure or facial matching. See discussion in section 4.4.2.1.
IPP 2 Use and disclosure Must not use or disclose personal information for a purpose other than the primary purpose of collection	Unlikely to be risks. VicRoads' participation in NDLFRS as a Data Holding agency. Disclosures authorised by RSA, Part 7B regulates use and disclosure of information; s 90K(a)(vi) allows disclosure in relation to an intergovernmental agreement; s 90K(g) allows disclosure for law enforcement purposes. No IIS recommends developing policy on use of information in audit logs to minimise risk Section 4.3.2.1.	As per design and build. No additional risks identified.
IPP 3 Data quality Must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date	IIS understands that there are inherent challenges with data quality – images and related biographical details – and that the VicRoads has taken reasonable steps so far to address the additional risks. Possible additional steps noted at Section 4.3.1	VicRoads has considered potential for accuracy issues to impact individuals once NDLFRS is in operation. While it considers extent of issues, and steps customers need to take, won't necessarily change as a result of the NDLFRS, issues could possibly arise. BAU accuracy issues are considered further at Section 4.4.2.2

Privacy Principle	Assessment – design & build	Assessment - BAU
IPP 4 Data security Must take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure Information no longer required for any purpose must be deleted or de-identified	From information reviewed and discussions with VicRoads, IIS considers approach is largely consistent with IPP 4. IIS considers there is some risk if VicRoads: ● Does not appropriately manage audit logs (Section 4.3.2.1) ● Retains personal information when no longer needed (Section 4.3.2.2) ● Data breach processes are not sufficient or do not work well in practice (Section 4.3.2.3)	As per design and build – approach largely consistent with principle and no additional issues identified.
IPP 5 Openness Must set out in a document clearly expressed policies on its management of personal information	Not relevant in this phase	Approach is consistent with IPP 5. VicRoads has an existing privacy policy and advises this will be updated to reflect involvement in the NDLFRS. IIS has some suggestions for better practice at Section 4.4.2.5.
IPP 6 Access and correction Must provide individuals with access to their information except in certain circumstances Must take reasonable steps to correct the information if individual is able to establish that the information is not - accurate, complete or up to date	Not relevant in this phase	Approach is consistent with IPP 6. IIS considers some specific steps needed in context of NDLFRS. See Section 4.4.2.6.
IPP 7 Unique identifiers Unique identifiers should not be assigned to individuals unless it is reasonably necessary to enable the organisation to carry out any of its functions efficiently. Organisations must not adopt, use or disclose other organisations' identifiers unless specified conditions apply	VicRoads will be using and disclosing driver licence number, which are unique identifiers in the context of the NDLFRS (see further Section 3.2). Under s.6 of the PDPA it has a lawful basis for disclosing information to the NDLRS under s. 90K(a)(vi) of the RSA. IIS has not identified risks against IPP 7.	As per design and build.
IPP 8 Anonymity Wherever lawful and practicable, individuals must have the option of not identifying themselves	Not relevant for this project.	Not relevant for this project.
IPP 9 Transborder data flows May only transfer personal information to someone outside	VicRoads' participation in the NDLFRS will involve it in transferring information to 'someone outside of Victoria'. IIS considers that it's likely the requirements in the NDLFRS	As for design and build.

Privacy Principle	Assessment – design & build	Assessment - BAU
of Victoria under certain circumstances including sub	governance framework, and that it is legally binding, would mean that the information will be protected in ways that are substantially similar to the IPPs. Alternatively, subject to its approach, it's likely that VicRoads could also rely on having 'taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the IPPs.' No risks identified.	
IPP 10 Sensitive information Must not collect sensitive information unless under certain circumstances, for example: consent, required by law, to prevent harm	The PDPA defines sensitive information as information about: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record.[16] Information of this nature not included in the NDLFRS. No risks identified.	As for design and build.

[16] See Schedule 1 http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/vic/num_act/padpa201460o2014317/

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898