newzealand.govt.nz

Ministry of Business, Innovation & Employment

Privacy impact assessment report: Collection and handling of biometrics at the Ministry of Business, Innovation and Employment

May 2016

Author

Ministry of Business, Innovation and Employment

Acknowledgement

The Ministry of Business, Innovation and Employment (the Ministry) acknowledges the internal business units and external agencies interviewed who provided information about their collection and handling of biometric information.[1]

Enterprise Reporting and Data Management Services
Compliance Risk and Intelligence Services
MBIE Risk and Assurance
ICT Security
Office of the Privacy Commissioner
MBIE Records Services
Refugee Quota Branch
Refugee Status Branch
Immigration Resolutions
Settlement, Protection and Attraction Unit
Visa Services and Operations Support
Department of Internal Affairs
New Zealand Customs Service
New Zealand Police
New Zealand Trade and Enterprise
Ministry for Primary Industries
Ministry of Foreign Affairs and Trade
Ministry of Justice

Disclaimers

The Ministry has made every effort to ensure that the information contained in this report is reliable and up to date, but makes no guarantee of its accuracy or completeness and does not accept any liability for any errors. The information and opinions contained in this report are not intended to be used as a basis for commercial decisions, and the Ministry accepts no liability for any decisions made in reliance on them. The Ministry may change, add to, delete from or otherwise amend the contents of this report at any time without notice.

[1] Internal business units and external agencies who have contributed to this PIA have been updated effective November 2015

ISBN 978-0-478-36056-1

May 2016

Ministry of Business, Innovation and Employment
PO Box 1473
Wellington
New Zealand
www.mbie.govt.nz

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

STRUCTURE OF THE PRIVACY IMPACT ASSESSMENT

The Ministry of Business, Innovation and Employment's (the Ministry's) objective for the management of biometric information is to ensure a consolidated and consistent best practice approach to the collection and handling of biometric information that is principled and consistent with privacy and immigration law, and with its national and international obligations and agreements. To that end, and for consistency with section 32 of the Immigration Act 2009 (the 2009 Act), the Ministry has completed a privacy impact assessment (PIA).

Section 32 of the Immigration Act 2009 requires the Ministry to undertake, publish and review a PIA in respect of the collection and handling of biometric information under the Act. In particular, the activation of the legislative provisions set out in the Immigration Act 2009 which are relevant to biometric information. Specifically these are sections 60, 99, 100, 104, 111, 120, 149, 287-291, 305 and 306.

This PIA was initially completed and published in 2010 (PIA 2010). It was reviewed, updated and republished in July 2012 (PIA 2012). A further review of the PIA 2012 has been undertaken in compliance with section 32 to consider the impact of changes on the handling and collection of biometric information by the Ministry since 2012. The PIA 2012 is replaced by this update - Privacy impact assessment report: Collection and handling of biometrics at the Ministry of Business, Innovation and Employment. This update will be referred to as the PIA 2016.

With the initial publication of the PIA 2010, the Ministry consulted the Office of the Privacy Commissioner (OPC) on the terms of reference (TOR). Through ongoing consultation, the PIA report structure was agreed to. The TOR and basic structure of the PIA 2016 has not altered from the original version. Existing appendices have been updated where required and new additional appendices have been included in the PIA 2016.

A PIA is a systematic process for evaluating a proposal in terms of its impact upon privacy. This PIA is evaluating the proposals related to the privacy impacts of implementing biometric provisions within the Ministry. It is intended to:

- Identify the potential impacts that the collection and handling of biometric information may have on a person's privacy;
- Examine how potential detrimental effects upon privacy might be overcome by providing mitigations;
- Equally examine how potential privacy enhancing outcomes of biometric information can be harnessed; and
- Ensure that new projects comply with the information privacy principles in the Privacy Act 1993.

The Privacy Act 1993 and related information privacy principles form the basis of this assessment. Each of the principles relates to a different stage of the

personal information life cycle. Therefore, this PIA assesses the collection, storage, use and disposal of biometric personal information.

The topics and issues for analysis in this PIA were sourced from the following documents considered best practice.

Title	Source	Version	ISBN
Privacy Impact Assessment Toolkit	Office of the Privacy Commissioner, Wellington	July 2015	978-0-478-11743-1
Guiding Principles for the Use of Biometric Technologies for Government Agencies	Cross Government Biometrics Working Group (CGBG) Department of Internal Affairs, Wellington	April 2009	978-0-478-29487-3
Trusted Computing and Digital Rights Management Principles and Policies	State Services Commission, Wellington	September 2006	978-0-478-30301-8
Trusted Computing and Digital Rights Management Standards and Guidelines	State Services Commission, Wellington	July 2007	978-0-478-30315-5

Since the first publication of this PIA in 2010, the Government ICT Strategy and Action Plan[2] been implemented. The role of Government Chief Privacy Officer (GCPO) was established to help agencies build trust and confidence in Government management of privacy matters. The Ministry is required to align its work with the Government ICT Strategy and Action Plan which has privacy-by-design as part of its guiding principle.

Conducting a PIA is an integral part of privacy-by-design, as it enables the Ministry to identify the risks upon the privacy of individuals early in the design of a new initiative, to ensure that the Ministry's services can be designed with privacy in mind.

Additionally, the PIA considers the requirements of the Public Records Act 2005 regarding the disposal and archiving of official information and the protection of government records of historical values such as immigration records.[3]

[2] https://www.ict.govt.nz/assets/Strategy-and-Action-Plan/ICT-Action-Plan-2014-NEW.pdf

[3] http://archives.govt.nz/advice/continuum-resource-kit/continuum-publications-html/g8-guide-public-records-act

This PIA provides a framework within which ongoing assessment of the privacy implications of implementing the biometrics provisions in the 2009 Immigration Act are addressed. It is structured so that subsequent implementations of biometrics can be integrated into a coherent document.

As the Ministry advances its biometrics programme, various initiatives will require activation of the legislative provisions in the relevant sections of the 2009 Act. The appendices document those initiatives, and provide an assessment of their possible risks and mitigations.

This PIA is the 'umbrella' that summarises the environment and permits a consolidated and consistent privacy best practice on the use of biometrics at all levels. It also provides the background for representations to Cabinet supporting the necessary Orders-in-Council.

This approach enables the PIA to act as a reference tool, ensuring each initiative is assessed separately in a corresponding appendix to address specific biometric information processing functions.

This PIA 2016 is the main source of impact assessment on the Ministry's use of biometric information. The following summarises the structure of chapters in this document.

Executive summary and summary of risks and mitigations

This section provides a summary of the PIA 2016 and describes current and future implementation of the biometric provisions of the 2009 Act. The executive summary includes two tables:

- Table 1 is a summary of the relevant sections from the 2009 Act and the actions the Ministry has taken or proposes to take under those sections; and
- Table 2 is a list of all of the biometric-specific privacy risks identified and the possible ways to mitigate those risks. The risks are separated into three groups, governance risks, handling risks and security risks.

The chapters in this PIA have been updated to reflect relevant changes since the most recent PIA was published (PIA 2012), and to reflect the Ministry's proposed practices with respect to the collection and handling of biometric information as part of the Vision 2015 Programme. The Ministry is introducing new initiatives which further integrate the use of biometric information in the immigration environment. This includes the proposed final state implementation of the supporting technology enabler, Immigration Global Management System (IGMS) as it is understood at the time of this review.

Chapters 1–3

These chapters cover:

- the background to the changes introduced by the 2009 Immigration Act;

- the context or reasons for the Ministry's intention to increase the use of biometric information to improve its management of identity of non-New Zealand citizens;
- the issues for identity information management faced by the Ministry and an examination of the options available; and
- How biometric information will be used.

Chapter 4

This is a short description outlining the scope of the PIA, what is covered and what is excluded.

Chapter 5

This covers the research process for the PIA and its results. It describes how the information was collected, the interview process, people interviewed and a summary of the results of the interviews. It includes a diagram that shows the current and expected future biometric information flows within the Ministry and explanatory text in support of the diagram.

Chapters 6 and 7

These chapters examine the Ministry's actual and proposed use of biometrics in the light of the guiding principles (chapter 6) and implementation principles (chapter 7) recommended by the Cross Government Biometrics Working Group (CGBWG). This includes a detailed examination of the proposed uses of biometrics against the information privacy principles from the Privacy Act 1993.

Chapter 8

This describes the main biometric related privacy risks identified. Each risk is classified as a governance, handling or security risk. The description of the risk is accompanied by recommendations for ways to mitigate the risk. Options are presented for a biometrics privacy strategy and on-going governance.

Chapter 9

Chapter 9 addresses general approaches to enhanced privacy responses by using tools such as privacy by design and privacy-enhancing technologies.

Chapter 10

Chapter 10 discusses the need for on-going routine monitoring and review.

Chapter 11

This chapter provides concludes the document with highlights of the key risks identified and recommended next steps.

Appendices

Appendix 1: A list of abbreviations used in the document.

Appendix 2: An outline of general privacy risks that are already being addressed.

Appendix 3: A summary of biometrics initiatives implemented currently and proposed for future state by the Ministry.

These are followed by appendices covering specific powers and uses of biometrics, which are maintained, as required, under section 32, subsection 3, of the 2009 Act. Each new initiative or significant change involving biometric information within the Ministry is assessed within a corresponding appendix and recorded in the updated PIA. The initiatives assessed to date, are:

Appendix 4: An assessment of the use of face biometrics.

Appendix 5: An assessment of manual data sharing.

Appendix 6: An assessment of automated data sharing.

Appendix 7: An assessment of alerts to identify criminals for removal.

Appendix 8: An assessment of refugee status branch.

Appendix 9: An assessment of quota refugees.

Appendix 10: An assessment of the use of biometric and special biometrics to enable deportation.

Appendix 11: As assessment of investigations.

Appendix 12: An assessment of data matching capability.

EXECUTIVE SUMMARY AND SUMMARY OF RISKS AND MITIGATIONS

The Ministry is required to establish confidence in and verify the identity of people wishing to travel to, enter or stay in New Zealand. The Ministry's challenge is to accomplish that while improving the effectiveness and efficiency of its processes. Biometrics is a critical enabler for the Ministry to meet this obligation.

Biometric information is used to improve effectiveness by facilitating service improvements, reducing costs and reducing the potential for identity fraud. It enables improved efficiency by permitting faster processing of low risk people and introducing automated processing of labour intensive operations such as identity verification.

The Immigration Act 2009 contained provisions that permit the Ministry to collect biometric information from clients on a mandatory basis. Section 32 requires the Ministry to conduct and maintain a PIA prior to implementing biometric provisions.

This PIA was initially completed and published in 2010 (PIA 2010). It was reviewed, updated and republished in July 2012 (PIA 2012). A further review of the PIA 2012 has been undertaken in compliance with section 32 to consider the impact of changes on the handling and collection of biometric information by the Ministry since 2012. The PIA 2012 is replaced by this update - Privacy impact assessment report: Collection and handling of biometrics at the Ministry of Business, Innovation and Employment. This update will be referred to as the PIA 2016.

The PIA 2016 takes into consideration the Ministry's Vision 2015 Programme which relates to INZ's new identity management processes and capability and in particular, the enhanced role of the use of biometric information. The programme will see biometrics used increasingly and consistently across the Ministry's immigration operations. It is supported by the implementation of the Immigration Global Management System (IGMS), a core component of Vision 2015 that is a key technology enabler.

Business processes are changing so that simple, low-risk decisions can be made quickly and human expertise and judgement will be focussed on more complex situations. Business systems are being transformed in a phased approach to an integrated infrastructure including leading edge biometrics collection, matching and processing. Two new initiatives in support of Vision 2015 are:

- An automated data sharing capability with Five Country Conference (FCC) Protocol partners which is in accordance with the existing FCC Partner Agreements for data sharing[4]. The main component is the development of

[4] http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/fccqa.htm

a real time data sharing platform ("Secure Real Time Platform" or SRTP), which can be used to securely share data of fingerprint match requests and responses with FCC partners.
- The capability to match biometric information with biographic information through the Identity Matching Engine, IDMe.

Both initiatives are part of the Immigration Global Management System.[5] Their implementation will provide further assurance of individuals' identity.

The Vision 2015 Programme is covered by a separate umbrella PIA, which references managing biometric information and relies on the guidance within this Biometric PIA 2016 specifically for the handling and use of biometric information. The Ministry is the authoritative source of identity information about non-new Zealand citizens, and its information is relied upon by other government departments such as the Department of internal Affairs when considering an applicant for New Zealand citizenship. This increases the need for accurate identification of people entering the country.

To understand the actual and proposed use of biometrics, interviews were conducted with internal staff and external stakeholder agencies. Existing and proposed biometric information flows were analysed and documented and these have been updated in this version of the PIA. A review of the privacy risks and their possible mitigations listed in Table 2 has been undertaken. These remain relevant and appropriate for the PIA 2016. Subsequently, internal Ministry control plans have been updated at a detailed level to manage privacy risks and their mitigations.

Alternatives to biometrics considered in the PIA include collection of more biographic information, increasing the use of interviews of visa applicants and more intensive document analysis. While these add limited improvement to the efficacy of the system, they would all require more effort and significant resources, delay processing times and still not provide high confidence in identity.

This PIA does not address the disclosure of biometric information under the relevant provisions in Part 8 of the 2009 Act as the Ministry must enter into individual agreements with each agency to which it intends to disclose information. Privacy protections remain, however, as section 32 requires a PIA to be completed prior to an agreement being made. The agreements must also be consulted with the Privacy Commissioner.

Table 1 below represents a summary of the sections of the Immigration Act 2009 that are relevant for the collection and handling of biometric information by the Ministry, and the actions required, which will be implemented in phases. This PIA identifies privacy risks in regards to both the current state (as of PIA 2016) and takes into account the proposed future state. This allows the privacy impacts and mitigations to be identified in a holistic manner and prior to any implementation.

---

[5] IDme and Immigration Global Management System are described in detail in Section 5, Process and Information Flows

This will enable the Ministry to design its systems, policies, procedures and products to take account PIA recommendations.

Sections 100 and 104 of the 2009 Act, although provided for and mandated, are not fully activated yet. The provisions are in place and biometric information is collected on an ad hoc and case by case basis by requesting a photo of an individual. When these provisions are to be applied systematically, this document will be updated.

Table 1: Summary of Immigration Act 2009 biometric privacy provisions

	Section of Act and proposed action
60	Biometric information may be required from visa applicant. • Require all foreign nationals[6] who make an application for a visa on or offshore to provide a 'passport grade' photograph or the photograph on the biographic page on a passport or in an e-chip passport. • All foreign nationals to be required to provide an in person photograph and/or fingerprints where requested.
99	New Zealand citizen may confirm citizenship before arrival in New Zealand. • New Zealand citizens may be required to provide a photograph before boarding a craft. If this is refused, section 104 applies on arrival.
100	Collection of biometric information from proposed arrivals. • All foreign nationals to be required to provide an in person photograph and/or fingerprints where requested.
104	New Zealand citizens photographed on arrival. • All New Zealand citizens to be required to provide an in person photograph.
111	Collection of biometric information. • All foreign nationals to be required to provide an in person photograph and/or fingerprints and the photograph on the biographic page on a passport or in an e-chip passport.
120	Persons other than New Zealand citizens leaving New Zealand to allow biometric information to be collected. • All foreign nationals to be required to provide an in person photograph and/or fingerprints and the photograph on the biographic page on a passport or in an e-chip passport.
149	Powers of refugee and protection officers. • All asylum claimants to provide an in person photograph and/or fingerprints. • All refugee and/or protected people being investigated to provide an in person photograph and/or fingerprints.

[6] The 2009 Act allows 'exceptions' to be established. For example, heads of state, guests of government, and so on. Any exceptions will be established as part of the policy development and implementation process.

287	Special powers pending deportation or turnaround. • Where any person is liable for deportation or turnaround, an immigration officer has such of the following powers as are necessary to meet the entry or transit requirements of any country to which or through which the person is to travel: (a) the power to photograph and measure the person; (b) the power to take the person's fingerprints, palm-prints, or footprints, or a scan of the person's irises.
288	Requirement to allow collection of biometric and special biometric information. All foreign nationals to be required to provide an in person photograph and/or fingerprints where they meet the criteria in section 288. This includes where an immigration officer has good cause to suspect that a person: a. is liable for deportation or turnaround; or b. is not complying with, or is materially breaching, the conditions of the person's visa; or c. is undertaking work or a course of study where the person is not entitled to undertake that work or study under this Act; or d. has obtained a visa under a fraudulent identity. There are circumstances where any biometric information or special biometric information obtained from a person must be destroyed if the person's liability for deportation is cancelled or suspended, or if the person is granted a visa and entry permission.[7]
289 to 291	An immigration officer may apply to a court for an order compelling the collection of biometrics if necessary (sections 289 to 291). Section 291 also provides further ability to apply for a compulsion order.
305 -06	The Ministry is authorised under the 2009 Act to exchange information, including biometric information with equivalent authorities in other countries for immigration purposes by virtue of sections 305–6.

Table 2 is a list of all of the biometric-specific privacy risks identified in the initial PIA 2010 and the possible ways to mitigate those risks. The risks are separated into three groups, Governance (G) risks, Handling (H) risks and Security (S) risks. Specific risks have been identified where relevant and are included in the supporting appendices for each of the biometric initiatives assessed (refer Appendices 4-12).

The risks have been reviewed for the PIA 2016. Both the risks and mitigations remain relevant and where there have been changes to the status of the mitigations, these has been identified in Section 8, Risk Assessment – Analysis of Impacts. In addition, internal Ministry privacy risk control plans have been updated at a detailed level to enable ongoing management and oversight of the risks and their subsequent mitigations.

[7] Section 288: replaced, on 7 May 2015, by section 73 of the Immigration Amendment Act 2015 (2015 No 48).

Governance risks are not all addressed or mitigated specifically within this PIA, as they may be broader risks addressed across the Ministry by way of the internal MBIE Privacy Policy or other relevant policies.

The Cross Government Biometrics Group (CGBG) stipulates the requirement for compliance with enabling legislation and it draws particular attention to compliance with the Privacy Act 1993 Privacy Principles. Mitigation strategies have been aligned to the privacy risks where non-compliance with a privacy principle may occur. These have been addressed in Section 6, Analysis of the Guiding Principles.

Table 2: Privacy risks and agreed mitigation actions

	Governance risks	Mitigations
G1	No formal centralised oversight of personal information management or privacy risk.	• Establish a governance group for biometric (and other personal) immigration information. • Include in the remit for the governance group formal responsibility for privacy issues, a consolidated comprehensive personal information management strategy and reporting structures for privacy issues. • The group contributes to Ministerial 'cultural' leadership; respect for privacy is not automatic and cannot be assumed.
G2	Inconsistent, limited or contradictory policies and instructions on the collection and handling of biometric information.	• Maintain a comprehensive policy that accommodates all aspects of the personal information management life cycle and all the information privacy principles.
G3	Unnecessary expense incurred because systems are not designed from the beginning to include privacy considerations.	• Incorporate 'privacy by design' for all new biometric/personal information management systems in the Ministry. • Ensure PIA's are undertaken (consistent with legislative obligations) for all new and significantly changed systems that store or process biometric information prior to their design/build phase and add as an appendix to this PIA. • Design personal information management systems (manual and automated) so that requests for personal information can be answered quickly, completely and without undue expense. • Design personal information management systems so that privacy request processes provide adequate management reports on the nature, frequency and resolution of issues.

G4	Authorisation to access biometric information too widely approved.	• Maintain adequate controls around granting authorisation to access biometric information. • Design audit processes into all systems used to store or process biometric information to control user accounts, access rights and security authorisations. • Base access rights to biometric information on the need to know (essential business justification).
G5	Inadequately managed collaboration and information sharing with other agencies putting biometric information at risk.	• Include privacy considerations in collaborative undertakings with other agencies. • Ensure that information-sharing agreements do not compromise the Ministry's ability to meet its statutory obligations. • Require measures to prevent unauthorised use or disclosure of biometric information.
G6	Inadequately managed outsourcing does not adequately protect biometric information. (This includes service agreements, contracts and memoranda of understanding with other agencies acting as agents/service providers for the Ministry.)	• Include privacy considerations in any tendering processes, negotiations and contracts for outsourced collection or handling of biometric information. • Maintain measures to monitor and audit outsourced collection or handling of biometric information to ensure that the Ministry's privacy responsibilities are met. • Require measures to prevent unauthorised use or disclosure of biometric information.
G7	This PIA is not reviewed, augmented or kept current in contravention of section 32 of the 2009 Act.	• Manage a process for review and amendment of this PIA if changes are made to the 2009 Act, regulations, operational policy with respect to the collection and handling of biometric data.
	Handling practices risks	**Mitigations**
H1	Biometric information is unnecessarily or excessively collected and retained, including multiple types of biometric information (multimodal) collected without adequate justification.	• Ensure that all implementations of the biometric provisions in the 2009 Act are in line with the statutory authority. • Limit collection of biometric information to what is needed (essential business justification) to support current decisions.
H2	Staff makes arbitrary 'requests' for biometric information.	• Maintain guidelines in operational policy, business processes and staff training/awareness for requiring biometrics from specific people. • Train staff in the application of the Ministry's Code of Conduct and the exercise of it in situations where professional judgment is required.
H3	Biometric information not collected directly from the person concerned.	• Maintain privacy protective processes for handling biometric information collected from third parties (for example, through information sharing and/or other service level agreements/contracts).

H4	People not adequately informed about the purposes of collection of biometric information.	• Ensure that people are appropriately notified in a relevant manner whenever biometric information is collected from them. • Build an acknowledgement of biometric collection into the biometric enrolment and verification processes.
H5	The manner in which biometric information collected is unfair or intrusive.	• Include appropriate responses in operational policy, business processes and staff training/awareness to cultural and physical considerations when collecting biometric information.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their biometric information.	• In immigration matters, these people will be treated as if they have the same rights as citizens and residents. This meets the requirements under section 34 of the Privacy Act 1993 as amended on 8 September 2010.[8]
H7	Due to inadequate system design, inability to respond to: • requests for access to information, or • requests for correction of information, or • Privacy Commissioner's investigations.	• Maintain oversight and review mechanisms. (See also G3.) • Design biometric information systems with the ability to respond to review agencies' requests/investigations.
H8	Biometric information incorrectly associated with a person.	• Maintain processes/checks to ensure that biometric information is not associated with a person record by mistake.
H9	Inaccurate or incorrect biometric data is used to make a decision about a person.	• Include biometric information in the processes for permitting comment on and rebuttal of potentially prejudicial information. • Develop processes for handling false negatives and false positives when matching biometrics.
H10	Biometric information retained longer than necessary.	• Apply to the Chief Archivist, Archives New Zealand, for a formal disposal authority. • Introduce standard processes for assessing biometric information for transfer to 'inactive storage' and/or for disposal. • Ensure that all implementations of the biometric provisions in the 2009 Act are in line with the statutory authority.
H11	Biometric information used for non-immigration purposes.	• Ensure staff training/awareness in permissible uses of the information. • Build auditing and security capability into any future ICT system. • Review the Ministry's Code of Conduct to include specific guidance on the handling of personal information.

8 http://inzkit/publish/visapak/visapak/#43967.htm

H12	Disclosure of biometric information without reasonable grounds.	• Maintain specific guidelines on the release and disclosure of biometric information into operational policy, business processes and staff training. • Ensure staff understanding of their responsibilities through training, awareness and other support materials.
H13	Unnecessary assignment of unique identifiers.	• Continue the current process of assigning unique identifiers that are not biometric templates.
H14	Widespread use of biometric templates as unique identifiers.	• Do not share biometric templates with other agencies as unique identifiers.
	Security risks	**Mitigations**
S1	Loss of biometric information.	• Ensure an adequate security environment for biometric information. • Apply appropriate encryption of biometric information when it is transferred between agencies where agreements are in place. • Maintain contingency plans to address any security breaches. • Comply with the Privacy Commissioner's Privacy Breach Guidelines.[9]
S2	Unauthorised access to, use, disclosure and modification of biometric information.	• Maintain preventive measures to guard against unauthorised access and subsequent unauthorised modification, use or disclosure of biometric information. (See also H12.)
S3	Safeguards implemented to ensure the security of biometric information are not reasonable (adequate) in the circumstances.	• Design and document appropriate security procedures for the collection, storage, transmission, and disposal of biometric information. • Ensure that security applied to biometric information is appropriate to the sensitivity of the information. • Apply to the Chief Archivist, Archives New Zealand for a formal disposal authority for biometric information.

[9] http://www.privacy.org.nz/privacy-breach-guidelines-2/?highlight=data%20breach%20notification

1. BACKGROUND

1.1 Biometric provisions in the Immigration Act 2009

Reliable identity information management is fundamental to the effective operation and integrity of New Zealand's immigration system. Immigration processes need to establish high confidence in a person's identity to enable decision makers to determine if that person should be permitted to travel to, enter or stay in New Zealand.

In 2007, an identity audit report[10] produced by the Office of the Auditor General highlighted areas for improvement in immigration identity information management. Particular focus was on significant weaknesses with the Ministry's lack of ability to use biometric information in a way which aligns with the information privacy principles in the Privacy Act 1993. That report challenged the Ministry to devise a way to permanently associate a person with an identity that can be consistently used across immigration transactions.

Biometric information is integral to the effective confirmation of identity and to prevent the fraudulent use of multiple identities in the immigration system and to assist in the streamlining of person focused processes. The CGBG defines biometrics as *"the science of measuring an individual's physical or behavioural characteristics"*[11]

Biometric information is defined in section 4 of the Immigration Act 2009 as:

> *Biometric information, in relation to a person,–*
>
> *(a) means any or all of–*
>
> *(i) a photograph of all or part of the person's head and shoulders;*
>
> *(ii) the person's fingerprints;*
>
> *(iii)an iris scan; and*
>
> *(b) includes a record, whether physical or electronic, of any of the above things.*

This *PIA on the collection and handling of biometric information* is specifically mandated in section 32 of the 2009 Act, which states:

> ***32. Ministry to undertake privacy impact assessment***
>
> *(1) The Ministry must complete a privacy impact assessment in respect of the collection and handling of biometric information under this Act to—*

---

[10] *Performance Audit Report, Department of Labour: Management of immigration identity fraud*. Wellington: Controller and Auditor-General, June 2007. ISBN 0-478-18188-4. Available at http://www.oag.govt.nz/2007/immigration/docs/oag-immigration.pdf/view?searchterm=immigration

[11] *Guiding Principles for the use of Biometric Technologies for Government Agencies*, Cross Government Biometrics Working Group, Wellington, 2009

(a) identify the potential effects that the Act may have on personal privacy; and

(b) examine how any detrimental effects on privacy might be lessened.

(2) The Ministry must consult the Privacy Commissioner—

(a) on the terms of reference developed for the assessment; and

(b) when completing the assessment.

(3) The Ministry must review its privacy impact assessment if changes are made to this Act, regulations made under it, or operational policy in respect of the collection or handling of biometric information and, if the review establishes that new or increased privacy impacts have resulted from the changes, must—

(a) amend or replace the privacy impact assessment; and

(b) consult the Privacy Commissioner on the amended or replacement assessment.

(4) The Ministry must ensure the current privacy impact assessment is—

(a) available on the Ministry's Internet site; and

(b) available or readily obtainable for inspection, free of charge, at—

(i) offices of the Ministry; and

(ii) New Zealand government offices overseas that deals with immigration matters.

(5) Nothing in subsection (4) requires the making available of information that could properly be withheld in accordance with the provisions of the Official Information Act 1982, were a request to be made for the information under that Act.

The original PIA covering the Ministry's use of biometric information was produced in 2010. Updates have been made since that time to accommodate changes to the way the Ministry collects uses and stores biometric information. The most recent published version of the PIA from August 2012 is now replaced by this updated PIA 2016. The PIA 2016 continues to comply with the mandated requirements of section 32 of the 2009 Immigration Act.

Biometric provisions are contained within the 2009 Immigration Act, which mirror the immigration information life cycle. Specifically, these are referenced in the summary of relevant sections of the Immigration Act in Table 1.

The powers to collect and handle biometric information come into force by Order in Council. Implementation details have been developed in consultation with the Ministry of Justice, the Department of Internal Affairs and the Office of the Privacy Commissioner[12]. Assessments of the initiatives that will use these powers are documented in the appendices attached.

[12] *Cabinet Policy Committee POL (06) 380, 17 November 2006*, p.44, para 291. Available at http://www.dol.govt.nz/PDFs/immigration-act-review-cabinet-paper.pdf

1.2 Privacy governance within the Ministry

The Ministry's management of privacy issues is decentralised with responsibility devolved to each business unit which has 'ownership' of personal information. This delegated model is managed within a Ministry-wide framework of information management, which involves using information effectively to achieve the Ministry's full range of organisational objectives, including: security; reporting; response; and consistent communication with customers. Governance is overseen by the Safety and Security Governance Committee.

The Safety and Security Governance Committee provides strategic direction and leadership of privacy and ensures coordination with the Safety and Security programmes of work. A Privacy Steering Group has been established to support the development and implementation of the privacy programme of work. The Steering Group reports to the Safety and Security Governance Committee.

The Privacy Steering Group brings together key cross Ministerial stakeholders reflecting the 'mixed' central and delivery-based nature of privacy issues. The Group provides Ministry oversight for privacy, including overseeing the development of MBIE-wide policies and standard procedures, and the privacy framework.

The Ministry is required[13] to have (a) nominated privacy officer(s) whose responsibilities include the encouragement of, and ensuring compliance with, the Privacy Act 1993. The Chief Legal Adviser is the Chief Privacy Officer. The Chief Privacy Officer is responsible for developing the cross Ministerial strategic direction for privacy management, enhancing privacy practices and for providing advice and assistance on privacy matters. The role is supported by a Principal Adviser, Privacy role. This role leads the development and implementation of a privacy programme of work across the Ministry.

A Privacy Working Group is also included in the governance arrangements. Its role is to support the Privacy Steering Group and assist the privacy programme to identify and address problems and emerging issues through consultation and information sharing. It will address issues at a technical level rather than a policy level.

The Privacy Steering Group has documented a Privacy Programme Strategy of work. This outlines responsibilities of the devolved privacy governance bodies across the Ministry and is aligned with the Safety and Security Governance Committee. The purpose of the programme is to improve the capability, consistency and maturity across the Ministry and in accordance with the introduction of the Government Chief Privacy Office in March 2013.

The Ministry has an internal Privacy Policy[14] which is reviewed and updated, annually. It is applicable to all Ministry staff, contractors, temporary staff and third parties. It explains how the Ministry complies with the requirements of the

[13] Section 23 Privacy Act 1993.

[14] http://thelink/how/Documents/privacy-policy.pdf

Privacy Act 1993 in relation to the collection, storage, use and disclosure of personal information that is collected and held by the Ministry. It deals with standardised procedures and guidelines across the Ministry for:

- Requests for personal information.
- Correction of personal information.
- Complaints about personal information management.
- Event or incident management.
- Third party arrangements.
- Information sharing.
- Information matching.
- New proposals involving personal information.

The policy provides links to explicit process instructions, tools and templates where required. Links to Privacy Impact Assessment templates are included for assessing new proposals impacting personal information or revisiting privacy impact assessments of existing initiatives such as the implementation of the biometric provisions.

An introductory 'Guide to Privacy' e-learning course is available in the Ministry's Learning Management System. It is an integrated part of the on-boarding of new staff and they are automatically enrolled to complete the course within one month of commencing employment. It is also available to all existing staff and contractors. Legal Services is responsible for the delivery of the Ministerial training on the Privacy Act 1993 and the Official Information Act 1990. The target audience is all staff and managers who handle requests for information to be managed under these statutes. The learning objectives of the training focus on the management of requests for information.

Ministry Business units have people identified as privacy officers who are primarily involved in the management of privacy requests.

Other aspects of privacy compliance appear in other policies dealing with security, retention of information and other subjects.[15]

[15] Most, if not all, of those policies can be found at: http://thelink/about/Pages/mbie-privacy.aspx

2. IDENTIFICATION OF THE NATURE AND SCALE OF THE PROBLEM

The Ministry's objective is to ensure a consolidated and consistent best practice approach to the collection and handling of biometric information, which is principled and consistent with privacy and immigration law and with its national and international obligations and agreements.

2.1 Effective and efficient immigration system

The Auditor-General's report challenged the Ministry to improve management of identity information and to use biometrics more effectively. The Ministry is also expected to respond to the drive to improve efficiency and effectiveness throughout the public service.

The Ministry's 2014/2018 Statement of Intent[16] is committed to develop a long term immigration strategy that supports economic growth, to develop an immigration system that increases New Zealand's international competitiveness and to improve the quality of immigration services.

The use of biometric information is a key facilitator for service improvement and future cost management by enabling quicker processing of low risk immigration applications and improved assessment of higher risk applications. It also enables improved cooperation with partner agencies in the border sector, particularly where agencies act on the Ministry's behalf.

The use of biometric information within immigration will provide specific benefits to the government and the people of New Zealand. It will:

- Permit faster and more effective processing of immigration applications;
- Enable the early identification and prevention of immigration and identity fraud;
- Facilitate immigration processing at the border, including automation and improved border security;
- Strengthen the Ministry's ability to protect people from identity theft and the misuse of their travel documents and/or visas by others;
- Provide authoritative identity information about non-New Zealand citizens for wider government use.

The Regulatory Impact Assessment (RIA) submitted to the Treasury in 2006 on the review of the Immigration Act 1987 noted that the use of a biometric system will allow the Ministry to focus verification work on potential risks rather than spread verification resources across all applicants.

---

[16] *Ministry of Business, Innovation of Employment Statement of Intent 2014-18*. http://thelink/news/Documents/2014-2018-SOI.pdf

The use of biometric information is seen as possessing advantages in identity assurance because it is unique to individuals and cannot be easily shared or stolen. In May 2016, the Ministry will implement the capability to match biometric information with biographic information through the Identity Matching Engine (IDme) which is part of the Immigration Global Management System.[17] This will provide further assurance of individuals' identity. International experience has demonstrated that biometric processes can be introduced at the border to improve both passenger facilitation and enhance border security.

2.2 Identity fraud

Identity fraud was mentioned as a significant driver for the introduction of biometrics in the discussion document prepared for public consultation during the Review of the Immigration Act.[18] Reliable information about the cost and extent of identity fraud in New Zealand, however, is limited.[19]

2. 2.1 Cost

The best estimates rely on scaling down figures from comparable countries. For example, a recent article[20] on the subject quoted annual figures for identity fraud of $A1.1 billion in Australia, £1.2 billion in Britain and $US8 billion in the United States. Proportionally to Australia, that would make New Zealand's identity fraud level around $180 million.[21]

Another recent article on the KPMG Fraud Barometer[22] claimed a total of $1.7 billion was defrauded in New Zealand between January and June 2012. The barometer (as is true of criminal law here) does not distinguish identity fraud from other frauds, but crimes such as fraudulently obtaining loans often involve identity fraud.

Recent statistics from the United States suggest that approximately 278,000 complaints were made to the Consumer Sentinel Network in 2009 of identity. More recent report from Javelin Strategies on the extent of identity fraud in the United States show 2013 as the second worst year for identity fraud in their

---

[17] IDme and Immigration Global Management System are described in detail in Section 5, Process and Information Flows

[18] *Immigration Act review Discussion Paper*. 2006. Section 11.

http://www.dol.govt.nz/PDFs/immigration-act-review-cabinet-paper.pdf

[19] *Am I Who I Say I Am? A Systems Analysis into Identity Fraud in New Zealand*, by Mireille Johnson. Thesis submitted to Auckland University of Technology for the degree of Master of Philosophy. 2009. Institute of Public Policy. http://aut.researchgateway.ac.nz/bitstream/10292/828/3/JohnsonM.pdf

[20] *Identity fraud takes new twists: academic*, by Nick Krause. 8 July 2010.

http://www.stuff.co.nz/business/3895503/Identity-fraud-takes-new-twists-academic

[21] General figures on economies from *CIA World Fact Book.*

https://www.cia.gov/library/publications/the-world-factbook/

[22] *Fraud Barometer – December 2012*. New Zealand: KPMG, December 2012.

http://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Fraud-barometer/Pages/edition-7.aspx

annual series with 13.1 million Americans victims of the crime although the total cost of that crime had dropped.[23]

2. 2.2 Extent

The Ministry currently has limited information on the full extent of identity fraud in the immigration system. However it can get a sense of the potential size of the problem by looking at the experience of its partners when they introduced biometrics into their immigration and border processes.

Immigration agencies in the United Kingdom, Australia, Canada and the United States found that the introduction of biometrics significantly increased the number of immigration cases identified involving undeclared criminal records, failed asylum claims, immigration alerts, unsolved crimes, missing persons and identity fraud.

The Ministry recently obtained updated quantitative data regarding the biometric matching for onshore claims for refugee status. In 2015, a total of 20% of all cases checked using a combination of biometric and biographic matching revealed identity fraud, immigration fraud or concealed criminality. This compares to a total of 10% of all cases in 2010. These represent cases the Ministry would not have found using traditional biographic checking processes.

---

[23]- https://www.javelinstrategy.com/news/1467/92/A-New-Identity-Fraud-Victim-Every-Two-Seconds-in-2013-According-to-Latest-Javelin-Strategy-Research-Study/d,pressRoomDetail

3. ASSESSMENT OF EXISTING IDENTITY OPTIONS

The Auditor-General's report on identity management highlighted the inadequacy of systems within the Ministry at that time. Those systems could not ensure that refugee status is granted only to genuine claimants nor could the Ministry associate each person with one consistent identity used across all immigration transactions.

The use of biometrics can be privacy-enhancing. This is because they can replace the need to collect a wide range of other personal information from people and can provide secure barriers to unauthorised access to personal information. In other circumstances, biometrics can be privacy-intrusive because of the nature of the information collected.

3.1 Using biographic information only

If the Ministry was to use biographic information only, it would remain overly reliant on identity documentation, names and date of birth in order to identify people. This is information that can be changed easily by those determined to use personal information for fraudulent purposes. The amount of information required from people would also be greatly increased. The type of information and the amount of detail about each type of information would become increasingly privacy intrusive and susceptible to fraud.

Increased amounts of biographic information could potentially be easily useable, both by the Ministry and by other agencies, for uses unrelated to the immigration purposes for which it was collected. In contrast, biometric information requires specialised equipment and training in order to be useful. This provides a limitation to its wider use.

Extra biographic information would be less effective than biometric information and potentially increase the chance of mis-identification. It would be inadequate and ineffective to try to obtain further biographic information from people who arrive in New Zealand with no travel documents or with invalid, altered, counterfeit or other suspicious travel documents or identities.

Biographic information also has limitations when dealing with people with similar or identical names and dates of birth. This difficulty often occurs, or is increased, when information has to be translated into English or to the Western calendar.[24]

3.2 Interviews

Interviews are currently used in the assessment process but are not considered an effective alternative to biometrics. The one major disadvantage of reliance on interviews is that they are very expensive in time and resources for everyone involved. They cannot be used at time sensitive events such as check in or the

[24] Many cultures do not use the Western calendar, and other cultures do not necessarily place the same emphasis on date of birth as do the Ministry's records systems. Transliteration of foreign-language names into English can be inconsistent.

border to facilitate the speedy processing of low risk travellers. They would be excessive for tourists and most other temporary visas.

Neither of the above solutions amount to a practical or efficient solution for the dual purpose of effective, robust immigration processing and identity assurance.

3.3 Document analysis and verification

Analysis of passports, identity cards and social footprint documents (such as bank statements and birth certificates) is a key part of immigration work. This will remain the case in the future.

Document analysis by itself, however, can never be fully relied upon to provide confidence in a person's identity. The Ministry processes applications from every part of the globe, all with their own standards around document production. Validation of these documents with the government that issued them is often impossible.

Document analysis is an important part of evidence of identity assessment, but it will always be limited in the level of identity confidence it can provide to the Ministry and other agencies that rely on Immigration for authoritative identity information and identity verification services.

3.4 Combination of interview, analysis, biographic and biometric information

Reliance on any one of the above options alone is not acceptable. Biographic information only is not a sustainable alternative, interviewing is an expensive and time consuming option and the Ministry cannot rely solely on the analysis of documentation. The Ministry continues progressing towards increased use of biometric information in conjunction with existing options for identity assurance.

Interviews and analysis of documentation further assist to clarify in more complex or uncertain cases, where biographic identity information provided is questionable. This combination of approaches will continue to be utilised by INZ as part of the range of tools to assist with establishing an accurate identity.

4. SCOPE OF THE PRIVACY IMPACT ASSESSMENT

The scope of this PIA 2016 extends to the review and update of the previous version (PIA 2012), to ensure the ongoing assessment of the Ministry's current and future practices with respect to the collection and handling of biometric information, is accurate and up to date.

The PIA first produced in 2010, and subsequently updated in 2012 met the requirements of Section 32 of the Immigration Act 2009 and established a sound basis for the use and handling of biometric information, which this PIA has subsequently built on.

A PIA is a systematic process for evaluating a proposal in terms of its impact upon privacy. It is intended to:

- identify the potential impacts that any proposal may have on a person's privacy;
- examine how those detrimental effects upon privacy might be overcome;
- ensure that new projects comply with the information privacy principles in the Privacy Act 1993.

A PIA does not remove risks; it exposes them and provides recommendations for mitigation. It is the Ministry's responsibility to manage the regulatory development and operational policy associated with the highlighted risks and to implement appropriate mitigations.

The chapters in this PIA have been updated to reflect relevant changes since the PIA 2012 was published, and to reflect the Ministry's proposed practices with respect to the collection and handling of biometric information as part of the changing management processes and systems as a result of the Vision 2015 Programme. This includes the proposed final state implementation of the Immigration Global Management Systems (IGMS) as understood at the time of writing this document.

The Vision 2015 Programme significantly enhances the Ministry's ability to use biometric information and will enhance the potential of biometric information as part of an efficient immigration system. IGMS will provide the enabling technology to increase confidence in accurate identity information. It is integral to the government's goals for immigration to have policies, systems and processes in place that make New Zealand an attractive place to visit, work and live[25]. The Ministry is responsible for facilitating the arrival of migrants, students, workers and tourists while preventing the entry of individuals with false identity credentials and those who may pose risks to the country.

[25] http://www.beehive.govt.nz/release/woodhouse-welcomes-positive-migration-figures

The Ministry is the authoritative source of identity information about non-New Zealanders[26] and its information is relied upon by other government agencies such as the Department of Internal Affairs when considering an applicant for New Zealand citizenship. This increases the need for accurate identification of people entering the country.

The Terms of Reference (TOR) submitted to the Office of the Privacy Commissioner outlined the purpose, objective and scope, arrangements, process and deliverables of this PIA. In the TOR, it was stated that an RIA would be required so that Cabinet would be satisfied the Ministry has appropriate procedures and processes in place.

Consistent with the guidelines developed by the Treasury, a preliminary impact and risk assessment (PIRA) was performed and concluded that a full RIA was not required. The Treasury agreed that the RIA requirements did not apply and that no further involvement was necessary, given that the policy work was completed during the Immigration Act review and was covered off in RIAs at that time. This remains the situation for the PIA 2016 update.

In this respect, Treasury was satisfied that no likely significant impact or risk was present and that the Ministry would be responsible for on-going quality assurance.

[26] See RealMe FAZ about identity verification for whole of government using Immigration NZ information for non-New Zealanders

5. PROCESS AND INFORMATION FLOWS

This section provides, as recommended by the Office of the Privacy Commissioner, the *Privacy Impact Assessment Toolkit,*[27] a description of the biometric information flows within the Ministry and externally. The Commissioner's Privacy Impact Assessment Toolkit describes as follows:

> "an information flow diagram – or a series of diagrams – can be a particularly clear and simple way of showing exactly where personal information is coming from, where it's going, how it's going to be used, and who it's going to be used by. This can help identify measures that can improve information security and reduce privacy risks".

The information flow diagram Figure 1 in section 5.2 shows the situation today and indicates the ideal state the Ministry is progressing towards when all the biometric provisions of the 2009 Act have been implemented. The information flow diagram is supported by descriptions of how biometric information is collected, circulates within the Ministry and is shared with external agencies. This captures what is known at the time of writing the 2016 PIA.

5.1 Approach to determine collection and use of biometric information

Internal insight into the use of biometric information

To determine how biometric information is collected and used across the Ministry, insight was gathered from:

- Existing policy and procedure manuals.
- Project plans and supporting documents for proposed initiatives.
- In person interviews with relevant internal personnel.

To inform an understanding of the use of biometric information in the Ministry interviews were conducted covering existing and proposed or planned aspects of biometric information handling. They took place in Wellington, Auckland and London, and involved one on one or group interviews. Recent interviews with the Vision 2015 Programme, Identity Services and Legal Services, have ensured the PIA 2016 is accurate and up to date.

External insight into the use of biometric information

Information sharing with third party agencies takes place with agencies that have a legitimate requirement to obtain and use biometric information. Discussions were therefore conducted with the relevant stakeholder agencies, including: the Department of Internal Affairs (DIA), New Zealand Customs Service (Customs),

[27] *Privacy Impact Assessment -Toolkit Part 2: How to do a Privacy Impact Assessment*, p.10. htttps://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/

New Zealand Police (Police), Ministry of Foreign Affairs and Trade (MFAT), New Zealand Transport Agency (NZTA), Ministry for Primary Industries (MPI) and Ministry of Justice (MoJ).

Interview checklists

Two indicative interview checklists were developed for internal use dependent upon whether the collection and handling of biometric data was current or proposed. Another set of interview questions was created for use with external agencies. These survey questions, intended for use in face to face interviews, were to help the interviewees understand what would be covered and to serve as a guide for the interviewers.

The checklists covered all of the information privacy principles in the Privacy Act 1993 and explored in detail the operational elements of them so that compliance could be assessed in current processes and future initiatives. They were submitted to the OPC in the TOR in relation to this PIA. Feedback from the OPC was received and the questionnaires amended accordingly.

Subsequent to the first publication of this PIA in 2010, this document has been updated to reflect changes in the Ministry, the immigration system and the wider environment within which immigration now operates. Additional interviews have been undertaken within the Ministry to reflect changes since 2012, including interviews with representatives from Identity Services, Immigration's Vision 2015 Programme and Legal Services.

Overview of the insights gathered

Table 3 shows the business units interviewed and their collection and handling of biometric information, either as a primary handler or where the biometric information is secondary to their purposes. With the updated PIA 2016 it has been confirmed that there has been no change in the business environments referred to below in terms of their status as primary or secondary handler. Some business unit titles may have changed and new business units have been included.

Table 3: Business units interviewed

Business unit (internal)	Known biometric collection and/or handling	Primary or secondary handler[28]
Settlement Services	• Biometric data not within scope	N/A
INZ Records Management	• Application Management System (AMS) • Enterprise Reporting and Data Management • Transfer of information to Archives NZ	Secondary
Strategic Programmes	• Biometric data not within scope	N/A
Border Operations	• Fingerprints	Primary

[28] Primary handlers are business units or agencies that collect and/or directly manage the biometric data. Secondary handlers are those entities that handle biometric data as part of their business function but biometric data is not a key component of their routine work – it is incidental to it.

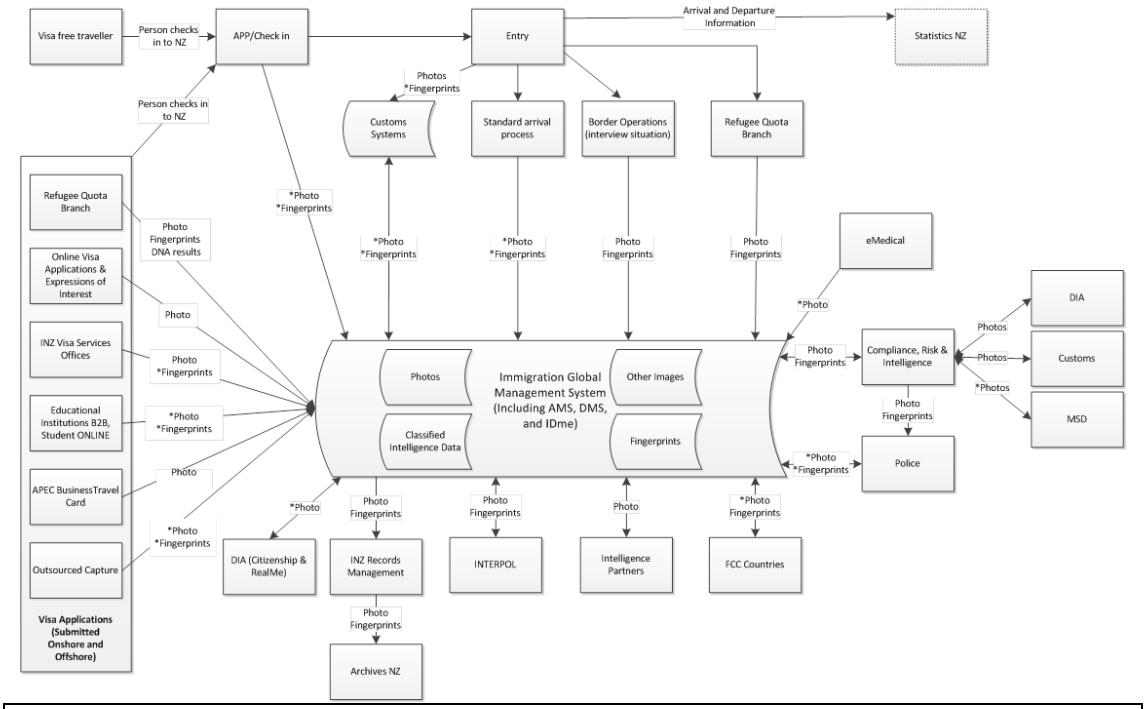
Business unit (internal)	Known biometric collection and/or handling	Primary or secondary handler[28]
	• Photographs (compared manually) • Ability to upload electronic photograph • Fingerprints taken by Police on behalf of the Ministry where required • Passport scans including upload of bio-page and e-chip photographs • Electronically check fingerprints against INZ, FCC and if necessary Interpol holdings	
Refugee Status Branch	• Fingerprints (checked with FCC partners) • Photographs (compared manually) • DNA results in some limited circumstances (not DNA samples) • Ability to upload electronic photograph • Passport scans including upload of bio-page and e-chip photographs	Primary
Compliance, Risk and Intelligence	• Fingerprints (may also be taken by Police on behalf of the Ministry where required) • Photographs (compared manually) • Ability to upload electronic photograph • Passport scans including upload of bio-page and e-chip photographs • ICE contains face images and other information from intelligence and enforcement sources	Secondary
Legal Services	• Biometric data not within scope other than to provide legal advice on Privacy and Immigration Acts	NA
Vision 2015 Programme	• Not collected for own purpose but may be accessed as part of development, testing and implementation of Vision 2015 operational processes and systems	Secondary
Refugee Quota Branch	• Fingerprints • Photographs (compared manually) • Ability to upload electronic photograph • DNA results data in some limited circumstances (not samples) • Passport scans including upload of bio-page and e-chip photographs • Photographs and fingerprints shared with FCC partners • Delegation of ink-set fingerprint capture to trusted agencies	Primary
Immigration Resolutions	• Not collected for own purposes but may be used	Secondary
Visa Services and Operations Support	• Collect facial images, scan passports and upload images	Secondary
Enterprise Reporting and Data Management	• A copy of the image database that is held at HP	Secondary
Identity Services	• Processing, sharing, matching and resolution of face biometrics (manual intervention)	Primary

Business unit (internal)	Known biometric collection and/or handling	Primary or secondary handler[28]
	• Fingerprints managed for matching against INZ, FCC and Interpol holdings	
Risk and Assurance	• Not collected for own purposes but may be accessed as part of the audit process	Secondary

5.2 How biometric information flows

Figure 1, outlines the flow of biometric information within the Ministry, and externally. Additionally, it indicates proposed information flows that are in plan but are not yet implemented; these are identified by an asterix next to the type of biometric information yet to be processed. This primarily relates to the collection and use of fingerprints in some Visa Application situations.

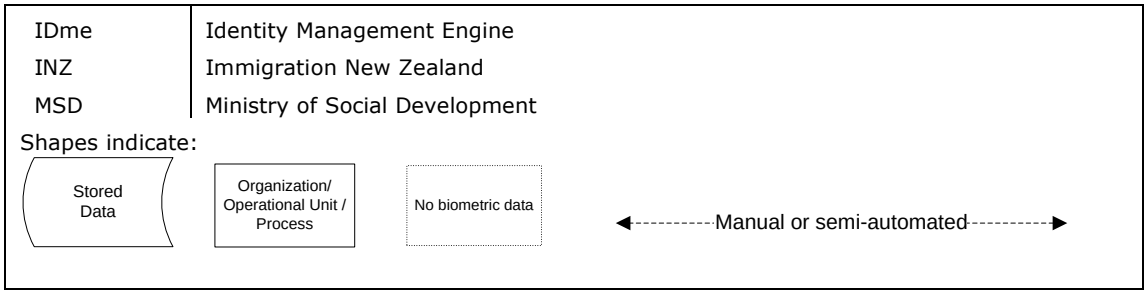
Figure 1: Vision 2015 Information Flow



Key

Abbreviations used in diagram:

*Fingerprints	Indicates that the capability to capture and use fingerprint biometrics will be extended to these areas in 2016
AMS	Application Management System (Immigration)
APEC	Asia Pacific Economic Cooperation
APP	Advance Passenger Processing
Branch	Ministry of Business, Innovation and Employment, Immigration Group Branch Office
DIA	Department of Internal Affairs
DMS	Document Management System
FCC	FCC Partner Conference (Australia, Canada, New Zealand, United Kingdom, United States of America)



5.2.1 Overview of the collection of biometric information

Biometric information is collected and used as a vital component of the identity establishment processes for people wishing to enter New Zealand. The biometric information collected is 'multi modal', i.e., it incorporates the collection of two or more types of biometric information. The Ministry collects both face and fingerprint biometrics. A photo image of a face is collected; an algorithm is applied which results in the photo being transformed to a biometric facial image. This enables measurement of the physical attributes of the face. The attributes are used to match for verification of identity. Fingerprint images are captured using finger-scan technology. All fingerprints have unique characteristics and patterns and these unique traits are used to match for verification of identity.

In addition, broader categories of personal information are collected: including biographic information such as Date of Birth, Names, National ID, Passport Numbers and Nationality information found in a passport. Other personal information collected may include: familial relationships; educational and work experience; New Zealand and foreign Police background checks; and medical information.

Biometric information processes are either manual or semi-automated. For example, hard copy photographs are scanned to provide a digital image. Passport photographs can be collected directly from passports. Increasingly automated processes are occurring when technical capabilities enable it. Business processes are changing so that simple, low-risk decisions can be made quickly and human expertise and judgement will be focussed on more complex situations. Business systems are being transformed in a phased approach to an integrated infrastructure including leading edge biometrics collection, matching and processing. The type of personal information being processed is not changing; it remains the core biographic details and biometric details identified above.

The Ministry is implementing new identity management processes and capabilities as part of the Vision 2015 Programme. The new identity processing model – IDme - will be implemented in 2016 (refer Appendix 12) as part of the Vision 2015 Programme. IDme is the identity matching engine that will enable the capture of identity information, such as biographic information from passport smart scanners, to biometrics such as facial images and fingerprints (including fingerprints collected in person from a subset of higher risk INZ clients). Personal information as described, in biographic and biometric categories will flow into the

IDme automated matching engine. The associated biographic and biometric information will be matched against all existing INZ identities or a new identity created if no existing one is identified.

Identities that produce inconsistent matching results (for example, matches with more than one existing INZ client); or which indicated possible fraud, will be managed by referral for manual identity resolution within INZ by new specialist roles. The roles have received specialist identity skills training to enable the incumbents to complete identity resolution tasks, including biometric searches. The role of Fingerprint Analyst will continue to be performed by the NZ Police under the Memorandum of Understanding (MOU) recently signed by the Ministry and NZ Police. Visa Services staff will manage less complex identity resolution cases that the IDme system cannot resolve.

With the introduction of the IDme identity matching engine, INZ is transitioning away from managing and matching biometric information manually, however this is a gradual transition, and will always require human intervention for the matches that automated processes are unable to complete successfully.

Further automation is intended as INZ is implementing an automated data sharing capability with Five Country Conference (FCC) Protocol partners in line with the existing data sharing agreements[29]. The main component is the development of a real time data sharing platform ("Secure Real Time Platform" or SRTP), which can be used to securely share data of fingerprint match requests and responses with FCC partners. This capability is in development and planned for 2016 implementation, (refer to updated Appendix 6).

FCC fingerprint matching is a well-tuned and refined process that has been in place since April 2011, covered by the FCC Partner Agreements for Sharing (refer Appendix 5). Responding to an FCC fingerprint matching request does however require the responding partner to manually process the response and therefore restricts the volume of fingerprint processing. Fingerprint biometric processing has been done by the NZ Police on the Ministry's behalf. The expertise of the NZ Police will continue to be relied upon by the Ministry for the resolution of fingerprint matching cases that are unable to be automatically matched by IDme and confirmation of automated matches.

In the majority of cases, the implementation of SRTP will enable requests to be responded to automatically by the responding country partner, without the need for manual intervention. INZ staff will be provided with access to view the response results of the matching and will not be required to manually handle all data relevant to the request and / or response.

The combination of the IDme and SRTP capabilities will allow for easier and quicker detection of identity fraud or equally, establishing identities with a high

[29] http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/fccqa.htm

level of confidence for the majority of people. Without high confidence in identity, watch lists and external data matching cannot work reliably.

Biometric information is and will be collected as follows.

Visa applications submitted onshore and offshore

- Visa applications can be submitted onshore and offshore directly to the Ministry, online or through an approved outsourced lodgement agent.
- Foreign nationals wishing to enter the country either apply for a visa before they leave or apply for entry on arrival if entitled to visa waiver status.
- People who apply for a visa are required to provide a 'passport grade' photograph. That requirement may be met through the photograph on the paper based application form, an electronic image with an online application, the biographic page on a passport or in an e-chip passport.
- Online visa applications enable the collection of an electronic image also received through approved Educational Institutions B2B and Student ONLINE services.
- Applications are also received through the APEC Business Travel Card scheme. These are accessed through the APEC system, which may make a photo of the applicant available. That photo is not transferred to AMS. Where the applicant is from a non-visa waiver country and their application is approved, a visa record is created in AMS.
- The outsourced MFAT post in Ankara has restricted and limited access to AMS including biometric information available through the Identity Report software application. Ankara also has a passport scanner.
- Application processing (including paper photos) and basic data entry is done by third party providers (outsourced capture) in, for example, Philippines, China, Russia and India. The business owner of this process is General Manager, Visa Services.
- Quota refugees are required to provide photographs and fingerprints and occasionally DNA to substantiate familial relationships with visa applications. DNA testing is done by an external contractor. The Ministry keeps only the DNA results, not the physical samples. Bone maturity tests to substantiate a claimed age are sometimes required. This is done by x ray so no physical samples are involved.
- With the exception of Refugee Quota Branch, only photos are currently collected for all visa applications submitted onshore and offshore. The capability to collect fingerprints will be implemented in 2016 as a result of IDme functionality being implemented for Visa Services, Educational Institutions, Student ONLINE and some approved outsourced capture agents. It is not anticipated that APEC Business Travel Card scheme or online visa applications and expressions of interest will have fingerprint capability. They will continue to collect photos only.

Border systems collection

- Customs and Standard Arrival Processes support border systems in various ways to collect biographic and biometric information.
- There are passport readers at airports to capture information from the Visual Inspection Zone and the Machine Readable Zone, as well as any microchip in the passport. The physical photo in the Visual Inspection Zone is always collected and stored by the reader for all passports it scans. If it is an e-chip passport, the electronic photo is also collected along with other data that may be included in the e-chip.
- From November 2011 all immigration locations began using a smart passport reader, enabling the capture of the photograph. New Zealand citizens arriving in New Zealand will be required to provide an in person photograph which may continue to be kept after the identity is confirmed.
- New Zealand citizens arriving in New Zealand and who opt to use the SmartGate readers at international airports are required to provide an in person photograph to enable face matching.
- Australian, UK, US and Canadian e-passport holders aged 12 and over arriving in or departing from New Zealand and who opt to use the SmartGate readers at international airports are required to provide an in person photograph to enable face matching.
- SmartGate services offered by Customs and at International Airports in New Zealand (as well as the other four countries in the FCC), have the potential to collect fingerprints but these are currently not actively collected.
- Foreign nationals arriving in and departing from New Zealand will be required – where requested - to provide an in person photograph and/or fingerprints and the photograph on the biographic page of their passport or in an e-chip passport.
- Foreign nationals suspected of breaching, or intending to breach the Immigration Act 2009 will be required to provide an in person photograph and/or fingerprints where requested.
- Immigration officers may require biometric information from foreign nationals to determine compliance with the Immigration Act 2009 under the conditions described in section 288.
- Border and onshore asylum claimants may have their claim determined on the basis of information available if they fail to provide photographs and fingerprints.
- Refugee Status Branch collects live fingerprints from people; these fingerprints are processed – and any matches resolved – in a dedicated immigration system provided by New Zealand Police. Limited automated matching of fingerprints is carried out by the Police on behalf of the Ministry. All matches indicating identity fraud are confirmed by a fingerprint expert before any action is taken.
- NZ Police takes fingerprints in some cases on behalf of Compliance, Risk and Intelligence using ink on paper, which is subsequently scanned for entry into the dedicated immigration database provided by the Police.

- The INZ fingerprint database currently stored on behalf of INZ by the New Zealand Police will transition to the Ministry in 2016. Automated fingerprint matching functionality and storage will be part of a new Identity Management Engine (IDme), with the exception of fingerprints requiring specialist analysis and resolution, which will continue to be performed by the Police on behalf of the Ministry.

Other collection activities

- eMedical collect photos which may be transferred to IGMS in future.
- Some applications will contain fingerprints because Police check reports from other countries may contain them. These fingerprints are not currently used by the Ministry but are retained.

Collection will be done electronically wherever possible. For example:

- Applications are increasingly achieved through an online process with the introduction of IGMS – that process may use trusted digital photograph intermediaries / outsourcers to collect biometric information.
- Arrival and departure information is collected electronically through border systems (Advance Passenger Processing, NZ Customs, overseas partner agency systems or airline Systems).
- Fingerprints are collected electronically using scanners – this will include third party visa application centres that collect information on the Ministry's behalf.
- Future IDme capability will extend to the implementation of IDme Enrolment Stations onsite for Border Officers, Refugee Officers, Compliance and Fraud Officers and Identity Services Analyst. This will assist with the time pressure of border facilitation.

All information will be kept and handled securely according to the Ministry's ICT security procedures.[30]

Biometric information will be collected from a wider range of people with the implementation of IDme. Direct electronic collection will be increasingly used in place of hardcopy collection.

Once the Ministry has collected biometric information, it is stored in various places depending on the status of the application, the format in which it is held and the branches that have a business need for the information. The Ministry is gradually transitioning to store information in fewer systems.

Biometric information is and will be stored as follows:

- AMS is the primary storage mechanism for the electronic information required to manage immigration case files. It sits within the Immigration Global Management System.

---

[30] MBIE ICT Information Security Policy
http://thelink/how/Lists/Security%20Policy/policies.aspx?RootFolder=%2Fhow%2FLists%2FSecurity%20Policy&

  - AMS is mirrored on separate servers between Auckland and Wellington for business continuity planning. This is part of the planning to help ensure 24/7 operation.
  - AMS records are kept indefinitely although some may become hidden from view. Biometric information is currently retained for 50 years from date of capture. This is to enable familial relationships and other linkages between people to remain available.
  - Each person is assigned a unique number within AMS, and all their applications are tied to that unique person number.
- Digital photographs and scanned copies of other images and information, such as passport biographic pages are stored in a separate server (AMS image database, IGMS, and the Document Management System). Photographs are copied from that server each night to the Enterprise Data Warehouse.
- Information from the passport readers is initially stored on the computer to which each is attached and transferred into the image database in IGMS. The introduction of smart passport readers in November 2011 provided an automated mechanism for capturing photographs directly from the passport.
- The introduction of IDme will allow the Ministry to store and manage both facial and fingerprint biometric information. It is a specialised biometrics identity management system that will associate all visa applications and client interactions with each individual case. Biometric images used for matching will be retained in IDme and the Automated Fingerprint Indexing System (AFIS). Images of faces taken from passports, digital photographs in passports, and other sources will be stored in IDme. Passport test results and scans of documents will be stored in the Document Management System.
- All immigration fingerprints, whether taken by NZ Police or the Ministry will eventually be stored within the IGMS environment in a fingerprint database. NZ Police will have the ability to access the IDme system for resolution requirements through Ministry equipment. Currently, INZ fingerprints are stored in AFIS. This is an INZ only database housed by the NZ Police. This data may be migrated to the new NZ Police database, Automated Biometric Indexing System (ABIS), until the IDme database is implemented in 2016.
- Compliance Risk and Intelligence holds biometric information acquired from law enforcement partners.
- Information that requires separation, such as that in the Intelligence system, may remain outside the central immigration system or could potentially become a segregated database with IGMS in the future.
- Refugee Quota Branch has a separate database for children's information.
- Fingerprints of high risk cases are stored in the dedicated immigration fingerprint database which is transitioning from NZ Police to the Ministry.
- NZ Customs System is linked to transfer information relating to immigration collected by NZ Customs on behalf of the Ministry. This connection may be extended to include biometric information in future.

- It is also possible that a direct link may be made with the Department of Internal Affairs records of Citizenship at some future time, as there is an obligation to delete biometrics of NZ citizens once citizenship has been confirmed in the immigration process.

Back-up and recovery environments are in place for each of the major systems. These have been implemented in accordance with the Ministry's ICT Security Policy and standards which also require the consideration of the Privacy Act principles for the secure and safe handling of personal information.

As many immigration processes are manual and paper based, there are separate storage arrangements for those records. Typically, paper applications are kept at the branch where the application is lodged.

For paper records only, the status remains as:

- Paper based biometric information is kept in the application files and stored at the processing business unit until the application is closed (completed or refused).
- Residence applications are kept for 20 years (approved and declined) and then sent to Archives New Zealand for permanent retention.
- Returning resident visas issued under the Immigration Act 1987 are kept for 10 years.

Temporary visit applications are kept for 2 years unless subject to an appeal, compliance order, Ombudsmen's investigation or similar restriction. IGMS is expected to essentially eliminate anything other than short term storage of paper based applications. All paper based applications will be scanned into electronic form and kept in the Document Management System within IGMS.

Retention of Government records is subject to the Public Records Act 2005. The Ministry has applied to Archives New Zealand for a Public Records Act authority to cover the Ministry as a whole. INZ is required to keep summary data and retention of biometrics (face and fingerprints) for a period of 50 years from date of capture.

The current FCC Protocol stipulates that personal information received from a partner where permissible may be retained as part of the Clients Personal Record for a maximum of 10 years from receipt. Information received from FCC partners may include: biographic information details about immigration history; movements; face images; and passport images. Fingerprints are sent for matching but are discarded when the matching process is complete.

The 2009 Act refers to the 'collection and handling' of biometric information. The term 'handle' is used here to cover uses that do not involve disclosure to other agencies. In some cases, another agency acts as an agent for the Ministry, such as when Police experts provide advice on fingerprint matching.

The basic premise behind the design of the immigration system is that all immigration information will be collected, stored and accessed through a central system.

Some extensions to the current information sharing activities with the FCC partners are planned.[31]

Biometric information is handled internally as follows:

- The immigration management processes coupled with the capability of IGMS will make it possible for authorised Ministry roles (such as Immigration Officers, Identity Service Officers) to see all available identity information from the case management, including biometric information and matching results and scans of any document related to an application such as passport scans. Quota refugees arriving are compared with their photograph already on record.
- Refugee Status Branch uses photographs and fingerprints to establish the identity of people who claim asylum on arrival in New Zealand.
- Compliance, Border and Investigations may use photographs and fingerprints to verify the identity and/or background of particular high risk people they are processing.
- The Resolutions Team handles statutory complaints, revocations and deportations. They will have access to all information held about an individual within the IGMS environment.
- Compliance, Risk and Intelligence has access to IGMS, which contains images of faces.
- Biometric information transfers between ICE and the photo database are done by intelligence officers only.
- With the introduction of IDme, the Ministry will continue to transition away from managing and matching biometric information manually. Matching will always require some manual interventions for the matches that are complex and unable to be completed successfully in an automated manner.
- Identities that produce inconsistent matching results (for example, matches with more than one existing INZ client); or which indicated possible fraud, will be managed by referral for manual identity resolution within INZ by new specialist roles.
- Identities will not be established simply on the basis of biometric matching. Advanced biographic matching will also be part of the identity verification process. If the automated matching results in a no match a new client will be created. If the data or biometrics is not of sufficient quality for matching they will not be used.
- NZ Police will continue to handle biometric information when providing expertise for the resolution of fingerprint matching cases that are unable to be automatically matched by IDme and confirmation of automated matches.

[31] In addition, the 2009 Act allows for more authorised information matching programmes than the five currently operating. See the Privacy Commissioner's website for details about the operating authorised information matching programmes – http://privacy.org.nz/operating-programmes/.

- The Identity Report uses photographs and other scanned information from the image server and biographic information from AMS to provide an integrated view of the identity information to immigration officers.

Biometric information is disclosed with and will be shared as follows:

- Five Country Conference (FCC) partners (fingerprints via the FCC Protocol and photographs where required during specific requirements). Disclosure will move towards an automated and real time secure platform (known as Secure Real Time Platform [SRTP], refer Appendix 6).
- The process of sharing biographic and biometric information assessed in Appendix 5 for the FCC Protocol covering manual sharing of biometric data will be increasingly automated with the first implementation of SRTP which is assessed in Appendix 6. No changes to the FCC sharing agreements are required as the biometric provisions that are met do not change the process and system used to share biometric information enable the increased automation.
- The FCC exchanges will be extended to include information about criminal deportees and formal intelligence exchanges of information.
- In addition, the number of fingerprints sent by any one country to another will be increased. In order to respond to increased volume, the processing is moving increasingly to an automated SRTP model.
- Checks on a broader range of case types will be implemented such as high risk visa applications or trusted traveller enrolments.
- Law enforcement agencies and agencies with enforcement powers, including Police, Interpol, Security Intelligence Service, Customs, Justice, Corrections and Ministry for Primary Industries, may also include exchanges. Typically for the purpose of enabling the Ministry to check identity information, character and immigration status of individuals.

All information will be kept and handled securely according to the Ministry's ICT Information Security Policy and standards in accordance with Government ICT Strategy and Action Plan.

6. ANALYSIS OF GUIDING PRINCIPLES

The Cross Government Biometrics Group (CGBG), of which the Ministry is a member, developed guiding principles for the use of biometric technologies, published in April 2009.[32] It is intended for use by government agencies to inform decision making when considering biometric technologies for identity related business purposes. The guiding principles are expressed in a general way so that they can be useful for all agencies to consider when researching, planning and deploying biometric technologies for identity purposes. They encompass the following considerations:

1. Justification for the use of biometric technologies.
2. Lawful and appropriately authorised use.
3. Collaboration with other agencies.
4. Impact on end users (those who will interact with the systems and processes).
5. Use of biometric formats appropriate to the situation.
6. Relevant international obligations.
7. Need for stewardship over systems and processes.

The guiding principles are supported by a set of implementation principles (see chapter 7) that the CGBG have defined for operational considerations. By taking these guidance and implementation principles into consideration, the agencies should be able to ensure that biometric technologies are used only where necessary and are designed and implemented to meet specific business requirements. This will assist to mitigate potential risks such as:

- Missing opportunities for collaboration with other agencies through lack of information and coordination.
- Lack of interoperability between agencies.
- Failure to adequately safeguard personal information.
- Escalating public concerns about privacy.

At the time of PIA 2016 update, no privacy breaches or complaints relative to the use of biometric information have been identified by the Ministry or raised by the public.

6.1 Justification for the use of biometric technologies

The first guiding principle from the CGBG requires that agencies need to justify their decision to use biometric technologies for identity purposes. Specifically, they are advised to 'evaluate the need to use biometric technologies' and 'ensure that it is the most appropriate and cost effective solution'. This was undertaken as part of the public consultation and review process that preceded the passage of the Immigration Act 2009. The proposed use of biometrics was discussed in

[32] *Guiding Principles for the Use of Biometric Technologies for Government Agencies*. Wellington: Department of Internal Affairs, April 2009. ISBN 978-0-478-29487-3

section 11 of the Immigration Act review discussion paper.[33] The Ministry received nearly 4,000 responses to that discussion paper, of which 102 related to the biometrics provisions.[34]

The final proposals relating to biometric collection and handling for immigration purposes were submitted to Cabinet for approval. The detailed technical recommendations described when biometric information could be collected from both non-citizens and citizens, how that information could be used and how it would be disposed of when no longer required.
Cabinet agreed that the Bill (now the 2009 Act) would enable:[35]

- *The following biometric information to be required from non-citizens for immediate use and storage for future use:*
  - *photographs*
  - *fingerprints*
  - *iris scans*
- *Photographic biometric information to be required from people arriving in New Zealand as citizens for immediate use*.

6.2 The use of biometric technologies must be lawful and appropriately authorised

The second guiding principle requires that, when government agencies use biometric technologies for identity purposes, they do so consistent with their enabling legislation and in a manner that is fully compliant with New Zealand laws. It draws particular attention to compliance with the Privacy Act 1993 and the New Zealand Bill of Rights Act 1990. The Ministry's commitment to this principle is demonstrated in the ongoing PIA reviews and stated desire to incorporate privacy by design into the implementation of IGMS and Vision 2015. This assists with addressing the Governance risks identified in Table 2 - G3 (unnecessary expense incurred be causes systems are not designed to include privacy considerations from the beginning) and G7 (the PIA is not reviewed, augmented or kept current, contravening Section 32 of the Immigration Act 2009),

6.2.1 Privacy Act 1993

The following table provides an overview of the Privacy Principles of the Privacy Act 1993 in relation to the Risks and Mitigations identified in Table 2.

---

[33] *Immigration Act Review: Discussion paper*. Wellington: Department of Labour, April 2006. Available at http://www.dol.govt.nz/PDFs/immigration-act-review-discussion-doc.pdf

[34] A summary of those responses is available at http://www.dol.govt.nz/actreview/index.asp

[35] *Cabinet Policy Committee POL (06) 380, 17 November 2006*.
Available at http://www.dol.govt.nz/PDFs/immigration-act-review-cabinet-paper.pdf

Table 4: Privacy principles and risks and mitigations identified

12 Privacy Principles	Identified Risks and Mitigations
1 Purpose of collection	H1 Unnecessary collection H2 Arbitrary collection
2 Source of personal information collected	H3 Indirect collection
3 Collection of information from individual	H4 Uninformed collection
4 Manner of collection	H2 Arbitrary collection H5 Unfair or intrusive collection
5 Storage and security	G4 Authorisation to access too wide G5 Inadequate sharing and collaboration G6 Inadequate use of agents S1 Loss of biometric information S2 Unauthorised access (use, disclosure, edit) S3 Inadequate safeguards
6 Access to information	H6 Non-New Zealand citizen access and correction rights H7 Ability to respond to New Zealand citizen access and correction requests
7 Correction of information	H6 Non-New Zealand citizen access and correction rights H7 Ability to respond to New Zealand citizen access and correction requests
8 Accuracy of information	H8 Incorrect information associated H9 Incorrect decision making
9 Retention of information	H10 Unnecessary collection H10 Information retained longer than needed
10 Purpose limitations	H11 Used for non-immigration purposes S2 Unauthorised access (use)
11 Disclosure limitations	H12 Disclosure unreasonable S2 Unauthorised access (disclosure)
12 Unique identifiers	H13 Unnecessary assignment of identifiers H14 Widespread use of identifiers

Principle 1 – Purpose of collection of personal information

This principle provides that personal information should not be collected by the Ministry unless it is collected for a lawful purpose connected with a function or activity of the Ministry and is necessary for that purpose.

It is also generally accepted that situations where people have no choice about whether to provide personal information are more privacy intrusive than where there is real choice. In this case, the Ministry has statutory authority for the mandatory collection of biometric information under the 2009 Act.

Whether specific implementations are in accord with that statutory authority and the information is necessary in order for the Ministry to carry out its responsibilities under the 2009 Act is a matter to be taken into consideration and is addressed by H1 – risk and mitigation for unnecessary collection of information.

Principle 2 – Source of personal information

This principle requires that the Ministry collects personal information directly from the person concerned unless a specified exception applies.

By the very nature of the biometric information, it is and will be collected directly from the person concerned by the Ministry or its agents, including the actual provision of a passport and/or photo by a person.

There are three major exceptions:

1. The first is information received from the information exchanges conducted under bilateral agreements with other agencies (including those overseas). The Ministry is authorised under the 2009 Act to exchange information with equivalent authorities in other countries for immigration purposes by virtue of sections 305–6. Separate privacy impact assessments have been performed addressing the exchange of fingerprint information under the High Value Data Sharing Protocol of the Five Country Conference (FCC).[36] This PIA does not address the disclosure of biometric information under the relevant provisions in Part 8 (sections 305-06) of the Immigration Act 2009 as the Ministry must enter into individual agreements with each agency to which it intends to disclose information. These agreements are in place and do not fundamentally change with the implementation of Vision 2015.

2. The second is information collected by carriers (or the person in charge of a commercial craft) under the Advance Passenger Processing (APP) provisions of the 2009 Act.[37]

3. The third is the use of immigration advisers by people submitting applications for a visa. Immigration advisers are regulated by the Immigration Advisers Licensing Act 2007 and applications submitted by advisers who are not licensed or exempt are not accepted.

This is a matter to be taken into consideration and is addressed at H3 – risk and mitigation for indirect collection.

---

[36] http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/

[37] Covered by section 96–100 of the 2009 Act.

Principle 3 – Collection of information from subject

This principle provides that, where the Ministry collects personal information from the person concerned, it must ensure that the person is made aware of the:

- Fact that information is being collected.
- Purposes for collection.
- Intended recipients.
- Contact details of the agency collecting the information and the agency that will store it.
- Law under which the information is collected.
- Supply of information being voluntary or mandatory.
- Consequences for not providing the requested information.
- Rights of access and correction to the information.

People will be made aware of the above issues by a variety of communication media. The Ministry has also published information on its internet site relating to the collection and handling of biometric data[38.]

This is a matter to be taken into consideration and is addressed at H4 – risk and mitigation for uninformed collection. The Ministry's existing practices in response to privacy risks will be continued and updated to accommodate biometrics. Refer to Appendix 2.

Principle 4 – Manner of collection of personal information

This principle states that the Ministry shall not collect personal information by unlawful, unfair or unreasonably intrusive means.

The collection of biometric information is authorised by numerous provisions in the 2009 Act in a variety of situations and contact points in the immigration processing life cycle (see Table 1).

This is a matter to be taken into consideration and is addressed at H5 – risk mitigation for unfair or intrusive use of information and H2 – risk and mitigation for arbitrary collection. The Ministry's existing practices in response to privacy risks will be continued and updated to accommodate biometrics. Refer to Appendix 2.

Principle 5 – Storage and security of personal information

This principle provides that the Ministry must take reasonable security safeguards to protect personal information against loss, unauthorised access, use, modification or disclosure and other misuse.

The Ministry's Code of Conduct[39] requires all employees to treat personal and confidential information with utmost care and to protect it from unauthorised

38 https://www.immigration.govt.nz/about-us/policy-and-law/identity-information-management

[39] *http://thelink/how/Documents/code-of-conduct.pdf*

access. For example, employees should secure personal information at the end of the day. Employees are referred to specific policies for information security available on the intranet.[40]

The Ministry's existing practices that comply with this principle will be continued and updated to accommodate biometrics – refer to Appendix 2.

The Ministry's Removable Media Security Policy has been updated in 2011 to only allow the use of encrypted, Ministry owned, removable media devices (i.e. USB memory sticks, portable hard drives, etc.).

This is a matter to be taken into consideration and is addressed by various risk and mitigation strategies defined in Table 2 - G4, G5, G6, S1, S2 and S3.

Principle 6 – Access to personal information

This principle provides that, where the Ministry holds information in a way that can be readily retrieved, the person concerned shall be entitled to obtain confirmation that the information is held, to have access to it and to be informed that they may request correction of it. Since September 2010, this right applies to all people worldwide who have dealings with the Ministry and not merely to New Zealand citizens and people in New Zealand.

The Ministry meets this requirement and provides in its internal policies and procedures for the right of access and correction to people about whom it has made a decision on an immigration matter.

The Ministry's existing practices that comply with this principle will be continued and updated to accommodate biometrics – refer to Appendix 2.

There are some procedural risks associated with this principle, addressed at H6 - and H7 risk and mitigation strategies defined in Table 2.

Principle 7 – Correction of personal information

This principle provides that the Ministry must entitle the person to request correction of personal information and to request that a statement of correction be attached to the information considered erroneous. Since September 2010, this right applies to all people and not merely to New Zealand citizens and people in New Zealand.

As mentioned above in Principle 6, the Ministry has policies and procedures in place to support the rights of access to and correction of personal information to any person on whom it holds personal information.

The Ministry's existing practices that comply with this principle will be continued and updated to accommodate biometrics – refer to Appendix 2.

---

[40] http://intranet/tools/searchcenter/Pages/results.aspx?k=information%20policy&s=All%20Sections

There are some procedural risks associated with this principle, addressed at H6 and H7 - risk and mitigations strategies defined in Table 2.

Principle 8 – Accuracy etc. of personal information to be checked before use

This principle states that the Ministry shall not use personal information without taking reasonable steps to ensure that it is accurate, up to date, complete, relevant and not misleading.

By its very nature, biometric data (particularly fingerprints and faces) is vulnerable to variations through disease, surgery, accident and/or deliberate acts.

The Ministry's existing practices that comply with this principle will be continued and updated to accommodate biometrics – refer to Appendix 2.

This is a matter to be taken into consideration and is addressed in Table 2 at H8 and H9 – risk and mitigations for incorrect information or incorrect decision making related to personal information.

Principle 9 – Not to keep personal information for longer than necessary

This principle states that the Ministry must not keep personal information for longer than is required for the purposes for which it may be lawfully used.

The Ministry's existing practices that comply with this principle will be continued and updated to accommodate biometrics – refer to Appendix 2.

Retention is a matter to be taken into consideration and addressed in Table 2 at H1 and H10 - risk and mitigations for unnecessary collection of personal information and retaining personal information for longer than needed.

Principle 10 – Limits on use of personal information

This principle provides that the Ministry may not use personal information collected for one purpose for any other purpose unless it can rely on one of the exemptions listed in Principle 10.

Principle 10 is inextricably linked with Principles 1 and 3 in that information collected by the Ministry must be necessary for its functions or activities and people must be aware of those purposes. The Ministry must consider the extent of the biometric information being collected and is bound by what it advised affected people in terms of its subsequent use.

This is a matter to be taken into consideration and is addressed in Table 2 risk and mitigations for purpose limitations at H11 and unauthorised access and use at S2.

Principle 11 – Limits on disclosure of personal information

This principle states that the Ministry must not disclose personal information unless it has reasonable grounds to rely on one of the exemptions specified.

Principle 11 is also closely linked with Principle 3 in terms of advising people of the purpose of collection and, specifically, intended recipients. As with Principle 10, the Ministry is then restricted in terms of its grounds for disclosure unless an exception applies, one of which permits disclosures that are necessary for the maintenance of the law.

Disclosure is a matter to be taken into consideration and is addressed in Table 2 risk and mitigations for purpose limitations at H12 and unauthorised access and disclosure at S2.

Principle 12 – Unique identifiers

This principle states that the Ministry must not assign a unique identifier (UI) to a person unless it is necessary for carrying out its functions efficiently.

The Ministry already assigns a UI to each person for the purpose of managing that person's records. The UI is assigned when a person record is initially created. All immigration applications made by the person are linked to the person record using the UI.

That UI is unrelated to the person's biometrics. Currently, the Ministry has no expressed intention of using biometrics as indices in its systems or to manage its records.

The possible use of biometric templates as indices has been identified as a matter to be taken into consideration and addressed in Table 2 risks and mitigations for H13 – unnecessary assignment of identifiers and H14 – the risk of widespread use of identifiers

6.2.2 Immigration Act 2009

The 2009 Act provides for the collection and handling of biometric information in various sections, as listed in Table 1, and mandates this PIA in section 32.

6.2.3 Other relevant legislation

The assessment of compliance with other legislation is outside the scope of the report.

6.3 Collaboration with other agencies

The third guiding principle encourages agencies to consider, as early as possible, the identification of opportunities to collaborate with other agencies and stakeholders. Examples of collaboration include but are not limited to sharing infrastructure, common design between systems, interoperability, joint business cases, budgets and procurement and the implementation of pilot programmes.

Vision 2015 demonstrates the Ministry's compliance with this principle in its collaboration with the CGBG and cooperative arrangements with the NZ Police, This relationship is underpinned by the Memorandum of Understanding (MOU) between the Ministry and the NZ Police who support the Ministry by providing

fingerprint expertise and resolution services. The MOU[41] includes provisions to ensure information will be shared in compliance with the Privacy Act 1993.

Comprehensive discussions and planning has also occurred with the DIA, NZ Customs, NZTA and MPI to identify joint procurement, shared services, interoperability, joint business cases and procurement opportunities for collaboration. Simultaneous work in the Ministry includes the development of a policy framework for the use of biometrics at the border in consultation with relevant agencies.

The Ministry is responsible for providing authoritative foreign national identity information to all government agencies. It will continue to work closely with the DIA on effective and efficient means of processing New Zealand citizens who present for entry at the border.

There is a range of Government policy frameworks and standards that should reduce potential security risks and risks around inadequate business cases and inappropriate procurement associated with collaborative undertakings.

Government recently issued *Directions and Priorities for Government ICT,* which sets the overall environment across government for information and communications technology (ICT) and replaces the 2006 eGovernment Strategy. The directions and priorities emphasise that agencies should 'prioritise investment in shared solutions for integrated, multi-channel, service delivery across government'. The risks and mitigations relevant to secure handling of biometric information (including loss, unauthorised access to, use, disclosure, modification, storage and disposal) are addressed in Table 2 at S1, S2 and S3.

The Ministry is also bound by existing government policies regarding major ICT projects. Those include State Services Commission guidelines on ICT projects,[42] government standards[43], the government procurement regime, the Gateway process (mandatory for all projects over $25 million) and the Treasury's Investment Management and Asset Performance regime[44] and Better Business Cases for Capital Proposals.[45] The risks and mitigations relevant to managing privacy considerations in outsourcing processes, negotiations and contracts related to the use of biometric information are addressed in Table 2 at G6.

The Ministry's participation in collaborative initiatives under the Joint Border Sector Governance Group will also be subject to the *Guiding Principles for the Use*

---

[41] Memorandum of Understanding between the Ministry of Business, Innovation and Employment and the NZ Police, January 2015

[42] *Guidelines for Managing and Monitoring Major IT Projects*. Wellington: State Services Commission and the Treasury, 2001. http://www.ssc.govt.nz/display/document.asp?NavID=114&DocID=6423

[43] *E-Government Interoperability Framework*. Wellington: State Services Commission: 2008.

[44] http://www.treasury.govt.nz/publications/guidance/mgmt/capitalasset superseded in June 2015 by http://www.treasury.govt.nz/statesector/investmentmanagement/review/assetperf

[45] http://www.treasury.govt.nz/statesector/investmentmanagement/plan/bbc

of Biometric Technologies[46] developed by the Cross Government Biometrics Group of which the Ministry and other border agencies are members.

6.4 Consideration of end users

The fourth guiding principle recommends that end users of any business process that includes biometrics should be appropriately consulted. The Ministry undertook widespread consultation prior to the introduction of legislation enabling biometric processing. Consultation should include social and cultural considerations, accessibility issues (if relevant) or other constraints or concerns. These concerns and constraints should inform the type of biometrics to be used or inform the development of requirements for implementation.

In April 2006, a public discussion paper was released covering all aspects of the Immigration Act review.[47] Officials held public meetings in May and June 2006 to outline the proposals, which were attended by more than 650 people. The Ministry received 3,985 written submissions in response to this paper. Submissions were received from a wide range of people and organisations.

Section 11 of the discussion paper dealt with the collection and handling of biometric data. Agencies that made submissions included immigration consultants, ethnic councils, refugee and migrant groups, human rights groups, law societies, community law centres, other community groups, businesses, representatives of the airline and tourism industries, a union representative, the United Nations High Commissioner for Refugees, government agencies and two political parties.

A number of submitters commented on the increasing use of biometric information internationally and the need for New Zealand to keep up to date with developments and make appropriate legislative provision for the use of biometric information in immigration processes. Some submitters noted the potential for biometric information to serve the dual purpose of enhancing border security and facilitating the entry of low risk travellers. Many submitters emphasised the need for the use of biometric information to be consistent with internationally agreed standards.[48]

Cultural considerations include the Ministry not requiring people who wear headgear for religious or cultural reasons to remove it, as long as it does not obscure the face. In cases where live photos are taken of a person, this is done in a private location. Similarly, facial markings such as bindis are not required to be removed.

Application forms, arrival cards and a variety of information media (for example, pamphlets and websites) are used to advise end users of the ways in which biometric information will be collected and how it will be handled by the Ministry.

---

[46] *Guiding Principles for the Use of Biometric Technologies for Government Agencies*. Wellington: Department of Internal Affairs, April 2009. ISBN 978-0-478-29487-3.

[47] http://www.dol.govt.nz/actreview/index.asp

[48] http://www.dol.govt.nz/actreview/summary/summary-immigration-h1_12.asp

6.5 Appropriateness of the biometrics used

The fifth guiding principle states that thorough research must be undertaken to identify the range of biometrics that can appropriately meet business requirements. The effectiveness and weaknesses of these alternatives must be understood as well as the benefits and costs. This ensures that the biometrics used is appropriate and proportional to Ministerial needs.

Biometric solutions each have their own positives and negatives. Therefore, many agencies opt for a 'multi modal' solution incorporating two or more biometric types. Following analysis of business requirements and overseas trends and research, the Ministry uses both face and fingerprint biometrics in a manner that is compliant with New Zealand laws. It draws particular attention to compliance with the Privacy Act 1993 and the New Zealand Bill of Rights Act 1990.

The combination of face and fingerprint biometric information (each is described further below), provides the ideal combination of ease of collection with high accuracy and high compatibility with overseas and domestic partners' capabilities. Fingerprint and face biometrics form the core of the Ministry's use of biometric information.

6.5.1 Fingerprints

Fingerprints have a much higher level of uniqueness than faces, particularly if all 10 fingers are used.[49] Fingerprints are the preferred method for tying a questionable identity to a person for immigration purposes. This is because of the high maturity and reliability of automated fingerprint matching technology supported by the depth of expertise in manual assessment of fingerprints available at Police. Fingerprints are regarded as being more effective than faces for matching against large databases, with fast, accurate matching demonstrated against databases of well over 100 million persons.

Fingerprints can also be used in a near anonymous (or pseudonymous) process to identify people of common interest between jurisdictions. This is because human beings typically identify each other through other biometric characteristics such as face, voice or gait and cannot recognise another person via their fingerprints without specialist training.

The Ministry will not collect fingerprints from everyone entering the country but will apply a risk based approach to requiring fingerprints from visa applicants. Fingerprints will continue to be collected from groups such as refugees and those who may be subject to turnaround or deportation orders.

The Ministry will collect fingerprints from some clients; primarily those perceived as high risk cases. Their fingerprints are searched and stored in the immigration dedicated fingerprint database held by NZ Police and which is expected to transition to the Ministry in 2016.

---

[49] People's fingerprint patterns are not completely unique (although, analysed alongside the individual marks and scars obtained through life, they are effectively so).

The Police may also collect fingerprints on behalf of the Ministry and this will continue for some cases following the transition of the fingerprint database to the Ministry. Typically, this occurs where the person has been in formal detention and served with a deportation liability notice by an immigration officer.

The introduction of the IDMe system enables the automated matching capability of biometric and biographic information, including fingerprints and provides for the storage of fingerprints with transition from NZ Police to the Ministry anticipated in early 2016. The introduction of IDme technology will enable the Ministry to store all fingerprints.

NZ Police will continue to provide matching / resolution support to INZ for complex fingerprint cases that are unable to be matched automatically by IDme, as well as the collection of fingerprints for deportation and turn around processes.

As a member of the FCC the Ministry exchanges fingerprint biometric information with its partners. This exchange will be automated with the implementation of the SRTP in 2016, commencing with Australia initially and other partners are anticipated to follow. SRTP will change the way fingerprint data is shared in terms of real time sharing and less manual involvement to transfer fingerprints. There will be no change to the type of data shared with the FCC partners or the collaboration provisions as defined in current agreements.

Fingerprints will be collected from refugees[50] who apply to enter New Zealand under the UNHCR programme (processed by Refugee Quota Branch). Those fingerprints will be stored in the immigration fingerprint system.

The fingerprint system and database currently managed by NZ Police on behalf of the Ministry, uses automated matching of fingerprints as the first stage in any search of the fingerprint databases. The system uses a high match threshold setting, with a very low false match rate (FMR) at the expense of a slightly higher false non match rate (FNMR). Any apparent match resulting from an automated search is always verified by a human expert before any further action is taken.

New matching capability provided by IDme, will enable automated biographic and biometric matching based on 'probabilistic matching' determined by pre-defined business rules. The output of matching is a list of candidate matches which can then be grouped into 'exact' or 'possible' matches. Matching an identity can occur against the entire database or against a specific identity in the database. There are two types of fingerprint matching: fingerprint identification and fingerprint verification.

In the automated match process, 'match' is the decision made by the system when the match score is above the threshold. Where there are two thresholds used in the match process, the match score is above the higher threshold. In manual resolution a 'match' is the decision made by the user when they

[50] Or be included in their identity documents.

determine that both the claimed and candidate identities belong to the same person. Matching scores that are "close" are automatically matched.

Face, fingerprint and biographic matching happen in parallel in IDme. A biometric match with scores above the upper threshold is an 'auto match', while scores below the lower threshold are an 'auto no match'. Scores between the thresholds require a manual intervention to determine the match.

There are multiple searches with biographic matching. Matches made by a conservative search are an 'auto match'; matches made by a looser search require a manual intervention to confirm. Candidates not matched by either a conservative or looser search are an 'auto no match'.

The arrangements with the Police raise governance risks identified at G6. When the storage of the fingerprints database moves to the Ministry this risk will be partially mitigated. Further mitigations are achieved through cooperative arrangements with NZ Police, underpinned by the Memorandum of Understanding (MOU) between the Ministry and the NZ Police. NZ Police will continue to support the Ministry by providing fingerprint expertise and resolution services for complex cases. The MOU[51] includes provisions to ensure information will be shared in compliance with the Privacy Act 1993.

Police security protocols and audit regulations apply to all fingerprints they collect and manage. When fingerprints are transmitted outside the Police system, they are always encrypted to international standards and only transmitted via secure servers.

6.5.2 Face recognition

The introduction of IDme enables biometric processing capabilities, for both fingerprints and face biometrics. This allows the Ministry to fully integrate the use of biometric information within the immigration services. Refer Appendix 12.

Automated face recognition is generally considered less exact than fingerprint matching in one to many situations, particularly when the 'many' is a very large database. Most face biometric systems return 'matching candidate' lists of multiple persons, whereas fingerprint systems will often return a single matching candidate depending on the thresholds set. Nevertheless, photographs are much easier to collect than fingerprints. They are also easier to manually compare and resolve than fingerprints – virtually any person can perform this task (at a basic level) without any specialist training required. Passports today invariably use a face image as a primary biometric.

Where the Ministry wishes to verify a person's identity against a reliable identity document (or its own earlier records in one to one matching), face recognition against a secure photograph in that identity document is considered a satisfactory

[51] Memorandum of Understanding between the Ministry of Business, Innovation and Employment and the NZ Police, January 2015

level of assurance. This is, essentially, what Customs and Immigration Officers have done manually for a long time.

IDme capability will now enable the matching process to be automated with some exceptions for manual resolution of complex cases. Automation will provide immigration management benefits and increased compliance with Government standards, Auditor General Review recommendations and industry advancements. Such benefits include:

- Improved risk mitigation.
- Improved capturing of identity information.
- Improved ability to search based on biometric data.
- Greater confidence making identity decision.

Ultimately, all of these benefits support the desire to increase the ease of immigration processes for individuals, and improved detection and management of fraudulent identities or criminal activity.

The facial image will be collected and matched with biographic information and compared with photos of existing identities and watch lists. If a match is not found a new record or identity is created, otherwise the existing identity record is updated. Alternatively, identities which produce inconsistent match results, (for example, matches with more than one existing INZ client) or indicate possible identity fraud will be managed by referral for manual identity resolution. The application then moves to the process of decision making.

Customs currently operates SmartGate. SmartGate allows New Zealand, UK, Canadian, US and Australian citizens who are e-chip passport holders aged 12 and over to use an automated primary line process. The SmartGate reads the electronic photograph in the passport and compares it with the person in front of a SmartGate camera.

The IDme solution must be able to achieve Ministry Security Accreditation. Therefore the design of security controls must take into consideration Government guidelines, directives and legislation for security of information systems for information classified as Restricted in Government classification terms. Additionally, Privacy by design has been taken into consideration in the development of the IDme solution. This is further enhanced by implementation of security controls appropriate for biometrics, including: storage; networks; access; encryption; integrity and malware protection.

6.5.3 Iris recognition

The 2009 Act includes iris scans in its definition of biometric information. At this time, the Ministry does not have any plans for implementing iris scans. While they are generally regarded as more accurate than fingerprints, they are not interoperable with overseas or domestic partners, and unlike fingerprints and face recognition, there is no infrastructure capability in place in New Zealand to collect them. It is possible that they might be introduced at some future date as an option to facilitate processing for frequent travellers.

The privacy risks attendant on iris recognition will need to be reviewed and addressed when more is known about why and how they might be used and managed.

6.6 Relevant international obligations

The sixth guiding principle requires regard to and demonstrated compliance with international obligations including a number of treaties and international agreements to which it must comply, including United Nations Conventions. The Convention Relating to the Status of Refugees (the Refugee Convention) is included as a schedule of the Immigration Act 2009, and it includes a process for determining New Zealand's immigration related obligations under the Refugee Convention, the International Covenant on Civil and Political Rights and the Convention Against Torture.

New Zealand has commitments as a member of the Five Country Conference (FCC) and undertakes biometric and biographic information sharing with its partners according to formal agreements with each partner. It is also a member of the International Civil Aviation Organization (ICAO)[52] which sets standards for passports and the information contained in them, applicable to machine-readable travel documents. New Zealand must comply with other relevant industry organisations such as the International Air Travel Association (IATA)[53], the Biometrics Institute[54] and the Inter-Governmental Consultations on Migration, Asylum and Refugees (IGC).

6.7 Stewardship – systems and processes

The final guiding principle requires that agencies have in place robust stewardship and integrity in relation to collection, storage and use of biometric information. This is addressed in Table 2 - G1 risk and mitigation for the formalised and central oversight of personal information management. All personal information (of which biometric information is a subset) is a valuable commodity and a strategic resource. Any compromise to that information can result in a lack of trust in immigration processes and systems and is a major reputational risk for the Ministry. Appropriate independent security assessments have been conducted and recommendations implemented where required.

A strategic approach to the overall management of personal information, including biometrics is required, and options are outlined in Section 9, Privacy Enhancing Technologies.

[52] http://www.icao.int/Pages/default.aspx
[53] http://www.iata.org/Pages/default.aspx

[54] http://www.biometricsinstitute.org/

7. ANALYSIS OF IMPLEMENTATION PRINCIPLES

The implementation principles support the guiding principles provided by the CGBG and outlined in Section 6. They identify the key operational matters to address when proceeding with the use of biometric technologies. The *Guiding Principles for the Use of Biometric Technologies for Government Agencies*[55] are expressed as implementation principles. They encompass the following requirements:

1. Information to and consultation with end users and stakeholders.
2. Establishment of processes and procedures.
3. Management of the life cycle of biometric information.
4. Establishment of procurement processes.
5. Standards for interoperability.
6. Legal information sharing and matching.

7.1 Information to and consultation with end users and stakeholders

The first implementation principle requires agencies to provide useful information to end users and stakeholders about its use of biometric information. The Ministry has already developed a *Policy Framework for Collection and Handling of Biometric Information under the Immigration Act 2009,* which sets out the objective and principles that will guide the policies, procedures and processes put in place to support the collection and handling of biometric information across the business units.[56]

Application forms, arrival cards and a variety of information media (for example, pamphlets and websites) are required to advise end users and other interested parties of the ways in which biometric information is collected and handled by the Ministry.[57] Further, the *Immigration New Zealand Operational Manual*[58] is available to the public, outlining the practical procedures currently in use in the immigration processing life cycle.

The initial consultation process undertaken in April 2006 has continued with ongoing consultation through to 2015. It has incorporated a variety of internal and external stakeholders and people affected by the collection and handling of biometric information. Many submitters commented on the safeguards that needed to be addressed in the legislation. Submitters commented that the legislation should be consistent with privacy and human rights legislation and include provisions on:

---

[56] http://www.immigration.govt.nz/NR/rdonlyres/CF1345B5-1578-45A4-B6F9-4806BB0480B7/0/DOL11423PolicyFrameworkforBIv12.pdf

[57] http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement

[58] http://www.immigration.govt.nz/migrant/general/generalinformation/operationalmanual

- The uses to which the information must be put.
- The length of time that information is stored and the means by which it must be stored.
- The circumstances under which information may be shared with other governments and other government Ministries.
- The means by which people can access and, if necessary, correct their personal information.
- A process for reviewing the handling and use of biometric information.

7.2 Establishment of processes and procedures

The second implementation principle provides guidance on the operational processes that will be required to ensure biometric information is handled appropriately. The operational processes are as follows:

- All means by which biometric data is collected; converted, stored, compared, decisions are made about it or the disposal of it.
- Data access security levels.
- Circumstances/guidance relating to the disclosure of biometric data.
- Exceptions for handling false positives, false negatives or other problems with biometrics.
- Resolving problems with the biometric system.
- Resolving issues/complaints by end users.
- System failures.
- Security components and safeguards.
- Auditing of biometric system and processes.
- Staff training/awareness.
- Scope creep (use of the information beyond the original purposes).

7.3 Management of the life cycle of biometric information

The third implementation principle requires the Ministry to apply all relevant legislation and standards for the management of biometric information it collects.

The Ministry is complying with this principle by having this PIA updated enabling reassessment to take account of changes – legislative, policy, business requirements and other agreements. The mechanism for documenting those updates and changes is provided in the appendices. In order to implement that mechanism, the Ministry manages a systematic process to conduct regular reviews and be able to ascertain and assess any of the changes as outlined in G7.

Additionally, the Ministry's general compliance with the ICT Strategy and Action Plan and other requirements established by the Government Chief Information Officer are evidenced, as are other mitigations being applied and identified in the Vision 2016 PIA.

7.4 Establishment of procurement processes

The fourth implementation principle asks agencies to comply with all relevant government procurement policies and guidelines,[59] when procuring biometric technologies. The Ministry met this requirement in its procurement activities for IGMS in 2011 as follows:

- Undertaken detailed scoping and definition of requirements in consultation with relevant agencies and stakeholders (where relevant).
- Investigated opportunities for collaborative procurement.
- Investigated the option of updating and utilising existing contracts negotiated by other agencies.

These steps aim to achieve the best value for agencies and government as a whole and will assist to inform procurement decisions.

Collaborative procurement and system development raise governance risks identified at G5 and G6.

7.5 Standards for interoperability

The Ministry aims to operate using internationally agreed standards for biometric information, this is the fifth implementation principle. For example, where there are relevant ISO/IEC JTC-1 standards,[60] those would be employed. There are other standards that are relevant. While not international standards, National Institute of Standards and Technology[61] standards for exchanging fingerprint information are internationally accepted and used in the FCC exchanges.

The Ministry is also a member of the Biometrics Institute, which issued a Privacy Code approved by the Australian Privacy Commissioner.

Other international standards issuing groups that are involved in biometrics work include the International Telecommunications Union (ITU),[62] the International Civil Aviation Organisation (ICAO), the International Labour Organisation (ILO)[63] and the Organization for the Advancement of Structured Information Standards (OASIS).[64]

---

[59] Government procurement policy framework, policies, mandatory rules, Auditor-General guidance and other material can be found at http://www.business.govt.nz/procurement

[60] ISO/IEC JTC-1 is the Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission. The primary subcommittee dealing with Biometrics is SC-37 Biometrics, but SC-27 IT Security Techniques and SC- 17 Cards and Personal Identification also issue standards relevant to biometrics implementation.

[61] US National Institute of Standards and Technology http://www.nist.gov/index.html

[62] The International Telecommunications Union is the relevant UN agency http://www.itu.int/en/pages/default.aspx

[63] International Labour Organization http://www.ilo.org/global/lang--en/index.htm

[64] Organization for the Advancement of Structured Information Standards http://www.oasis-open.org/home/index.php

7.6 Legal information sharing and matching

The sixth implementation principle requires agencies to ensure that any information matching or sharing is appropriately authorised. It is Ministry policy that all information matching or sharing of biometric data between the Ministry and any other agency will have legislative authority and/or the necessary agreements such as a Memorandum of Understanding, is in place to ensure compliance with the Privacy Act 1993. Several provisions exist in the Immigration Act 2009 to regulate information sharing and matching (see sections 294–306).

8. RISK ASSESSMENT – ANALYSIS OF IMPACTS

A summary of the proposed actions to implement the biometric provisions is shown in Table 1. The identified risks and mitigations are shown in Table 2.

The risks involved are divided into three categories:

- Governance (G1-G7).
- Handling practices (H1-H14).
- Security (S1-S3).

Specific risks follow with their accompanying mitigations.

8.1 Governance risks

These identified risks are concerned with the framework and strategy for privacy compliance within the Ministry. The PIA 2016 update identified that there is a Ministry wide Privacy Steering Group that reports to the Safety and Security Governance Committee. The Steering Group has the responsibility to oversee the development and execution of a privacy strategy, which will identify the system and process changes needed across the Ministry. Furthermore, within its business units to have systems which provide a high degree of assurance that they are in compliance with legislation, with the Government Chief Privacy Office and other whole-of-government requirements, and with the Ministry's internal policies.

Compliance will remain decentralised at the function and business unit level. As well as specific risk mitigations, this section also provides options for the Ministry's consideration of an enterprise privacy strategy.

G1 Formal/centralised oversight of personal information management or privacy risk

The Ministry's Safety and Security Governance Committee provides the strategic oversight for privacy across the Ministry. Its membership is outlined in its Terms of Reference and responsibilities include:

- Provision of strategic oversight and timely decision making for privacy.
- Approval of the internal Ministry Privacy Policy and Privacy Strategy.
- Reviewing reports from the Privacy Steering Group on Ministry privacy risks, incidents, and activities to implement the privacy strategy.
- To champion and promote privacy and the management of privacy risks within the Ministry.
- Setting the Ministry's privacy risk appetite and tolerance.

Recommended mitigations:

- Review the Safety and Security Governance Committee, which has the responsibility for policies and oversight of handling practices for personal information within the Ministry.

- The review will ensure effective responsibility for privacy issues, including a comprehensive consolidated Privacy Programme Strategy and reporting structures for privacy issues.
- The group contributes to Ministerial 'cultural' leadership; respect for privacy is not automatic and cannot be assumed.

G2 Inconsistent, limited or contradictory policies and instructions on the collection and handling of biometric information

The Ministry is developing an integrated strategy for personal information collection and handling aimed at mitigating the risk of having fragmented policies or practices around the collection and handling of biometric information.

The Ministry has developed a privacy framework.

Recommended mitigation:

- Implement the integrated and comprehensive privacy policy that accommodates all aspects of the information management life cycle and all information privacy principles. This work is underway and due for implementation during 2016.

G3 Unnecessary expense incurred because systems are not designed with privacy considerations from the beginning

When systems are designed without consideration of privacy for personal information, the Ministry is exposed to the risk of on-going unnecessary expense. These include difficulties in meeting statutory requirements to provide access to and correction of personal information, answering requests under the Official Information Act, providing management reports on handling of statutory requests for information and increased exposure to data breach risks.

The recommended mitigations have been identified in the PIA 2016 as being underway or implemented.

Recommended mitigations:

- Commit to incorporate 'privacy by design' for all new biometric and other personal information collection and handling systems in the Ministry.
- Require privacy impact assessments for all new and significantly changed systems that store or process biometric and other personal information prior to their design and construction.
- Design and build biometric and other personal information systems so that requests for personal information can be answered quickly, completely and without undue expense.
- Design and build biometric and other personal information systems so that privacy request processes provide adequate management reports on the nature, frequency and resolution of issues.

G4 Authorisation to access biometric information is too widely approved

When authorisation to access personal (biometric) information is too widely approved, it increases the risk of inappropriate disclosure and use of that information. This is also a security risk for all information. This risk needs to be balanced against the need for an appropriate information sharing culture in the public sector as identified in the recent Law Commission review.

Recommended mitigations that are identified in the 2016 PIA as underway or implemented:

- Establish adequate controls around the granting of authorisation to access biometric information.
- Design audit processes into all systems used to store and process biometric information to control user accounts, access rights and security authorisation.
- Base access rights to biometric information on the need (essential business justification) to know.

G5 Inadequately managed collaboration and information sharing with other agencies puts biometric information at risk

The Ministry shares biometric information with other government agencies, both in New Zealand and overseas. When the agreements underlying those arrangements are not adequately drafted, the Ministry runs the risk of being unable to meet its statutory obligations. Those obligations go beyond mere security of the information but also include the ability to respond adequately to personal information requests and official information requests.

Recommended mitigations that are identified in the 2016 PIA as underway or implemented:

- Include privacy considerations in collaborative undertakings with other agencies.
- Ensure that information sharing agreements do not compromise the Ministry's ability to meet its statutory obligations.
- In particular, require measures to prevent unauthorised use or disclosure of biometric information.

G6 Inadequately managed outsourcing does not adequately protect biometric information

This includes service agreements, contracts and MOU's with other government agencies acting as agents/service providers for the Ministry as well as contracts with the private sector.

The Ministry is responsible for the actions of any agencies acting on its behalf in the collection and handling of biometric information. Poorly drafted agreements

and contracts can leave the Ministry exposed to non-compliance with its statutory obligations including privacy responsibilities.[65]

Recommended mitigations that are identified in the 2016 PIA as underway or implemented:

- Include privacy considerations in any tendering processes, negotiations and contracts for outsourced collection or handling of biometric information.
- Establish measures to monitor and audit outsourced collection or handling of biometric information to ensure that the Ministry's privacy responsibilities are met.
- In particular, require measures to prevent unauthorised use or disclosure of biometric information.

G7 This PIA is not reviewed, augmented or kept current in contravention of section 32 of the 2009 Act

The Ministry should continue with the existing process for review and amendment of this PIA (or have a procedure for assessing the requirement to create a new one) if changes are made to the 2009 Act, regulations, operational policy with respect to the collection and handling of biometric data. The use of the templates in the appendices to this document is expected. This PIA 2016 and previous PIA 2012 indicate that this governance risk is being managed.

Governance options

Responsible governance requires proactive on going stewardship of data, systems and processes. A comprehensive approach is often referred to as an enterprise privacy strategy.[66] As with any strategy, an enterprise strategy needs to be proactive and expressed rather than implied. Therefore, it should be articulated into a plan. Execution of the plan should be resourced and performance should be monitored against the plan.

The Ministry has established a combined strategy that reflects its values and statement of intent. The chosen privacy strategy the Ministry is implementing is aligned with a combination of Options 2 and 4 below. These options were initially provided in the PIA 2010 as guidance for the possible strategies that could be adopted. Since then, a comprehensive information privacy strategy overseen by the Safety and Security Governance Committee has been designed and is due for implementation in early 2016. The Ministry has also implemented an ICT Strategy, combining information data and systems stewardship with procurement, security and development controls[67].

---

[65] A useful guide is the State Services Commission's *Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management*. This is a comprehensive overview of managing outsourced risk including privacy risks. While targeted at overseas service providers, much of the content is also applicable to local providers.

[66] *Privacy Impact Assessment Code of Practice* . Wilmslow, UK: Information Commissioner's Office, February 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[67] https://www.ict.govt.nz/assets/Uploads/Government-ICT-Strategy-and-Action-Plan-to-2017.pdf

1. A minimalist information privacy strategy

The most basic approach to an enterprise privacy strategy is to reflect the requirements of privacy law, including (but not limited to) the information privacy principles established by the Privacy Act 1993.

The minimum that the Ministry can reasonably be expected to do is:

- Continue developing an organisational understanding of privacy and of the key privacy issues that arise in the relationships with people.
- Regularly review the Ministry's holdings of personal information and the business processes relating to that information.
- Reinforce recognition of privacy matters into project processes (for example, a component of project scoping documents or budget approvals), which should include:
  - a requirement that PIAs be considered where appropriate
  - a requirement that a privacy law compliance check be performed

2. A comprehensive information privacy strategy

The Privacy Act 1993 focuses on data privacy concepts that originated in the 1970s. Public expectations have moved well beyond those ideas, and a range of claims have emerged for more extensive forms of privacy protection. The Ministry could recognise privacy as being a strategic factor in trust relationships with its people and acknowledge that privacy is a matter of corporate responsibility, to ensure a more comprehensive strategy. This goes beyond the conduct and reporting on of specific PIAs such as this document.

It involves the following measures being driven from a senior management level:

- Establish and maintain a focal point that ensures executive attention to privacy including commitment by senior management to a privacy programme, appointment of a Chief Privacy Officer who has a practical overview of Ministerial privacy issues and periodic inclusion of privacy matters in senior management agendas.
- Conduct a strategy formation process that anticipates problems and is based on an appreciation of the Ministry's information holdings, practices, technologies and relevant laws as well as dealing with public sensitivities in relation to the information, practices and technologies.
- Ensure that business process engineering and re-engineering activities have privacy sensitivity embedded into them. This involves provisions with supplier contracts and in the Ministry's project management framework and methodology, especially during the project initiation stages, through phases of conception, analysis, design and implementation and on to post implementation review and audit.
- Structure a programme that builds privacy respect into the Ministry's philosophy, mind-set and business processes. This requires both formal and informal measures. Crucial among the formal measures is the integration of the PIA process within all of the Ministry's procedures. A key location for such a programme is in staff training initiatives. Another is internal audit of personal information practices, including both periodic

audit and on demand audits occasioned by specific incidents and/or general concerns.

- Establish and maintain an internal communications programme, utilising such vehicles as the intranet, training courses and newsletters that keep privacy in the minds of operational staff, managers and senior managers. Staff could be provided with a mechanism to raise privacy and data breach concerns – anonymously, if necessary.
- Establish and maintain an external communications programme, comprising at least the following elements:
  - Integration of privacy-related messages into communications with affected people (including staff).
  - Identification of relevant representative and advocacy organisations and collection of information about them.
  - Creation and maintenance of channels to and from relevant representative and advocacy organisations.
  - The capacity to receive and handle incoming communications through procedures for handling incidents, enquiries, submissions and complaints.

A comprehensive information privacy strategy is likely to encompass additional aspects beyond basic provisions addressed in legislation, such as the following:

- Protection for all categories of people, without restrictions such as 'citizen', 'resident' or 'person' and with provisions related to the interests of deceased persons and their relatives, where applicable.
- Recognition of the benefits as well as the risks involved in 'data silos'. Such patterns as the consolidation of data from multiple sources into a single virtual databank, the use of personal information for additional purposes, 'function creep' from one business function to another, data warehousing and data mining all encroach on privacy to a degree. These considerations should be taken into account when designing immigration ICT systems.
- Recognition of the benefits as well as the inefficiencies involved in 'identity silos' by avoiding the use of the same identifier in multiple organisations, systems and programmes.
- Approval for and facilitation of anonymous and pseudonymous transactions services in all circumstances where that is realistic (for example, the initial exchange of information in the Five Country Conference (FCC) under the High Value Data Sharing Protocol).
- Avoidance of prejudice to people's access to services or their ability to exercise other benefits because of the exercise of privacy rights.
- Control over identification and authentication tokens, such as chip cards and digital signature keys.

Some of these expectations may engender concerns about the Ministry's administrative efficiency, the management of waste and fraud and an integrated view of people across business units and even across the Ministry's boundaries to its strategic partners.

3. A broad privacy strategy

The Privacy Act 1993 is limited to information privacy. People are concerned about other aspects of privacy as well, and the Ministry may judge it to be advantageous to define the scope of their enterprise strategy to reflect broader concerns.

A broad enterprise privacy strategy could also encompass impacts on:

- Privacy of the person, which relates to safety and interference with the human body – this intersects information privacy in several ways, for example, in relation to sample extracting for testing and other biometric measures.
- Privacy of personal behaviour, which relates to surveillance of both physical and electronic activities – this also intersects with information privacy, particularly where data is recorded (for example, by surveillance cameras) that may be or may become associated with a person.
- Privacy of personal communications, which relates to conversation and message interception, traffic analysis and access to recorded and stored messages – similarly, this, has intersections with information privacy.

4. A social impacts or public policy strategy

The Ministry may decide it is advantageous to adopt a scope that is broader than privacy alone but encompasses it. An enterprise social impacts or public policy strategy would also incorporate impacts (both positive and negative) on such matters as:

- The availability and quality of services.
- The accessibility and equity of services.
- The allocation of effort, costs and risks, particularly when they are shifted in the direction of people.
- Choice in relation to the provision of biometrics including benefits foregone if not provided and penalties for non-compliance.
- Consent in relation to the provision of biometrics rather than legal compulsion or other forms of coercion.
- Job market and industry structure impacts.
- Geographical equity impacts, for example, differential service depending on location or access to facilities.
- Social equity impacts, for example, differential service depending on ethnic background, lingual skills and education or physical limitations.
- The human rights of people, employees and contractors.
- The accessibility of information.

8.2 Handling practices risks

These risks are recognised as practical implementation issues that the Ministry needs to consider with respect to both current and future information handling activities. They align with the Privacy Act 1993 Privacy Principles. Progress in the management of handling risks has been steady since the previous PIA 2012. The Ministry's updated Privacy Policy and Strategy addresses many of the risks

identified and the introduction of the Government Chief Privacy Office[68] has provided core expectations in the form of a Privacy Maturity Assessment upon which the Ministry is required to comply with and compared against for progress with a view to increasing privacy maturity.

The following business process activities support the Ministry's Privacy Policy by establishing organisation-wide standards for managing personal information and privacy issues:

- Collection of personal information.
- Requests for personal information.
- Correction of personal information.
- Complaints.
- Privacy events.
- Third party arrangements.
- Business process changes.

The following is an extract from the Ministry's Privacy Strategy, which at time of drafting this PIA 2016 update, was awaiting final senior level sign off, although considerable progress has already been made within the Ministry towards what is outlined below.

"The Ministry's privacy strategy is designed to achieve privacy management excellence by embedding a culture and developing systems, which incorporate 'privacy by design'. This approach is based on the following strategic outcomes:

- MBIE values personal information, treats it with care and respect, and manages it as an asset.
- MBIE builds privacy into how we do business through considered change.
- MBIE continually looks to improve its privacy performance so it can appropriately use the information efficiently to meet its objectives.

The approach MBIE is taking is to raise its general maturity across privacy governance and management (measured against the GCPO Assessment Framework). This requires establishing a robust privacy framework for consistently identifying and managing the opportunities and risks associated with personal information. This will provide managers with the confidence to innovate and encourage mature areas of the business to optimise the value obtained from personal information, for both individuals and the public, while protecting privacy. The success of this approach requires:

- Changing the behaviour of management and staff in relation to privacy and personal information.
- Facilitating the identification of privacy risks and establishment of effective controls to manage or mitigate the risks.

[68] https://www.ict.govt.nz/assets/Guidance-and-Resources/Privacy-Framework-August-online.pdf

- Establishing organisation-wide standards to ensure privacy compliance requirements are met.
- Alignment and coordination with related functions, programmes, and initiatives (refer Privacy Stakeholders)."

Awareness raising and training have previously been of concern but improvements in training initiatives have included the requirement for privacy training to be completed by all new staff at point of induction into the Ministry. This is overseen by the Privacy Programme. In addition there is the intent to establish and monitor a long-term training plan and schedule for all staff and third party contractors. Communications regarding privacy matters will be increased and the updated privacy policy and guidance information made available on the intranet to raise privacy awareness with Ministry staff. Regular communications about key issues via intranet and other channels will be established.

The handling risks are ordered to align with the information privacy principles in the Privacy Act 1993.

H1 Biometric information unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification

It is generally accepted that situations where people have no choice about whether to provide personal information are more privacy intrusive than where there is real choice. The Ministry has statutory authority for the mandatory collection of biometric information under the 2009 Act.

There is a natural propensity to collect information because it is possible to do so rather than because the information is actually needed for current business processes. A key privacy protection principle is that agencies should only collect the minimum information that is necessary in relation to the purpose they have for collecting the information.

Similarly, there is a tendency to collect more information on the basis that more is better or that it may be useful at a later date. In the case of biometrics, the argument is often made that multi modal biometrics collection improves the effectiveness of biometric processing. From a privacy perspective, improved accuracy in and of itself is not a justification for the collection of more than one biometric. Rather, the improved accuracy should be necessary to the adequate operation of the activity in question.

The 2016 PIA review has identified that progress has been made towards achievement of the following recommended mitigations:

- Ensure that all implementations of the biometric provisions in the 2009 Act are in line with the statutory authority.
- Limit collection of biometric information to what is needed (essential business justification) to support current decisions, and establishing identity.

H2 Staff make arbitrary 'requests' for biometric information

The 2009 Act permits the Ministry to require biometric information from certain people, for example, in section 100. How much biometric information and of what type to collect is in some circumstances left to immigration officers to 'request'. Unless employees and agents are well informed as to what circumstances warrant requiring a person to provide a particular biometric or, contrarily, when to waive collection, the Ministry leaves itself open to charges of arbitrary and discriminatory practices.

Recommended mitigations:

- Staff training/awareness in the appropriate circumstances and justification required for 'requesting' biometrics from specific people.
- Staff training in the application of the Ministry's Code of Conduct and its application in situations where professional judgment is exercised.

H3 Biometric information not collected directly from the person concerned

The privacy risk is that biometric information obtained from a source other than the person in question may have been misidentified, as that person's information or may be of poor quality and therefore not properly match information obtained from the person directly.

Recommended mitigation:

- Establish processes to ensure the integrity of biometric data collected from third parties including that received through information sharing or other service level agreements/contracts.

H4 People not adequately informed about the purposes of collection of biometric information

It is a fundamental principle of fair information handling principles that people should understand why an agency is collecting their personal information and the ways the information will be used.

Recommended mitigation:

- Ensure that people are appropriately notified in a relevant manner whenever biometric information is collected from them.

H5 The manner in which biometric information collected is unfair or intrusive

If Ministerial employees or agents are inappropriate in their interactions with people when collecting biometric information, the Ministry risks complaints to the Privacy Commissioner or Ombudsmen about unfair treatment. This would also be the case if collection processes are perceived to be unnecessarily intrusive.

Recommended mitigation:

- Staff training and awareness raising of appropriate respect for and responses to cultural and physical considerations when collecting biometric information.

H6 The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their biometric information

The Privacy Act 1993 was amended to extend the rights of access to and correction of personal information to all people regardless of location.

Recommended mitigation:

- In immigration matters, these people will be treated as if they have the same rights as citizens and residents. This meets the requirements under section 34 of the Privacy Act 1993 as amended on 8 September 2010.[69]

H7 The Ministry is unable to respond effectively to requests for personal information or to investigations by the Privacy Commissioner (and others) because of inadequate system design

When personal (biometric) information systems are designed and built without proper consideration of statutory obligations, responding to legitimate requests for access to personal information may be difficult, expensive or impossible.

Recommended mitigations:

- Implement oversight and review mechanisms. (See also G2)
- Design biometric information systems with the ability to respond to review agencies' requests/investigations.

H8 Biometric information incorrectly associated with a person

It is possible, particularly with information not collected directly from the person, for biometric information to be incorrectly associated with a person.

Recommended mitigation:

- Implement processes/checks to ensure that biometric information is not associated with a person record by mistake.

H9 Inaccurate or incorrect biometric data is used to make a decision about a person

This may be based on a perception that biometrics is infallible and therefore the usual checks and balances within immigration processing do not apply. If a biometric is wrongly associated with a person or of poor quality, they may have unnecessary difficulty challenging an invalid decision based on that biometric.

Concern surrounds the use of automated processing and decision making as a way of abdicating responsibility for the results of the automatic processes. This is particularly sensitive when automated data matching is used and where the nature of the processing (biometric template creation and matching) is, essentially, comprehensible only to experts.

69 http://inzkit/publish/visapak/visapak/#43967.htm

Applying the principles of the Privacy Act 1993 and those of natural justice provide protection against the use of inaccurate and incorrect information in making decisions about people.

Recommended mitigations:

- Explicitly include biometric information in the processes for permitting comment on and rebuttal of potentially prejudicial information.
- Develop specific processes for handling false negatives and false positives when matching biometrics.

H10 Biometric information retained longer than necessary

Biometric information should not be retained beyond the natural business requirement underpinning its collection and use. To do so risks unauthorised exposure of the information. That business requirement can last beyond the natural life of the person but needs to be justified. For example, information about migrants to the country has an historic value.

Recommended mitigations:

- Apply to the Chief Archivist, Archives New Zealand, for a formal disposal authority.
- Introduce standard processes for assessing biometric information for transfer to 'inactive storage' and for final disposal.

H11 Biometric information used for non-immigration purposes

The Ministry's justification for collecting and retaining biometric information is that it is necessary for the identification of people as part of the immigration decision(s) relating to that person. If the information is used for non-immigration purposes without authority, the Ministry could be in breach of the Privacy Act 1993 and its own policies.

Recommended mitigation:

- Standardised and routine staff training and awareness rising in permitted uses of the information.

H12 Disclosure of biometric information without reasonable grounds

Social engineering, curiosity, inadequate security and other causes can result in biometric information being disclosed without proper authority or justification.

Recommended mitigation:

- Ensure staff understanding of their responsibilities through staff training, awareness and support materials.
- Establish and promote access protocols and preventative measures to guard against unauthorised access and subsequent unauthorised use or disclosure of biometric information

H13 Unnecessary assignment of unique identifiers

There is concern about unique identifiers because they can be used as indices across multiple unrelated databases of personal information, linking disparate information into a comprehensive, detailed and unjustified picture of a person.

That concern underlies the prohibition in the Privacy Act 1993 about not assigning another agency's unique identifier.

Recommended mitigation:

- Continue the current process of assigning to people and records about them their own unique identifiers (and which are not biometric templates).

H14 Widespread use of biometric templates as unique identifiers

Biometric templates are a concern as they may be able to be used as indices across multiple databases of personal information.

Recommended mitigation:

- Biometric templates should not be shared with other agencies.

8.3 Security risks

The nature of biometric information means that storage and security aspects should be a primary consideration. In some other jurisdictions, this information is classified as 'sensitive personal data'[70] and is singled out for tightened security practices and increased privacy measures to ensure its protection. These risks all relate to information privacy Principle 5 in the Privacy Act 1993.

S1 Loss of biometric information

As the Ministry increases collection of electronic biometric information, security continues to be an important element for the management of immigration information to avoid loss.

Recommended mitigations:

- Ensure an adequate security environment for biometric information.
- Establish clear protocols for the storage and handling of biometric information.
- Establish contingency plans to address any security breaches.
- Adopt and implement the Privacy Commissioner's Privacy Breach Guidelines.[71]

S2 Unauthorised access to biometric information

Increased access to large amounts of information and its portability increase the risk that carelessly defined access protocols can be abused deliberately or by accident.

Recommended mitigation:

- Establish and promote access protocols and preventative measures to guard against unauthorised access and subsequent unauthorised use or disclosure of biometric information. (See also H12.)

---

[70] http://ec.europa.eu/justice/policies/privacy/index_en.htm

[71] http://www.privacy.org.nz/privacy-breach-guidelines-2/?highlight=data%20breach%20notification

S3 Safeguards implemented to ensure the security of biometric information are not reasonable (adequate) in the circumstances

The Privacy Act 1993 requires that the Ministry takes reasonable precautions to protect the personal information it collects. It also requires that the Ministry does not keep personal information after it has no continuing business reasons for its retention (see also H10) and that, when it disposes of personal information, it does so securely.

Recommended mitigations:

- Design and document appropriate security procedures for the collection, storage, transmission and disposal of biometric information.
- Ensure that security applied to biometric information is appropriate to the sensitivity of the information.
- Apply to the Chief Archivist, Archives New Zealand, for a formal disposal authority for biometric information.

9. PRIVACY ENHANCING RESPONSES

Having acknowledged the privacy risks associated with the collection and handling of biometric data, it is incumbent on the Ministry to propose management and technical responses to mitigate them. A range of privacy enhancing responses may be appropriate to the identified risks.

9.1 Privacy by design

The purpose of privacy by design is to give due consideration to privacy needs prior to the development of new initiatives – in other words, to consider the impact of a system or process on people's privacy and to do this through the system's life cycle, thus ensuring that appropriate controls are implemented and maintained.[72] This is a risk identified and addressed at G3.

An example of a relevant privacy by design feature is incorporating privacy metadata into the architecture of the system. Privacy metadata includes:

- The date the personal information was collected.
- The source of the information, for example, directly from the person, from a completed application form, through an information sharing agreement.
- This 'expiry date' of the information item.
- Any usage permissions or restrictions.
- Logs of every access to and modification of the information.

Other privacy information that should be linked to personal information includes records of:

- Any information access requests – date of receipt, requestor's name and contact information, information released, information withheld and the relevant justification(s), date of formal response.
- Information correction requests and their outcome.
- Complaints made to the Chief Privacy Officer/Resolutions team.
- Complaints made to the Privacy Commissioner.

The design of the IDme solution has incorporated privacy by design considerations. An example of this is the functionality available to Privacy Officers and Identity Service Analysts to enable approved and access controlled extraction of individual's information if required for compliance with an access request or investigation, as defined in Privacy Principle 6 of the Privacy Act 1993.

9.2 Privacy-enhancing technologies

There is no widely accepted definition for the term 'privacy-enhancing technologies' (PETs), although most encapsulate similar principles. A PET:

---

[72] *Privacy by Design*. Wilmslow, UK: Information Commissioner's Office, November 2008. ICO/PBD/1108/1K.

- Reduces/eliminates the risk of contravening privacy principles and legislation.
- Minimises the amount of data held about people.
- Empowers people to retain control of information about themselves at all times.

PETs should not be bolted on to systems or technologies that would otherwise be privacy-invasive. Privacy-related objectives must be considered alongside business goals and privacy considerations addressed at every stage of the system's life cycle.[73]

There are three categories of PETs:

1. Counter privacy-intrusive technologies

Technology applications that gather data, collate and apply it or otherwise assist in the surveillance of people are called privacy invasive technologies (PITs). Data warehousing and data mining, because of their capacity to extract new information about people, and the use of biometric information for its potential use in surveillance are considered PITs.[74]

Some PETs are designed to counter the effects of PITs. Examples include spam filters and cookie managers. The effective incorporation of PETs into a scheme, project or initiative may reduce pressures on privacy that result from programme goals or efficiency requirements, with little increase in cost.

2. Anonymity PETs

The first category of PETs described above does little to stop the accumulation of personal information. Another approach sets out to deny personal identity by providing anonymity. There are many circumstances in which the Ministry can and should permit anonymous communications, such as general enquiries, the provision of generalised (as opposed to person specific) information and to support whistle blowing. Genuine anonymity, however, has the disadvantage that it can be used to avoid detection of criminal activity.

3. Pseudonymity PETs

With anonymity, the Ministry is prevented from being able to identify the person who it is dealing with. Pseudonymity refers to a situation where the person's identity is not apparent, but could, under some circumstances, be discovered.

To be effective, pseudonymous mechanisms must involve legal, organisational and technical protections to ensure the link between a transaction/encounter and an identifiable person can be achieved only under appropriate circumstances. The

---

[73] Fritsch, Lothar. *State of the Art of Privacy – Enhancing Technology (PET)*. Oslo, Norway: Norsk Regnesentral, 22 November 2007. ISBN 978-82-53-90523-5. http://publ.nr.no/4589

[74] *ICT Acceptable Use Policy (no date on the policy)*
http://thelink/how/Documents/ict-acceptable-use-policy.pdf

Ministry already does this in its first stage exchanges with Five Country Conference (FCC) countries under the High Value Data Sharing Protocol.

9.3 Security responses and other privacy protective tools

The Ministry has a suite of policies, standards and guidelines that relate to information security, including personal information security. The information security suite sits within a broader regime for security and acceptable behaviour generally. The overarching policy is the Ministry's Code of Conduct,[75] which addresses, at a high level, employees' responsibilities towards personal information and related responsibilities such as use of the Ministry's computer network.

Examples of specific policies and guidelines can be located on the Ministry's website[76] and include:

- Code of Conduct.
- Information Security Policy.
- Information Security Classification and Handling Policy.
- Physical and Environmental Security Policy.
- Acceptable Use of Ministerial Technology.
- *Removable Media Security Policy* and the Mobile Device Security Standard.
- General guidelines for all ICT users, managers, ICT managers and ICT operational staff.
- Privileged account authentication, cryptography and firewall standards.

These policies address current best practice in information security, specifically address the Ministry's handling of personal information and incorporate current best practices including encryption of any personal information when it is sent outside Ministerial systems. They include the advice to avoid the use of operational data containing personal information in testing situations or to edit the information so that people are no longer recognisable.

While not specific to the Ministry's use of biometrics, there are some actions that should be taken to ensure that general security policies and procedures are sufficient to protect biometric information contained in Ministerial systems.

General security recommendations

1. Adopt the principle in the MBIE Security Policy[77] that all security policies and processes applicable to its information assets are commensurate with the sensitivity of the data.
2. Ensure that controls on data are based on a need to know for access to biometric information, physical access and transmission of biometric information from Ministerial systems.

---

[75] *MBIE Code of Conduct 2015, http://thelink/how/Documents/code-of-conduct.pdf*

[76] http://thelink/about/Pages/mbie-security-policy-2013.aspx

77 https://www.ict.govt.nz/strategy-and-action-plan/strategy/

3. Incorporate external expert advice on security of biometric information in the design and construction of any future immigration information systems.
4. Review the existing policy regime for its adequacy with respect to biometric information.
5. Review staff training and training materials for their adequacy with respect to biometric information.
6. Ensure authorisation controls are adequate to protect biometric information from unauthorised access, modification, use, disclosure and disposal.
7. Ensure that all access and changes to biometric information are logged by unique user ID and date and that those logs provide an adequate audit trail.
8. Establish/document procedures for handling of any improper collection, access, modification, use or disclosure of biometric information.
9. Ensure that the control system for user accounts, access rights and security authorisations is comprehensive and adequate records are maintained of all such processes.
10. Implement contingency planning for biometric information data breaches and other unauthorised information disclosures. Those plans should include notification procedures for all affected parties.
11. Ensure that the Ministry includes adequate resources (financial and personnel) to permit security upgrades as they are made available by the developer(s) or as new threats emerge.
12. Incorporate performance indicators for security in system maintenance plans.

10. ON GOING EVALUATION, REVIEW AND MONITORING

The requirements of section 32 subsection 3 of the 2009 Act requires the Ministry to review its privacy impact assessment in several circumstances. Those are when changes are made to the 2009 Act, regulations are made under it or operational policy is made or changed in respect of the collection or handling of biometric information.

If those reviews establish that new or increased privacy impacts have resulted from the changes, the Ministry must amend or replace the PIA and consult the Privacy Commissioner on the amended or replacement assessment.

The attached appendices are designed to permit the documentation of such assessments and the mitigations proposed to respond to the risks identified. Together with this umbrella document and the global risks and mitigations identified, they should provide a comprehensive picture of the privacy environment around biometrics use in the Ministry.

However, the framework provided by this PIA and its appendices has to be incorporated into operational policies and procedures so that the reviews are performed in a timely fashion and the Privacy Commissioner is given adequate time in which to consider the changes and comment on them.

The requirements in section 32(3) suggest that the Ministry should consider:

- Within wider privacy governance systems manage Ministry wide privacy issues/risk including having assigned owners, accountability and closure steps and dates.
- How the identified risks will be appropriately monitored, reviewed and controlled.
- What commitments have/will be made by management following adoption of this PIA.
- What arrangements have been made for audit compliance and enforcement mechanisms for the management of biometric information.
- What procedure has been established to log and periodically review complaints and their resolution with a view to improving management practices and standards.

The Ministry requires all significant changes that impact the collection and handling of biometric information to be subject to a PIA. This is evidenced by the updates resulting in the updates to the previous PIA 2012 and the now current PIA 2016. Each update is only relevant for as long as the fundamental assumptions upon which it is based, remain unchanged. As parts of the immigration system or processes are redesigned following completion of the current review and update, the PIA 2016 will be subject to a further update, as and when appropriate to do so.

11. CONCLUSION

The implementation of the Vision 2015 Programme has significantly enhanced the Ministry's ability to use biometric information and increased its future capability as part of an efficient immigration system. Confidence in accurate identity information is key to the Government's goals for immigration to have policies in place that make New Zealand an attractive place to visit, work and live. The Ministry is responsible for facilitating the arrival of migrants, students, workers and tourists while preventing the entry of individuals with false identity credentials and others who may pose risks to the country.

The PIA 2010 was the first step in the Ministry's progress to implementing the biometric provisions in the 2009 Act. It was the first step to meeting the compliance obligation in section 32(3) of the 2009 Act. This update provides a snapshot of the situation today and a description of future planned implementations. It has identified the main privacy related risks and put forward potential mitigations for those risks. Future implementations of biometrics in the Ministry will be informed by the risk analysis and potential mitigations.

Several potential biometric information handling risks are identified, most of which can be addressed with properly designed procedures and policies. As the Ministry will be increasingly collecting biometric information about everyone who applies for a visa, claims refugee status, or crosses the border, some security processes may require review and updating, and these are identified as security risks.

On-going consideration and revision of the PIA is crucial to the Ministry meeting its obligations under the 2009 Act and the Privacy Act 1993. To ensure that happens, it is strongly recommended that the Ministry attend to and assign the appropriate resources to the following:

1. Maintain its governance group to provide comprehensive oversight of all Ministerial privacy risks.
2. Develop comprehensive strategy and policy to manage all elements of information processing in the Ministry, including biometrics.
3. Create a risk register in which to log and monitor all privacy risks and assign accountability for them. Enforce monitoring of privacy risks to enable status updates and escalation of actions not taken in a timely manner to mitigate privacy risks.
4. Set up processes for the following:
    - 4.1 Systemic assessment for updating this PIA or situations where new ones are required.
    - 4.2 Audit of existing practices for collection and handling of personal information.
    - 4.3 Training and awareness for all staff above and beyond the current offering.
    - 4.4 Comprehensive oversight of all situations where Ministry information is being handled by third parties.

APPENDIX 1 – ABBREVIATIONS USED

(the) 2009 Act	Immigration Act 2009
ABIS	Automated Biometric Indexing System
AFIS	Automated Fingerprint Identification System
AMS	Application Management System
APEC	Asia Pacific Economic Cooperation
APP	Advance Passenger Processing
Corrections	Department of Corrections
Customs	New Zealand Customs Service
(the) Ministry	Ministry of Business, Innovation and Employment
DIA	Department of Internal Affairs
DMS	Document Management System
FCC	Five Country Conference
FMR	False match rate
FNMR	False non match rate
GCPO	Government Chief Privacy Officer
ICAO	International Civil Aviation Organisation
ICE	Intelligence Capability Enhancement
ICT	Information and communication technology
IDme	Identity Management Engine
IGC	Intergovernmental Consultations on Migration, Asylum & Refugees
IGMS	Immigration Global Management System
ILO	International Labour Organisation
ITU	International Telecommunications Union
IVS	Identity Verification Service
MFAT	Ministry of Foreign Affairs and Trade
MPI	Ministry for Primary Industries
MoJ	Ministry of Justice
MOU	Memorandum of Understanding
NZSIS	New Zealand Security Intelligence Service
NZTA	New Zealand Transport Agency
NIST	National Institute of Standards and Technology
OASIS	Organisation for the Advancement of Structured Information
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner
PET	Privacy-enhancing technology
PIA	Privacy impact assessment
PIRA	Preliminary impact and risk assessment
PIT	Privacy invasive technology
NZ Police	New Zealand Police
RIA	Regulatory impact analysis
SAML	Security Assertion Mark up Language
SRTP	Secure Real Time Platform
SSC	State Services Commission
TOR	Terms of reference
UI	Unique identifier
UK	United Kingdom of Great Britain and Northern Ireland
UNHCR	United Nations High Commissioner for Refugees
US	United States (of America)
Vision 2015	Immigration change programme

APPENDIX 2 – PRIVACY RISK MITIGATIONS ALREADY IN PLACE

The Ministry's updated Privacy Policy outlines a programme of privacy work in its supporting Strategy that includes an action around developing a privacy framework for the Ministry which include policies, standards, ownership and guidelines.

These privacy mitigations are arranged in the order of the information privacy principles in the Privacy Act 1993.

While these mitigations exist today, care will need to be taken that they remain as part of the Ministry's operational 'business as usual' and are updated where appropriate to incorporate biometric privacy considerations.

Principle 3

All visa applicants complete a formal online or paper-based visa application to enter or remain in New Zealand – there are differing versions depending on the different status applied for, e.g. Student Visa Applications.[78] All online and paper-based forms give indicative information about the processing of the information provided, including photographs.

All travellers crossing New Zealand's border complete an arrival or departure card that states that the (currently only biographic) information is being collected for immigration purposes. The cards state that the information collection is mandatory, required under the 2009 Act, contact information is provided for immigration information and enquiries, and Customs and the Ministry are clearly identified as the chief collection agencies with appropriate contact information provided.

There is a formal privacy statement explaining how the information may be shared among border agencies and a statement about authorised information matching programmes. That statement also includes information about rights of access and correction and contact information for exercising those rights.

SmartGate[79] gives eligible travellers arriving at New Zealand international airports the option to self-process through passport control. It uses the electronic information in the e-chip passport and facial recognition technology to perform the immigration checks that are usually conducted at the primary line.

The use of SmartGate is optional. People can still use the existing immigration process at the manual primary line. Information is provided to the traveller at the SmartGate kiosk, on the arrival and departure card and is available on the internet.

---

[78] http://www.immigration.govt.nz

[79] http://www.customs.govt.nz/features/smartgate/Pages/default.aspx

In the case of clients who are required to provide fingerprints a leaflet is available explaining the collection and handling of their biometric information, entitled *Immigration Fingerprint and Photograph Checks*[80.]

There is already information relating to the exchange of biometric data under the Five Country Conference (FCC) Protocol on the Ministry's public web site[81.]

Principle 4

The Ministry already collects biometric data in a sensitive and culturally appropriate manner. Where photos are required to be provided, this is done regardless of age (although, in a refugee context, fingerprints will not be taken from those under 14 years of age), ethnicity, religious or cultural background or belief.

The Ministry does not require people who wear headgear for religious or cultural reasons to remove this headwear, as long as it does not obscure the face. In cases where live photos are taken of the person, this may be done in a private room. Similarly, facial markings such as bindis are not required to be removed.

Principle 5

The foundation document on the intranet about information security is *ICT Acceptable Use Policy*[82,] which states that users must:

- Understand their personal responsibility as an information system user.
- Ensure that, when entering or leaving Ministerial premises, unauthorised persons do not gain access.
- Ensure that information is kept secure – this includes information that is paper based or electronic.
- Dispose of sensitive information effectively – shred, wipe disks, destroy media – and lock screens when away from their desk.

Conversely users must not:

- Disclose confidential or sensitive information to persons who are not authorised to receive it.
- Be careless with confidential or sensitive information carried on their person – this applies to both paper based and electronic information.

The intranet also has targeted guidelines for groups such as managers and other supporting documents.

The Ministry has processes in place to manage access to and security of all personal information. Those processes have evolved to encompass the current

80 http://www.immigration.govt.nz/NR/rdonlyres/DCB4582E-3230-4656-BD97-0BFE120DFDAA/0/DOL11500AImmigrationFingerprintandPhotographChecksA4flierEnglishonly.pdf
81 http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/
82 MBIE ICT Acceptable Use Policy - http://thelink/how/Documents/ict-acceptable-use-policy.pdf

reliance on paper-based primary documentation and are supported by automated systems, for example, Conduct Privacy Impact Assessment, Conduct Privacy Incident Assessment, Conduct Personal Information Access and / or Correction Request. These provide access to key information collected on INZ's clients.

Physical protection for paper documents includes the use of locked filing rooms for visa applications in branches and clear desk policies for officers handling personal information. INZ expects to manage less hard copy documents over time with its transition to online visa applications.

The current handling of biometric information is, in part, controlled by those existing processes and, in part, by newly devised and evolving processes and systems. The Identity Report relies on Identity Access Management system restrictions to control access to the images of faces and document scans (including passports) in the database. The implementation of SRTP relies on compliance with and adherence to several Government ICT Security standards and a requirement for the security of each initiative handling biometric information to achieve MBIE Security Accreditation.

Internal compliance and policing of these policies is undertaken by the Security Risk function. At the time of the PIA 2016 update, the Ministry's Compliance Management Framework and Compliance Policy were under development.

Current responsibilities of the Security Risk function include monitoring system usage and, where necessary, acting on cases where use or access may be deemed unnecessary, suspicious or otherwise untoward. The MBIE Information Security Policy outlines minimum security standards, including both physical and technical security requirements.[83]

Where fingerprints are shared with FCC partners, processes that encrypt the fingerprints whenever they are being transferred (physically or electronically) and new limited access equipment are employed to protect the biometric information.

Those processes have been reviewed and evolved where required, as the Ministry continues to move towards implementation of new initiatives.

This principle further requires that the Ministry ensures that, if it provides biometric (or other personal) information to another agency for the purposes of the provision of a service, everything in the Ministry's power must be done to prevent the unauthorised use or disclosure of the information. Although not explicit, this generally requires contractual terms to ensure that the service provider protects the Ministry's information adequately.

Principles 6 and 7

The Ministry meets this requirement and provides in its internal policies and procedures for the right of access and correction to people about whom it has

83 MBIE ICT Information Security Policy
http://thelink/how/Lists/Security%20Policy/policies.aspx?RootFolder=%2Fhow%2FLists%2FSecurity%20Policy&

made a decision on an immigration matter. That right applies to anyone whose information is held in an accessible form by the Ministry. Specifically:

> *In immigration matters, where the Ministry has made a decision on a person's application for a permit or a visa, the Ministry's policy is to respond to requests as if the person were eligible to make a request, even where they are not a New Zealand citizen or resident, and are outside New Zealand.* [84]

Even if any person is refused access to personal information, the letter they receive includes reference to their ability to contact the Office of the Privacy Commissioner. This is so that they can make their views known to the Commissioner or receive confirmation directly from the Commissioner that she has no jurisdiction to investigate the matter.

Principle 8

Currently, the Ministry relies on Police experts to assess any apparent match between a sample fingerprint and fingerprints in the immigration fingerprint database. The implementation of IDme will see the transfer of Immigration fingerprints from the NZ Police database into the Ministry's IDme database. Although the fingerprint database will be part of IDme, the Ministry will continue to rely on the expertise of NZ Police fingerprint experts when manual resolution of fingerprint matching exceptions is required.

It is Ministerial policy that applicants are informed of any 'potentially prejudicial information' that the Ministry may hold and that they are given an opportunity to respond to or explain the circumstances behind that information.[85] There is a standard letter sent to applicants in these circumstances. Officers are also advised to 'consider all the facts, keeping an open mind towards all relevant forms of evidence; and distinguish fact from opinion, rumour, allegation, assumption or report'.

Principle 9

The Ministry has a dedicated business function to manage all aspects of records management, though does not, as yet, have a consolidated electronic document records and management system. The policies managed by this unit do not distinguish between paper based and electronic records; therefore, periods of retention (and methods of deletion) are implicit within the available guidance.[86]

---

[84] *Privacy Act Policy 2005*. Wellington: Department of Labour, October 2005. Section A.3 http://www.dol.govt.nz/PDFs/privacyactpolicy.pdf

[85] *Immigration Operational Policy Manual*. Section A 1.5 Fairness. Wellington: Department of Labour, Updated 29 November 2010. http://inzkit/publish/opsmanual/

[86] http://thelink/how/Pages/identify-and-manage-records.aspx

APPENDIX 3 – MATRIX OF INITIATIVES BY SECTION

Biometric information may only be collected in relation to those sections of the Immigration Act 2009 which specifically enable the collection of biometrics. The following table outlines the sections of the Act that are relevant and these are cross referenced with the Ministry's biometric initiatives, indicating the supporting assessment in the enclosed appendices.

Section 96 of the Immigration Act 2009 is not referenced in the table below. It enables the collection of biometric information by airlines as part of the Airline Passenger Processing (APP) process, as they are the agents acting on behalf of the Ministry under sections 99 and 100 of the Act.

Sections 100 and 104 of the 2009 Act, although provided for and mandated, are not fully activated yet. The provisions are in place and biometric information is collected on an ad hoc and case by case basis by requesting a photo of an individual. When these provisions are to be applied systematically, this document will be updated.

Section 100 enables photographs and images of New Zealand citizens to be retained when they opt in to use the SmartGate operations owned by Customs at all New Zealand international airports.

Biometric Initiatives	**Appendix**	**Immigration Act Section**													
		60	**99**	**100**	**104**	**111**	**120**	**149**	**287**	**288**	**289**	**290**	**291**	**305**	**306**
Face Biometrics	4	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Manual Data Sharing	5	x				x		x						x	x
Automated Data Sharing	6	x		x		x		x		x				x	x
Criminal Removals	7									x				x	x
Refugee Status Branch Enrolment	8					x		x						x	x
Quota Refugees	9					x		x						x	x
Biometrics and Special Biometrics to enable deportation	10								x	x	x	x	x	x	x

Invest-igations	11	x		x	x	x		x		x				x	x
Data Matching Capability	12	x	x	x	x	x	x	x	x	x	x	x	x	x	x

APPENDIX 4 – FACE BIOMETRICS

Background

In addition to the usual format of biometric information that is collected, i.e., photographs on applications, Immigration New Zealand (INZ) and the New Zealand Customs Service (Customs) use passport readers to improve the speed and accuracy of data entry, passport verification and automated face / travel document image capture.

The passport images are captured by the smart passport reader from a customer's passport.

Live capture of client photographs is also used in some circumstances. Refer to Appendices 8, 9 and 11.

Smart passport readers:

- Capture biographical data from the machine readable zone (MRZ) and/or the e-chip if the passport has one; and
- Conduct security tests to determine if the passport is genuine and unaltered; and
- Read and authenticate the e-chip in passports equipped with them; and
- Capture an image (scan) of the bio page in the passport including the photo; and
- Capture the digital photo from e-chip equipped passports.

People can choose to use the SmartGate passport readers and they are aware when using the reader services that their images will be collected. Passport readers at INZ connect to the Ministry of Business, Innovation and Employment's (the Ministry's) secure network. Primary line systems connect to Customs' secure network and applications. The face biometrics and bio page images collected by INZ are stored in the INZ Image System and linked to the client's immigration identity number in the INZ Application Management System (AMS).

When IDme is implemented, Daon Enrol (a component of IDme) will capture biometric and biographic identity information, and capture scans of all supporting documentation. This information will be stored in the Document Management System (DMS).

Passport images will be collected from:

- Any foreign nationals; and
- Persons who claim to be New Zealand Citizens where their identity is in doubt. INZ retain images where New Zealand Citizenship is proven.

There are exceptions where a passport photo image may not be collected, such as emergency visas and sometimes diplomatic visas.

IDme will use biometric facial images

IDme will introduce facial biometrics software in 2016, which will allow existing client records (biographic and / or biometric) to be linked and will enable INZ to identify potential immigration and identity fraud cases. IDme will enable new facial images to be collected and subsequently a new identity created. Matched

facial images and biographic information, whether for new or existing identities will be held in the IDme database.

New Zealand Citizens Face Images

When making a determination of a New Zealand citizen's face image, the passport image is used to conduct identity verification against records held by the Department of Internal Affairs (DIA). If the immigration officer disproves, or cannot confirm the person's citizenship, the passport images will be kept.

If a visa holder becomes a New Zealand citizen, INZ will retain historical images for immigration purposes, but further images are unlikely to be collected once citizenship is granted.

Face Biometrics of Visa Applicants

INZ face biometric images are used to enable visa applicants to obtain an Identity Verification Service (IVS) account as part of the immigration process.

This is an opt-in customer choice. The 'co apply' approach will facilitate the issuance of an IVS credential for visa holders to access government services online after they arrive in New Zealand.

Face Biometrics of Children

Images of children under 10 years of age will be stored following the implementation of the IDme technology and will be available for searching.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

Section 104 refers to the photographing of NZ citizens on arrival. This is permissible under the Act but is not yet in force.

Section	Section Description	Client Group
60	Biometric information may be required from visa applicant.	All visa applicants, including at the border
99	New Zealand citizen may confirm citizenship before arrival in New Zealand.	New Zealand Citizens
100	Collection of biometric information from proposed arrivals.	All non-NZ Travellers
104	New Zealand citizens photographed on arrival.	New Zealand Citizens
111	Collection of biometric information.	Applicant for entry permission

120	Persons other than New Zealand citizens leaving New Zealand to allow biometric information to be collected.	All non-NZ Travellers
149	Powers of refugee and protection officers.	Refugee and asylum claimants
287*	Special powers pending deportation or turnaround	Non NZ nationals where required by 3rd country
288	Requirement to allow collection of biometric and special biometric information.	All non NZ nationals
289 to 291	An immigration officer may apply to a court for an order compelling the collection of biometrics if necessary (sections 289 to 291). Section 291 also provides further ability to apply for a compulsion order.	Persons liable for deportation or turnaround
305 & 306	Enables Ministry to exchange information, including biometric information	All passengers and crew

*Under Section 287 Special biometric information means, any of the following that are or may be required in order to meet the entry or transit requirements of any country to which or through which the person is to travel:

(a) the person's palm-prints:
(b) the person's footprints:
(c) measurements of the whole person:
(d) photographs of the whole person.

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
G4	Authorisation to access biometric information is too widely approved	Access to biometric information only available to approved INZ staff.
G5	Inadequately managed collaboration and information sharing with other agencies puts biometric information at risk	Passport images are captured by INZ staff, by Customs Officers at the border who are delegated as Immigration Officers under section 465 of the Act, and/or by automated systems (i.e. SmartGate). Information sharing agreements with other government agencies include measures to prevent unauthorised use or disclosure of biometric information.
G6	Inadequately managed outsourcing does not adequately protect	Passport images are captured by INZ staff, by Customs Officers at the border

Risk	Initiative specific risk(s)	Mitigation(s)
	biometric information	who are delegated as Immigration Officers under by s465 of the Act, and/or by automated systems (i.e. SmartGate). Future agreements with outsourcing providers will cover biometrics collected and delivered to INZ. All outsourcing providers will be required to delete any biometrics collected upon the successful secure transfer of data to INZ. Measures will be included to prevent unauthorised use or disclosure of biometric information.
H1	Biometric information unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification.	Ensure that all implementations of the biometric provisions in the Act are in line with the statutory authority. Limit collection of biometric information to what is <u>needed</u> (essential business justification) to support current decisions.
H2	Staff make arbitrary requests for biometric information.	Passports and client photographs are required by <u>all</u> foreign nationals during immigration application processes (as standard but there is discretion not to). Staff will not have discretion that can be abused. At the border, passport images will be collected from <u>all</u> people referred from the primary line who presented as New Zealand citizens. Staff will not have discretion that can be abused.
H3	Biometric information not collected directly from the person concerned.	Passport images will be collected from the passport presented by the person as part of an immigration process.
H4	People not adequately informed about the purposes of collection of biometric information.	Privacy information is provided through INZ customer information channels (forms, arrival / departure cards, web and leaflets). The INZ Biometric PIA is published on INZ's public web site (www.immigration.govt.nz).
H5	The manner in which biometric information collected is unfair or intrusive.	The Ministry collects and will continue to collect biometric data in a sensitive and culturally appropriate manner. The Ministry has procedures for handling cultural and physical considerations.

Risk	Initiative specific risk(s)	Mitigation(s)
H6	The right of people outside the country who are not New Zealand citizens or residents, to access and request correction of their biometric information.	In immigration matters those people will be treated as if they have the same rights as citizens and residents. This meets the requirements under section 34 of the Privacy Act 1993 as amended on 8 September 2010.
H7	The Ministry is unable to respond effectively to requests for personal information or to investigations by the Privacy Commissioner (and others) because of inadequate system design.	The Ministry already has procedures in place for requests for personal information. IDme will provide additional Look-Up and Extract Information functionality in support of Privacy Act requests and investigations.
H8	Biometric information incorrectly associated with a person.	The use of face images will reduce the chance of incorrectly associating biometric information with a person. The Smart Passport Readers will increase the accuracy of data entry and all images captured from the passport are uploaded directly against the client's records. Staff will be trained to ensure that the correct image is uploaded to the correct client. Correcting errors is easier when using face images than using biographic data comparison only. The system allows for correction of any mismatches if they occur. IDme functionality will enable biographic and biometric matching; increasing assurances that biometric information is associated to the "right" person.
H9	Inaccurate or incorrect biometric data is used to make a decision about a person.	All potentially prejudicial information will be presented to the customer for their comment or rebuttal prior to a final decision.
H10	Information kept longer than is necessary.	Passport and face images retained for 50 years from date of capture). If the immigration officer determines that doubt remains about the person's claim to NZ citizenship, the image will be retained until the investigation is completed.
H11	Biometric information used for non-immigration purposes.	Staff will be trained to ensure awareness in permitted uses of biometric

Risk	Initiative specific risk(s)	Mitigation(s)
		information. Specific training will be provided to specialists managing complex identity resolution involving facial biometrics.
H12	Disclosure of biometric information without reasonable grounds.	Staff will be trained to ensure awareness in permitted uses of biometric information.
H13	Unnecessary assignment of unique identifiers.	Continue the current process of assigning unique INZ identifiers to people and records.
H14	Widespread use of biometric templates as unique identifiers.	Biometric templates will not be shared with other agencies unless supported by legally approved information sharing agreements and privacy impact assessments.
S1	Loss of biometric information.	All information will be kept and handled securely according to the Ministry's ICT security procedures.
S2	Unauthorised access to biometric information.	Access to biometric information is only available to approved INZ staff unless supported by legally approved information sharing agreements and privacy impact assessments. All information will be kept and handled securely according to the Ministry's ICT security procedures.
S3	Safeguards implemented to ensure the security of biometric information are not reasonable (adequate) in the circumstances.	All information will be kept and handled securely according to the Ministry's ICT security procedures.

Date finalised: 13 May 2016

Version number: V1.2

APPENDIX 5 – FCC PROTOCOL MANUAL DATA SHARING

Background
The Five Country Conference (FCC) Protocol ('The Protocol') enables FCC partners to run, on a case by case basis, searches of high risk client's fingerprints against each other's databases in order to detect identity and immigration fraud. All fingerprints for matches and non-matches are deleted by the receiving country once the checks have been completed.

If there is a successful match, further information is shared bilaterally (this may include biographic details and other immigration records in accordance with FCC bilateral agreements).

Four PIAs for implementation of the Protocol have been developed in consultation with the Office of the Privacy Commissioner (OPC), one each between Immigration New Zealand (INZ) and the border / immigration authorities of the United States, the United Kingdom, Australia and Canada. INZ has been manually sharing data with all four partners since April 2011.

INZ is supported by the NZ Police who provide resolution services, including fingerprint matching and expertise. A Memorandum of Understanding (MOU)[87] between the Ministry and the NZ Police exists, formalising these services, including the sharing of information and enabling strategies to take advantage of new technology. The MOU includes provisions to ensure information will be shared in compliance with the Privacy Act 1993.

INZ is transitioning away from managing and matching biometric information manually, however this will be a gradual transition, and will always require human intervention for the matches that are complex and cannot be automated to complete successfully.

Fingerprints stored by the NZ Police on behalf of the Ministry for INZ clients, will be transitioned for storage from the INZ Automated Fingerprint Identification System (AFIS) (which is fully segregated from the NZ Police criminal fingerprint database) to INZ's new identity management system, IDme in 2016. This will reduce the sharing of files manually between INZ and NZ Police. INZ will continue to require the services of Police Fingerprint specialists (refer Appendix 12 Data Matching Capability). During the transition, data is being migrated to the new NZ Police database, Automated Biometric Indexing System (ABIS) until IDme is implemented.

IDme provides technology to enable the automated matching capability of biometric and biographic information and to provide for the storage of fingerprints within INZ. The introduction of IDme technology will enable the Ministry to store all fingerprints. NZ Police will continue to provide matching / resolution support to INZ for complex fingerprint cases that are unable to be matched automatically by IDme, NZ Police will also continue to support INZ in its collection of fingerprints for deportation processes.

Up to 3,000 fingerprint requests per year per country with a three day response time can be managed. Requests beyond this number may be actioned at the discretion of the providing country.

---

[87] Memorandum of Understanding between the Ministry of Business, Innovation and Employment and the NZ Police, January 2015

In addition to the automated data matching capability provided by the implementation of IDme, further technical capability will be enabled with the implementation of Secure Real Time Platform (SRTP) in 2016. Refer Appendix 6 which provides an assessment of the privacy impact of increased automation to enable real time processing of fingerprints with FCC partners.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

Section	Section Description	Face	Fingerprint	Client Group affected
60	Biometric information may be required from visa applicant	X	X	Visa applicant
111	Collection of biometric information	X	X	Applicant for entry permission
149	Powers of refugee and protection officers	x	x	Refugee and asylum claimants
305 & 306	Enables Ministry to exchange information, including biometric information	x	x	All passengers and crew

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
G4	Authorisation to access biometric information is too widely approved	Access to biometric information only available to approved INZ and authorised third parties.
G5	Inadequately managed collaboration and information sharing with other agencies puts biometric information at risk	Fingerprints are collected and stored by NZ Police staff acting on behalf of the Ministry for immigration purposes, until such time as they are transitioned to IDme. Information sharing agreements with other government agencies include measures to prevent unauthorised use or disclosure of biometric information.

Risk	Initiative specific risk(s)	Mitigation(s)
G6	Inadequately managed outsourcing does not adequately protect biometric information	Future agreements with outsourcing providers will cover biometrics collected and delivered to INZ. All outsourcing providers will be required to delete any biometrics collected upon the successful secure transfer of data to INZ. Measures will be included to prevent unauthorised use or disclosure of biometric information.
H1	Biometric information unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification	Only fingerprints of high risk clients are collected for checking via the Protocol. The initial use of pseudonymous fingerprints to determine if the agencies involved share an interest in an individual is considered privacy protective. Alternative processes would be more vulnerable to subjective assessments of interest rather than an objective measurement of the similarity of two examples of a physical characteristic. All fingerprints are deleted by the receiving country once the match checks have been completed.
H2	Staff make arbitrary 'requests' for biometric information	Only fingerprints of high risk clients are collected for checking via the Protocol. Definition of 'high risk' is defined by INZ business rules and operational policy.
H3	Biometric information not collected directly from the person concerned	All biometric information collected for use in the Protocol is done so directly from the person concerned. INZ is authorised under the Immigration Act 2009 to exchange information with equivalent authorities in other countries for immigration purposes by virtue of ss.305 and 306 in the Immigration Act 2009
H4	People not adequately informed about the purposes of collection of biometric information	The INZ website contains detailed information about biometric collection and data sharing with FCC partners[88].

[88] http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/fccqa.htm

Risk	Initiative specific risk(s)	Mitigation(s)
		A multilingual leaflet is given to all subjects fingerprinted by INZ explaining why we are collecting their fingerprints and how their biometrics will be handled.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their biometric information	The Protocol requires participating countries to abide by all legal requirements within their own countries, including those relating to privacy. All INZ clients can request a copy of their biometric information from INZ. This same right is mirrored across FCC partners.
H7	The Ministry is unable to respond effectively to requests for personal information or to investigations by the Privacy Commissioner (and others) because of inadequate system design	The Ministry has procedures in place for requests for personal information. IDme provides functionality for Identity Services Analysts and Privacy Officers to look up requests directly in IDme to facilitate client requests under the Privacy Act 1993
H8	Biometric information incorrectly associated with a person	Fingerprints are collected directly from the individual, and their biographic details are entered directly into the fingerprint record itself (i.e. no cross linking required)
H9	Inaccurate or incorrect biometric data is used to make a decision about a person	The accuracy of any matching tool is dependent on the quality of the data it is matching. It is possible that biometric information associated with a client may be inaccurate. IDme has inbuilt quality controls around biometric information, so over time, IDme matching processes should progressively resolve exceptions. Further, photos of the subject are also shared following a match. Lastly, all applicants are informed of information that might harm their case (often referred to as "potentially prejudicial information" or PPI) and given a reasonable opportunity to respond to harmful information.
H10	Biometric information retained longer than necessary	All Protocol fingerprints collected by FCC partners are automatically deleted after the search has been completed. All other information is retained for 10 years as specified by the Protocol.

Risk	Initiative specific risk(s)	Mitigation(s)
H11	Biometric information used for non-immigration purposes	The Protocol has assigned 'Search Codes' which dictate what may be searched and what may not. This also controls what information is released if a match occurs. The information that New Zealand receives from FCC partners will be used exclusively for immigration and identity purposes in both countries.
H13	Unnecessary assignment of unique identifiers	INZ does not use AMS client numbers when checking clients under the FCC Protocol – a uniquely generated number is used.
S2	Unauthorised access to biometric information	IDme has undertaken a rigorous security risk assessment process and will be required to pass a formal security accreditation process to ensure that appropriate physical and technical security standards are in place. This will provide assurance that the required protection to fingerprints is in place after the holdings have been migrated from ABIS to IDme. INZ is required under the Protocol and the MOU with Police to take care to protect the information against loss, misuse, and unauthorised disclosure. Information will be encrypted by an internationally accepted protocol and handled in New Zealand as required by a "restricted" classification. All fingerprint information provided by FCC partners will be securely deleted from the secure file server once the match cycle has ended. Only specified employees of INZ will be permitted access to the information and all access will be logged and audited. Both FCC and New Zealand agencies are entitled to request an audit of the other's handling procedures to provide assurance that appropriate security is in place.

Date finalised:
December 2010 (PIA for data sharing with Canada)
November 2010 (PIA for data sharing with US)
September 2010 (PIA for data sharing with UK)
June 2010 (PIA for data sharing with Australia)

Amendments to this appendix included 13 May 2016

Version number: V1.2

APPENDIX 6 – FCC PROTOCOL AUTOMATED DATA SHARING (SRTP)

Background

INZ is implementing an automated data sharing capability with Five Country Conference (FCC) protocol partners in line with the existing data sharing agreements[89]. The main component is the development of a real time data sharing platform - the 'Secure Real Time Platform' (SRTP) - which can be used to securely share fingerprint match requests and responses with FCC partners. This capability is in development. Implementation will commence in 2016 with FCC partner Australia. Other FCC partners will follow at a later date.

FCC fingerprint matching is a well-tuned and refined process that has been in place since April 2011 (refer Appendix 5). Responding to an FCC fingerprint matching request does however require the responding partner to manually process the response and therefore restricts the volume of fingerprint processing.

In the majority of cases, the implementation of SRTP will enable requests to be responded to automatically by the responding country partner, without the need for manual intervention.

There will be no increase in the personal data requested and shared with FCC partners (as defined in the agreement with each partner) only the process for sharing data changes. There is likely to be a reduction in the amount of supplementary information shared through the provision of additional documents.

The inclusion of SRTP in the sharing process will allow the initial request for a fingerprint match to be sent via SRTP to all FCC partners with SRTP enabled systems. This removes the need for spreadsheets, shared drives and for data to be stored in local repositories. It also eliminates having to decrypt and manually process the request.

If an initial request results in a match, a small amount of biographic data will be returned as a response. The requesting partner will assess the information provided and determine if there are grounds to request more.

The use of SRTP provides enhanced security for data both during transmission through network gateways and storage in processing systems.

The use of SRTP will enable less data to be shared in the initial SRTP response from FCC partners than the current process. The initial response will include only a 'yes/no' reply to a fingerprint match request with minimal biographic data included. This eliminates the sharing of other personal information (such as travel document details, other names and note or comments) linked to the

[89] http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/fccqa.htm

fingerprinting These documents can be provided if requested but are not automatically included in the initial response.

INZ staff will be provided with access to view the response results of the match request but will not be required to manually handle all data relevant to the request and/or response. This is a privacy enhancing step, reducing the risk of unnecessary data collection and sharing.

Whilst there will be no change in the type of personal data shared, there will be a change in the volume of fingerprint processing and an increase in ad hoc requests. Higher volumes will be processed due to the ability to share fingerprint information automatically for low-risk requests. Previously, reliance on manual data sharing meant that only high risk fingerprint requests were processed

It is anticipated that as many as 2 million requests per annum will be received by 2022 from all FCC partners by 2022. INZ anticipates raising approximately 300 thousand requests per annum for fingerprint processing to FCC partners within the same time frame.

Information exchanged between the FCC partners will be protected by robust technical security measures in keeping with Government and industry standards.

The SRTP implementation will be phased in over time progressively adding connections to FCC partners. It is designed to be used widely, facilitating efficient processing for low-risk clients as well as mitigating the risk of identity fraud.

Eventually SRTP enabled automated data sharing will replace the majority of manual data sharing activities for low-risk clients (refer Appendix 5) and will enable larger numbers of fingerprints to be processed in a more timely and efficient manner with all FCC partners.

FCC data sharing initiatives will continue to progress and will likely extend further than sharing fingerprint biometrics. This appendix will be updated to reflect the privacy assessment of future changes when they are due.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being affected by this initiative.

Section	Section Description			
		Face	Finger-print	Client Group affected
60	Biometric information may be required from visa applicants	X	X	Visa applicants

100	Collection of biometric information from proposed arrivals	X	X	All non-NZ travellers
111	Collection of biometric information	X	X	Applicant for entry permission
149	Powers of refugee and protection officers (and their agents)	X	X	Refugee and Asylum claimants
288	Requirement to allow collection of biometric information and special biometric information	X	X	Person liable for deportation or turnaround
305 & 306	Enables Ministry to exchange information, including biometric information	X	X	All passengers and crew

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
G5	Inadequately managed collaboration and information sharing with other agencies putting biometric information at risk	Individual PIA conducted with each overseas FCC partner. Measures taken to ensure that information sharing agreements do not compromise the Ministry's ability to meet its statutory obligations. Measures in place to prevent unauthorised use or disclosure of biometric information.
G6	Inadequately managed outsourcing does not adequately protect biometric information	Fingerprints are collected and stored by NZ Police staff acting on behalf of the Ministry for immigration purposes. Future transfer of fingerprints to IDme. Future agreements with outsourcing providers will cover biometrics collected and delivered to INZ. All outsourcing providers will be required to delete any biometrics collected upon the successful secure transfer of data to INZ. Measures will be included to prevent unauthorised use or disclosure of biometric information.
H1	Biometric information unnecessarily or excessively collected and retained,	Fingerprints of high-risk clients are collected for checking. Enhanced automated secure sharing capability will

Risk	Initiative specific risk(s)	Mitigation(s)
	including multiple types of biometric information (multi modal) collected without adequate justification	enable checking of low risk fingerprints to identify potential immigration and identity fraud. Increased volumes of fingerprint checking will be enabled but managed through business rules, operational policy and specifically by high matching thresholds. Inconsistent matches are manually resolved. The initial use of pseudonymous fingerprints to determine if the agencies involved share an interest in an individual is considered privacy-protective. Alternative processes would be more vulnerable to subjective assessments of interest rather than an objective measurement of the similarity of two examples of a physical characteristic. All fingerprints are deleted by the receiving country once the match checks have been completed.
H2	Staff make arbitrary 'requests' for biometric information	Business rules and operational policy will determine which clients will have fingerprint checks undertaken via the Protocol. Ad hoc requests will be made by access-controlled role profiles and access will be logged for audit trail. Staff will follow operational policy and business rules when requesting ad hoc searches.
H3	Biometric information not collected directly from the person concerned	All biometric information collected for use in the Protocol is done so directly from the person concerned. INZ is authorised under the Immigration Act 2009 to exchange information with equivalent authorities in other countries for immigration purposes by virtue of s.305 and 306 in the Immigration Act 2009.
H4	People not adequately informed about the purposes of collection of biometric information	The INZ website contains detailed information about biometric collection and data sharing with FCC partners. A multilingual leaflet is currently given to all

Risk	Initiative specific risk(s)	Mitigation(s)
		subjects fingerprinted by INZ explaining why we are collecting their fingerprints and how their biometrics will be handled. Communications will be reviewed for future changes.
H5	The manner in which biometric information collected is unfair or intrusive	Include appropriate responses in operational policy, business processes and staff training/awareness to cultural and physical considerations when collecting biometric information.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their biometric information	The Protocol requires participating countries to abide by all legal requirements within their own countries, including those relating to privacy. All INZ clients can request a copy of their biometric information from INZ. This same right is mirrored across FCC partners.
H7	The Ministry is unable to respond effectively to requests for personal information or to investigations by the Privacy Commissioner (and others) because of inadequate system design	The SRTP system is being designed taking into account OIA and privacy request requirements. IDme provides functionality for Identity Services Analysts and Privacy Officers to look up requests directly in IDme to facilitate client requests.
H8	Biometric information incorrectly associated with a person	Fingerprints are collected directly from the individual, and their biographic details are entered directly into the fingerprint record itself (i.e. no cross-linking required). The data is double checked before fingerprints are uploaded. There is always a risk of incorrect match decisions being made. It is not possible to entirely mitigate against this risk but this can be partially mitigated by setting an appropriate match threshold to minimise false matches. Additionally, data collected on false matches will be reviewed when available to further reduce the likelihood and/or consequences as much as possible.
H9	Inaccurate or incorrect biometric data is used to	AFIS are extremely accurate particularly using all ten fingerprints (which the

Risk	Initiative specific risk(s)	Mitigation(s)
	make a decision about a person	Protocol does). IDme may mirror the thresholds used by NZ Police in AFIS but the threshold can be lowered. Any matching exceptions are referred to NZ Police for decision. Further, photos of the subject are also shared following a match. Lastly, all applicants are informed of information that might harm their case (often referred to as "potentially prejudicial information" or PPI) and given a reasonable opportunity to respond to harmful information. The accuracy of any matching tool is dependent on the quality of the data it is matching. It is possible that biometric information associated with a client may be inaccurate. IDme has inbuilt quality controls around biometric information, so over time, IDme matching processes should progressively resolve exceptions.
H10	Biometric information retained longer than necessary	All Protocol fingerprints are automatically deleted after the match process has been completed. All other information shared within the Protocol is retained for a 10-year period.
H11	Biometric information used for non-immigration purposes	The Protocol has assigned 'Search Codes' which dictate what may be searched and what may not. This also controls what information is released if a match occurs. The information that New Zealand receives from FCC partners will be used exclusively for immigration and identity purposes in both countries.
H12	Disclosure of biometric information without reasonable grounds	Maintain specific guidelines on the release and disclosure of biometric information in to operational policy, business processes and staff training. Ensure staff understanding of their responsibilities through training, awareness and other support materials.

Risk	Initiative specific risk(s)	Mitigation(s)
H13	Unnecessary assignment of unique identifiers	The URL used to access the SRTP UI includes the AMS client number.
S2	Unauthorised access to biometric information	Compliance with several Government Security Standards is required in addition to achievement of MBIE Security Accreditation. IDme has undertaken a rigorous security risk assessment process and will be required to pass a formal security accreditation process to ensure that appropriate physical and technical security standards are in place. This will provide assurance that the required protection to fingerprints is in place after the holdings have been migrated from ABIS to IDMe. INZ is required under the Protocol and the MOU to take care to protect the information against loss, misuse, and unauthorised disclosure. Information will be encrypted by an internationally-accepted protocol and appropriate handling instructions are applied. All fingerprint information will be securely deleted from the secure file server once the match cycle has ended. Only specified employees of INZ will be permitted access to the information and all access will be logged and audited. Both FCC and New Zealand agencies are entitled to request an audit of the other's handling procedures to provide assurance that appropriate security is in place.

Date finalised: 13 May 2016
Version number: V2.1

APPENDIX 7 – FCC CRIMINAL REMOVALS

Background

Biometric (face and fingerprints), biographic and criminality information will be received from, and sent to Five Country Conference (FCC) partners on foreign nationals removed from FCC borders who have committed serious criminal convictions (currently being done only with UK partner).

The Participants may exchange, using secure mechanisms, relevant immigration information which may include, but is not limited to:

- Immigration history and immigration status;
- Details of known suspected immigration abuse and offences, including overstays of authorised presence in a country, or peoples and/or goods smuggling;
- Criminality and other information that is pertinent to immigration and nationality purposes;
- Copies of travel documents or other identity documents;
- Such other information as the Participants may mutually consider appropriate.

Information exchanged will be provided as a result of a foreign national being deported / removed due to their criminal history and in line with the criteria outlined in bilateral MOU's between each country.

New Zealand will apply section 15 of the Immigration Act 2009 when determining information to share under this arrangement. This includes persons:

- Convicted of an offence and sentenced to imprisonment for a term of 5 years or more, or for an indeterminate period capable of running for 5 years or more; or
- At any time in the preceding 10 years has been convicted of an offence and sentenced to imprisonment for a term of 12 months or more, or for an indeterminate period capable of running for 12 months or more.

Fingerprints and facial biometrics, as well as biographic data are collected and sent to INZ by FCC partners on persons with serious criminal convictions who have been deported from their borders. This may include citizens of FCC countries, including New Zealanders.

FCC inbound identities search and match against AMS clients. Alerts are raised against existing clients where a match is made, or new clients created where a match is not made. Inbound face images are collected and stored against the appropriate identity and alert.

The implementation of the IDme search engine in 2016 will enable increased automation and quicker processing of new and existing information to specifically

combine and match identity information, including biographic information from passport smart scanners to biometric information such as facial images and fingerprints.

INZ currently receive, match and store fingerprints on the AFIS database held by New Zealand Police (NZ Police). NZ Police supports INZ by providing fingerprint resolution expertise, where required. This resolution expertise will continue with the implementation of IDme. A Memorandum of Understanding (MOU)[90] between the Ministry and the NZ Police exists, formalising these services, including the sharing of information and enabling strategies to take advantage of new technology. The MOU provides assurance that information will be shared in compliance with the Privacy Act 1993.

Fingerprint match results will be provided to INZ for auditing and investigation purposes and will transition from the NZ Police to be stored by INZ with the implementation of IDme matching technology (Refer Appendix 12).

The purpose of collecting and sharing biometric information on foreign nationals removed from FCC borders is to:

- Raise alerts against persons not permitted entry to NZ for criminality reasons.
- Assist in identity establishment – biometric enabled identity management enables the Ministry to be sure that the person has not already made an immigration application under another identity.
- Ensure reliable identification of people in subsequent transactions both with the Ministry and other agencies – the Ministry is the authoritative source of identity information for non-New Zealand citizens.
- Conduct international identity checks with partner countries under the FCC Protocol.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

Section	Section Description	Biometric type		Client Group
		Face	Finger print	
120	Foreign nationals leaving New Zealand to allow biometrics to be collected.	X	X	Any person leaving New Zealand who is not a New Zealand Citizen.

[90] Memorandum of Understanding between the Ministry of Business, Innovation and Employment and the NZ Police, January 2015

288	Requirement to allow collection of biometric information and special biometric information	X	X	Any person liable for deportation or turnaround.
305 & 306	Enables Ministry to exchange information, including biometric information	X	X	All passengers and crew

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
G3	Unnecessary expense incurred because systems are not designed from the beginning to include privacy considerations.	• Incorporate 'privacy by design' into the Foreign Criminal Alerts solution, including reporting. • Ensure a PIA is undertaken (consistent with legislative obligations) for this project prior to their design/build phase and add as an appendix to this PIA.
G4	Authorisation to access biometric information too widely approved.	• Establish adequate controls around granting authorisation to access biometric information held on identities shared with and received from FCC partners. • Design audit processes into systems used to store or process biometric information to control user accounts, access rights and security authorisations. • Base access rights to biometric information on the need to know (essential business justification).
G5	Inadequately managed collaboration and information sharing with other agencies putting biometric information at risk.	• Include privacy considerations in collaborative undertakings with NZ Police and FCC Partners. • Ensure that information sharing agreements do not compromise the Ministry's ability to meet its statutory obligations. • Require measures to prevent unauthorised use or disclosure of biometric information by FCC partners and NZ Police.

Risk	Initiative specific risk(s)	Mitigation(s)
H1	Biometric information is unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification.	• Ensure that all implementations of the biometric provisions in the 2009 Act are in line with the statutory authority. • Biometrics will only be collected and stored onshore from persons who will be deported due to criminality threshold set in legislation. • Biometrics will only be received and stored from FCC countries against persons who have been deported from FCC borders due to criminality, which is set out in the bi-lateral MOU's.
H2	Staff make arbitrary 'requests' for biometric information	• Build targeted guidelines into operational policy, business processes and staff training/awareness for 'requesting' biometrics from persons being deported for reasons of criminality. • Train staff in the application of the Ministry's Code of Conduct and the exercise of it in situations where professional judgment is required.
H3	Biometric information not collected directly from the person concerned.	• Establish privacy protective processes for handling biometric information collected from FCC partners through bi-lateral MOU's. • Fingerprints collected by INZ will be acquired directly from the individual, and their biographic details entered directly into the fingerprint record itself.
H4	People not adequately informed about the purposes of collection of biometric information.	• People will be appropriately notified in a relevant manner whenever biometric information is collected from them. • Build an acknowledgement of biometric collection into the compliance process.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their biometric information.	• Ensure FCC bi-lateral MOU's contain expectations of partners to adequate inform their clients of use of biometrics, and that partners abide by all legal requirements within their own countries, including those relating to privacy. • All INZ clients can request a copy of their biometric information from INZ. This same right is mirrored across FCC partners.

Risk	Initiative specific risk(s)	Mitigation(s)
H8	Biometric information incorrectly associated with a person.	• All inbound fingerprints from FCC partners will be labeled with the AMS client number prior to being stored in the AFIS; • All outbound fingerprints, face and biographic data will be manually checked for matching accuracy before being sent to FCC partners once SRTP is implemented. The IDme report may require manual edits to include further information (such as sentencing information) and therefore all data is checked; • Any mismatched data will be rectified prior to sending or not sent to FCC partners.
H9	Inaccurate or incorrect biometric data is used to make a decision about a person.	• Processes for handling false negatives and false positives when matching biometrics will be developed.
H10	Biometric information retained longer than necessary.	Business rules will be developed to: • ensure biometrics are not retained for longer than 50 years from date of capture; and • are deleted as specified in the bi-lateral MOU's.
H11	Biometric information used for non-immigration purposes.	The information that New Zealand will receive from and share with FCC partners will be used exclusively for immigration and identity purposes in both countries.
H12	Disclosure of biometric information without reasonable grounds.	Staff will be trained to ensure awareness in permitted uses of biometric information. Appropriate audit and security processes will be in place.
H13	Unnecessary assignment of unique identifiers.	Continue the current process of assigning unique INZ identifiers to people and records.
H14	Widespread use of biometric templates as unique identifiers.	Biometric templates will not be shared with other agencies.
S1	Loss of biometric information.	All information will be kept and handled securely according to the NZ Police and the Ministry's ICT security procedures.
S2	Unauthorised access to, use, disclosure and modification of biometric information.	Access to biometric information only available to approved NZ Police and INZ staff. All information will be kept and handled securely according to NZ Police and the Ministry's ICT security procedures.

Risk	Initiative specific risk(s)	Mitigation(s)
S3	Safeguards implemented to ensure the security of biometric information are not reasonable (adequate) in the circumstances.	All information will be kept and handled securely according to NZ Police and the Ministry's ICT security procedures.

Date finalised: 13 May 2016
Version number: V1.2

APPENDIX 8 – REFUGEE STATUS BRANCH ENROLMENT

Background

Biometric information in the form of fingerprints is collected from asylum claimants aged 14 or over.

The fingerprints are collected and used to confirm their identity and background. These are checked against Five Country Conference (FCC) partner databases under the FCC Protocol. Face images are collected for claimants of all ages and stored for INZ reference but not currently used for automated biometric matching purposes. When IDme is implemented both face and finger biometrics will be matched against INZ's internal holdings. Fingerprints will continue to be matched with FCCs.

The purpose of collecting biometric information from asylum claimants under investigation is to:

- assist in identity establishment – biometric enabled identity management enables the Ministry to be sure that the person has not already made an immigration application under another identity,
- ensure reliable identification of people in subsequent transactions both with the Ministry and other agencies – the Ministry is the authoritative source of identity information for foreign nationals; and
- conduct international identity checks with partner countries under the FCC Protocol.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

Section	Section Description	Biometric type		Client Group
		Face	Finger print	
111	Collection of biometric information.	X	X	Applicant for entry permission
149	Powers of refugee and protection officers (and their agents).	X	X	Asylum Claimants

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
H1	Claimants lack a real choice about providing biometric information.	The 2009 Act provides statutory authority for the collection of biometric information. This information is necessary to enable the Ministry to undertake its statutory responsibilities. It will be used to help establish and verify the identity of the claimant. Claimants will be informed about why the information is being collected and how it will be used. Claimants may refuse to provide biometric information but this may draw a negative inference. Should claimants refuse to provide, they would be informed that it may have a bearing on the determination as part of the process and may apply their appeal rights. All information will be kept and handled securely according to the Ministry's security procedures.
	Excessive collection was not identified as a specific risk as the proposed collection was limited and the rationale for the limitations described in full.	The 2009 Act does not set an age limit for the collection of biometric information. The appropriate age needs to be determined as a matter of operational policy. The Ministry considered a range of factors. Setting the age at 14 is consistent with practice in other comparable jurisdictions such as Australia, Canada, the United States, Germany, Switzerland, Sweden and the European Union Schengen Agreement. Discretion can be applied to not collect biometrics. Advice was also sought from the Police on how fingerprints develop as children grow and at what age fingerprints become useful for automatic comparisons. Additional safeguards will be applied when collecting fingerprints from minors. For example, their parent or guardian would have the opportunity to be present. In the case of unaccompanied minors onshore, the fingerprinting would be undertaken in the presence of the Police or a representative from Child, Youth and Family.
H4	People will not know what is happening with their information.	All applicants for entry into New Zealand receive information about what personal information will be collected and how it will be used. It is provided with entry and departure cards. It is available on the Ministry's website at www.immigration.govt.nz/migrant/stream/live/visa/ and in the Immigration New Zealand Operational Manual http://www.immigration.govt.nz/NR/rdonlyres/607ED409-0193-46A1-B3FF-

Risk	Initiative specific risk(s)	Mitigation(s)
		8496DCB2FAC7/0/Administration.pdf and in web pages that explain the Ministry's use of authorised information matching http://www.immigration.govt.nz/migrant/general/generalinformation/immigrationact/factsheets/biometrics.html A translated brochure is available for asylum claimants and their representatives explaining the collection and handling of biometric information.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their personal information.	The Protocol requires participating countries to abide by all legal requirements within their own countries, including those relating to privacy. All INZ clients can request a copy of their biometric information from INZ. This same right is mirrored across FCC partners.
H9	Adverse action being taken against a person without that person being given the opportunity to explain or challenge potentially prejudicial information.	All potentially prejudicial information will be presented to the person for their comment or rebuttal.
	A perception that biometrics is infallible and therefore the normal checks and balances within immigration processing do not apply.	To ensure accuracy any matched prints, which indicate an identity discrepancy, would be verified by a Police fingerprint expert. All potentially prejudicial information will be presented to the person for their comment or rebuttal.
H11	The information will be used for purposes unrelated to immigration process.	The fingerprints will be securely stored in an immigration fingerprint database until transitioned to IDme in 2016. Access will be restricted to approved staff. Face images are securely stored in AMS.
H14	Widespread use of common unique identifiers (UIs).	All people are assigned a unique identifier for all their dealings with the Ministry. That UI is not used by any other agency.
S3	The biometric information is compromised by a lack of security in storage or transmission.	All information will be kept and handled securely according to the Ministry's ICT security procedures.

Date finalised: 13 May 2016
Version number: V1.2

APPENDIX 9 – UNHCR REFUGEE PROGRAMME

Background
Fingerprint and face biometric collection will be used to assist in confirming the identity and background of persons seeking resettlement in New Zealand under the UNHCR Refugee Programme – "Quota Refugees" of whom NZ accepts around 750 per year.

Fingerprints collected will be searched and stored in the immigration fingerprint database and may also be searched via the Five Country Conference[91] (FCC) Protocol.

Face images (photographs) may be taken and manually compared for complex cases. This initiative applies to persons seeking resettlement in New Zealand under the UNHCR Refugee Programme.

The use of biometrics will:

- assist in identity establishment – biometric enabled identity management enables INZ to be sure that the person is not already known to immigration under another identity.
- ensure reliable identification of people in subsequent transactions with INZ and other agencies to whom INZ provide approved identity verification services– INZ is the authoritative source of identity information for foreign nationals, and
- enable approved international identity checks with partner countries (i.e. under the FCC Protocol).

The drivers for this initiative are:

- to identify and check the identity of persons offshore seeking resettlement in New Zealand under INZ's Refugee Quota Programme, who are often undocumented and difficult to identify,
- to identify and check persons who are suspected of breaching, or intending to breach the Immigration Act 2009,
- to identify high risk visa applicants and prevent those under assumed identities from being granted a visa; and
- to use biometrics in a privacy protective and accurate manner by running approved domestic and international checks with trusted partners via the FCC Protocol (for the above examples).

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

[91] The Five Country Conference ('FCC') is a forum for immigration and border security – involving Canada, Australia, the United Kingdom (U.K), the United States (U.S) and New Zealand.

Section	Section Description	Biometric type		Client Group
		Face	Fingerprints	
111	Applicant for entry permission to allow collection of biometric information.	X	X	Travellers formally interviewed at the border by INZ
149	Powers of refugee and protection.	X	X	Refugee and asylum claimants
305 & 306	Enables Ministry to exchange information, including biometric information.	X	X	All passengers and crew

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
H1	Applicants lack a real choice about providing biometric information.	The 2009 Act provides statutory authority for the collection of biometric information. This information is necessary to enable the Ministry to undertake its statutory responsibilities. It will be used to help establish and verify the identity of the client. Clients will be informed about why the information is being collected and how it will be used. All information will be kept and handled securely according to the Ministry's security procedures.
H1	Excessive collection is not identified as a specific risk as the proposed collection is limited and the rationale for the limitations described in full.	The Act does not set an age limit for the collection of biometric information. The appropriate age needs to be determined as a matter of operational policy. For the purpose of this project, persons aged 14 or over may be required to provide fingerprints.
H2	Staff make arbitrary 'requests' for biometric information	Formal risk profiling and business rules will determine which application types or clients would be required to provide biometrics. Collection will be mandatory in most enforcement or refugee scenarios, therefore mitigating the potential for 'arbitrary' requests.
H4	People will not know what is happening with their information.	Information about what personal information will be collected and how it will be used is provided with arrival and

Risk	Initiative specific risk(s)	Mitigation(s)
		departure cards. It is available on the Ministry's website at www.immigration.govt.nz/migrant/stream/live/visa/ and in the Immigration Policy Manual www.immigration.govt.nz/NR/rdonlyres/607ED409-0193-46A1-B3FF-8496DCB2FAC7/0/Administration.pdf and in web pages that explain the Ministry's use of authorised information matching. A translated leaflet will be available for clients and their representatives explaining the collection and handling of biometric information. A translated leaflet will be provided to clients explaining the collection and handling of biometric information during their offshore resettlement interview and clients are given an opportunity to ask questions through an interpreter. For any refugee quota cases not interviewed in person by RQB pre-arrival, this information is provided again on arrival.
H5	The manner in which biometric information collected is unfair or intrusive. Adverse action taken against a person without that person given the opportunity to explain or challenge potentially prejudicial information.	See explanation in H1 and H2. All potentially prejudicial information will be presented to the person for their comment or rebuttal, before an application or claim is decided.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their personal information.	In immigration matters, those people will be treated as if they have the same rights as citizens and residents. This meets the requirements under section 34 of the Privacy Act 1993 as amended on 8 September 2010.
H9	A perception that biometrics is infallible and therefore the normal checks and balances within immigration processing do not apply.	All potentially prejudicial information will be presented to the person for their comment or rebuttal, before an application is decided.
H11	The information will be used for purposes unrelated to an immigration determination.	The fingerprints will be securely stored in an immigration fingerprint database hosted within NZ Police's database until transitioned to IDme in 2016. Access will be restricted to approved staff. Face

Risk	Initiative specific risk(s)	Mitigation(s)
		images are securely stored in AMS.
S1-S3	The biometric information is compromised by a lack of security in storage or transmission.	All information will be kept and handled securely according to the Ministry's ICT security procedures. All biometric information collected via SRTP will be encrypted before transmission. Standard encryption procedures are applied otherwise.

Date finalised: 13 May 2016
Version number: v1.3

APPENDIX 10 – USE OF SPECIAL BIOMETRICS TO ENABLE DEPORTATION

Background
Biometric information or physical measurements may be required from a person due to be deported or turned around at the border in order to be able to remove them back to their country of origin.

The most common example of this is a deportee who does not have a valid travel document – a passport photo and/or other biometric must be taken to obtain a valid travel document.

One requirement for a travel document is a photo of the subject. Some countries also require a fingerprint or thumbprint, height or other physical measurement.

Some countries require a photograph of the person before they will authorise transit.

Lastly, some countries require biometric evidence before they will agree that the person is one of their citizens.

Section 287 of the Immigration Act 2009 ("The Act") allows this.

What biometrics are involved?
The most common biometric is a facial photo. In some circumstances fingerprints may also be required.

Biometric information as defined in Section 4 of the Act, may also include use of iris biometrics, however iris scans are not currently intended to be used by INZ.

Other biometrics may also be used if required in order to be able to meet entry or transit requirements of a third country through which someone is due to travel, notably: palm-print, foot-print or body measurements as permitted under Section 28 of the Immigration Act 2009.

Who will be subject to this?

The scope is persons who:

- Are being deported, or
- Are being turned around at the border, and

How will the biometrics be used?

The biometrics will assist in:

- Obtaining a travel document
- Proving identity
- Meeting transit and/or entry requirements

- Future immigration decisions.

Biometrics will be stored to establish a record identity (Section 30 of the Act).

If electronic fingerprints are required, they will be searched as part of the storage process to avoid duplication. The client will be advised of this if electronic fingerprints are required.

Palm-prints, footprints and body measurements, which are not covered under Section 4 of the Act, will be destroyed once used for the purpose for which they were obtained.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

Section	Section Description	Biometric type			Client Group
		Face	Fingerprints	Special*	
287	Special biometric information	X	X	X	Persons being deported or turned around at the border, where biometrics required by 3rd country.
288	Requirement to allow collection of biometric information and special biometric information	X	X	X	Any person liable for deportation or turnaround.
289	Application for order authorizing collection of biometric	X	X	X	Onshore Compliance Operations and Investigations clients whom attempt to subvert an investigation by refusing to provide biometrics when requested by INZ.
290	Judge may authorize biometric information and special biometric information to be collected.	X	X	X	As stated for section 289.

290A	Obtaining biometric information by compulsion	X	X	X	As stated for Section 289.
291	Further applications for compulsion order	X	X	X	As stated for Section 289.
305 & 306	Enables Ministry to exchange information, including biometric information	X	X	X	All passengers and crew

*Under Section 287 Special biometric information means, any of the following that are or may be required in order to meet the entry or transit requirements of any country to which or through which the person is to travel:

(a) the person's palm-prints:
(b) the person's footprints:
(c) measurements of the whole person:
(d) photographs of the whole person.

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
H1	Applicants lack a real choice about providing biometric information.	The 2009 Act provides statutory authority for the collection of biometric information. This information is necessary to enable the Ministry to undertake its statutory responsibilities. It will be used to inform the investigation process of persons who have breached their visa conditions or have obtained a visa under a false identity, or to facilitate the process for persons who are liable for deportation or turnaround or whose liability are suspected.' Clients will be informed about why the information is being collected and how it will be used. All information will be kept and handled securely according to the Department's security procedures.
H1	Biometric information is un-necessarily or excessively collected and retained, including multiple types of biometric information (multimodal) collected without adequate justification.	The scope for collection under this Section of the Act is extremely narrow and tightly defined. The Act does not set an age limit for the collection of biometric information. The appropriate age needs to be determined as a matter of operational policy. For the purpose of this project, persons aged 14 or over may be required to provide fingerprint biometric information. There is no lower age limit for facial photo collection or individual ink fingerprints in this situation as these are sometimes required for children's travel documents. Footprints and palm-prints, if required by the circumstance and taken using Section 287, will not

Risk	Initiative specific risk(s)	Mitigation(s)
		be stored and will be destroyed once used for the purpose for which they were obtained. Iris biometrics are currently unused by the Ministry, and it is unlikely that iris biometrics will be required under Section 288. Should the Ministry ever seek to deploy this technology the associated privacy risks will first be analysed separately in this Privacy Impact Assessment.
H2	Staff make arbitrary 'requests' for biometric information	Who this section relates to is tightly defined. Collection of biometric information can occur and be used to interview someone to inform a decision on whether deportation or refusal to enter is applicable. Collection may also occur once someone has been made subject to a deportation order, or has been refused entry, and biometrics or other measurements or scans are required in order to remove them to their country of origin.
H4	People will not know what is happening with their information.	Information about what personal information will be collected and how it will be used is provided with arrival and departure cards. It is available on the Ministry's website at www.immigration.govt.nz/migrant/stream/live/visa/ and in the Immigration New Zealand Operational Manual www.immigration.govt.nz/NR/rdonlyres/607ED409-0193-46A1-B3FF-8496DCB2FAC7/0/Administration.pdf and in web pages that explain the Ministry's use of authorised information matching. A translated leaflet will be available for clients and their representatives explaining the collection and handling of biometric information.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their personal information.	In immigration matters, those people will be treated as if they have the same rights as citizens and residents. This meets the requirements under section 34 of the Privacy Act 1993 as amended on 8 September 2010.
H11	The information will be used for purposes unrelated to an immigration determination.	Any information collected will be securely stored. Access will be restricted to approved staff, and in the case of fingerprints will be kept securely in the IDme. The special biometric information will be used only to enable a deportation or turnaround subject to be successfully deported, to establish a record of their identity and to assist in making immigration decisions in the future.
S1	The biometric information is compromised by a lack of security in storage or transmission.	All information will be kept and handled securely according to the Ministry's ICT security procedures. Fingerprint biometric information transmission will be solely via the secure INZ biometric file-share while face photos are handled within the AMS system. Fingerprints will remain in the NZ Police database until transitioned to IDme in 2016.

Risk	Initiative specific risk(s)	Mitigation(s)
S2	Disclosure of biometric information without reasonable grounds	Disclosure of Foreign Criminal Removals is shared with the UK and there are plans to expand this. Further details on this are covered elsewhere in this Privacy Impact Assessment.

Date finalised: 13 May 2016
Version number: v1.2

APPENDIX 11 – INVESTIGATIONS

Background

Fingerprint and face biometric collection will be used to assist in confirming the identity and background of persons under investigation for potential offences against the Immigration Act 2009.

Fingerprints collected will be searched and stored in the immigration fingerprint database and may also be searched via the Five Country Conference[92] (FCC) Protocol.

Face images (photographs) may be taken and manually compared. With the implementation of the automated identity matching engine, IDme, the manual comparison will be supported by IDme matching technology.

This initiative applies to the following case types:

- Border investigations of passengers of interest,
- Compliance and fraud investigations,
- Persons applying for a visa whom it is suspected may be using a false identity, and
- Persons applying for a visa whom represent high risk to INZ or New Zealand (this is determined via existing client risk profiling processes).

The use of biometrics will:

- assist in identity establishment – biometric enabled identity management enables INZ to be sure that the person is not already known to immigration under another identity,
- ensure reliable identification of people in subsequent transactions with INZ and other agencies to whom INZ provide approved identity verification services– INZ is the authoritative source of identity information for non-New Zealand citizens, and
- enable approved international identity checks with partner countries (i.e. under the FCC Protocol).

The drivers for this initiative are:

- to identify and check persons under investigation at the border,
- to record the identity of persons subject to deportation, and in the long term to prevent those persons re-entering New Zealand under another identity,
- to facilitate the identification and deportation of those who use false identities in order to try to prevent their deportation,

[92] The Five Country Conference ('FCC') is a forum for immigration and border security – involving Canada, Australia, the United Kingdom (U.K), the United States (U.S) and New Zealand.

- to identify and check persons who are suspected of breaching, or intending to breach the Immigration Act 2009,
- to identify and check high risk visa applicants and prevent those under assumed identities from being granted a visa, and
- to use biometrics in a privacy protective and accurate manner by running approved domestic and international checks with trusted partners via the FCC Protocol (for the above examples).

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being enacted by this initiative.

Section	Section Description	Biometric type		Client Group
		Face	Fingerprints	
60	Biometric information may be required from visa applicant.	X	X	Visa applicants
100	Collection of biometric information from proposed arrivals	X	X	All non-NZ travellers
104	New Zealand citizens photographed on arrival.	X		All New Zealand citizens
111	Applicant for entry permission to allow collection of biometric information.	X	X	Travellers formally interviewed at the border by INZ.
120	Foreign nationals leaving New Zealand to allow biometrics to be collected.	X	X	Persons being deported from New Zealand.
288	Immigration officer may require biometric information to determine compliance with the 2009 Act.	X	X	Persons suspected of breaching, or intending to breach, the Immigration Act 2009.

289	Application for order authorizing collection of biometric information.	X	X	Onshore Compliance Operations and Fraud clients who attempt to subvert an investigation by refusing to provide biometrics when requested by INZ.
290	Judge may authorise biometric information to be collected.	X	X	As stated for section 289.
291	Further applications for compulsion order	X	X	As stated for section 289.
305 & 306	Enables the Ministry to exchange information, including biometric information	X	X	All passengers and crew

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
H1	Applicants lack a real choice about providing biometric information.	The 2009 Act provides statutory authority for the collection of biometric information. This information is necessary to enable the Ministry to undertake its statutory responsibilities. It will be used to help establish and verify the identity of the client. Clients will be informed about why the information is being collected and how it will be used. All information will be kept and handled securely according to the Ministry's security procedures.
H1	Excessive collection is not identified as a specific risk as the proposed collection is limited and the rationale for the limitations described in full.	The Act does not set an age limit for the collection of biometric information. The appropriate age needs to be determined as a matter of operational policy. For the purpose of this project, persons aged 14 or over may be required to provide biometric information.
H2	Staff make arbitrary 'requests' for biometric information	Formal risk profiling and business rules will determine which application types or clients would be required to provide biometrics. Collection will be mandatory in most enforcement or refugee scenarios,

Risk	Initiative specific risk(s)	Mitigation(s)
		therefore mitigating the potential for 'arbitrary' requests. Clients can refuse to provide biometric information but this may have a negative effect on their application or claim.
H4	People will not know what is happening with their information.	Information about what personal information will be collected and how it will be used is provided with arrival and departure cards. It is available on the Ministry's website at www.immigration.govt.nz/migrant/stream/live/visa/ and in the Immigration Policy Manual www.immigration.govt.nz/NR/rdonlyres/607ED409-0193-46A1-B3FF-8496DCB2FAC7/0/Administration.pdf and in web pages that explain the Ministry's use of authorised information matching. A translated leaflet will be available for clients and their representatives explaining the collection and handling of biometric information.
H5	The manner in which biometric information collected is unfair or intrusive. Adverse action taken against a person without that person given the opportunity to explain or challenge potentially prejudicial information.	See explanation in H1 and H2. All potentially prejudicial information will be presented to the person for their comment or rebuttal, before an application or claim is decided.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their personal information.	In immigration matters, those people will be treated as if they have the same rights as citizens and residents. This meets the requirements under section 34 of the Privacy Act 1993 as amended on 8 September 2010.
H9	A perception that biometrics is infallible and therefore the normal checks and balances within immigration processing do not apply.	All potentially prejudicial information will be presented to the person for their comment or rebuttal, before an application is decided.
H11	The information will be used for purposes unrelated to an immigration determination.	The information will be securely stored in IDme. Access will be restricted to approved staff.

Risk	Initiative specific risk(s)	Mitigation(s)
S1-S3	The biometric information is compromised by a lack of security in storage or transmission.	All information will be kept and handled securely according to the Ministry's ICT security procedures. All biometric information collected will be encrypted before transmission.

Date finalised: 13 May 2016
Version number: v1.2

APPENDIX 12 – DATA MATCHING CAPABILITY

Background

The Ministry's Vision 2015 Programme established the capability for routine collection, storage and matching of multi-modal biometrics for identity verification, to manage risk for immigration into New Zealand. Multi-modal biometrics refers to the use of more than one type of biometric identifier to enhance the confidence in matching identities. For the Ministry this will primarily mean using both face and fingerprint biometrics.

The Ministry is introducing new initiatives which further integrate the use of biometric information into the immigration environment. INZ is transitioning away from managing and matching biometric information manually, however this will be a gradual transition, and will always require human intervention for the matches that are complex and cannot be automated to complete successfully.

What are the benefits of IDme for the Ministry?

This appendix deals specifically with the initiative to implement an Identity Matching Engine - IDme - in 2016. IDme will provide the capability to match core biographic information with biometric information and automated matching of face images. It will enable faster processing of new and existing information. It will provide the capability to combine and match identity information, including biographic information from passport smart scanners to biometric information such as facial images and fingerprints. Additionally, IDme will enable INZ to conduct ad-hoc searches for specific instances. Ultimately, the use of IDme will provide the Ministry with increased assurance of individuals' identity in a timely manner.

How will IDme work?

Existing biometric and biographic information will be copied into the IDme database from AMS and Immigration ONLINE. The new system does not expand on the biometric information already being collected. INZ will capture the biometric and biographic identity information using IDme and facial images and biographic information through AMS and Immigration ONLINE.

Biographic and biometric information is collected in the following circumstances and matched within IDme:

1) Individuals arriving in the country at the border. Those who fail to proceed through the standard processing at the border are referred to INZ and their biometrics, including fingerprints, are captured.
2) Individuals claiming refugee or protection status onshore in New Zealand or candidates for refugee status under the quota for UNHCR. Biometrics will be collected through Daon Enrol.
3) For situations where individuals are removed from NZ, biometrics are collected to detect if the individual tries to re-enter the country.

Biographic and biometric information captured in IDme will be used to match the associated biographic and biometric information against all existing INZ identities. An identity match will be established by automated processing, either to existing

information previously captured. If there is no match to existing information, then a new identity will be created.

Where matches reach a high threshold of identity assurance these are automatically resolved. Where there are inconsistencies in a match result, for example, matches with more than one existing INZ client, or that indicate possible identity fraud, these will be referred for manual identity resolution.

Manually resolved identity exceptions that involve face biometrics are resolved via a typical face-image matching process. This process is conducted by a newly created specialist identity role. Individuals in this role will be appropriately skilled and trained to resolve facial biometrics and will concentrate on complex exceptions only.

If an identity is referred for manual resolution, a warning indicating this pending action is attached to the corresponding client record in AMS. The warning is removed once the manual identity resolution activities are completed. When capture, match and management of the identity information is completed, the results are updated in AMS so they can be accessed by Ministry staff in Border Operations, Compliance, Identity Services, Refugee Services and Visa Services.

The implementation of IDme will occur in two releases. Release 1.0 is anticipated for May 2016 and is reliant on significant manual intervention to test that the system and supporting processes are making matches correctly. This will be for a period of less than a year. Increased automated processing functionality will be included in Release 1.1 by December 2016 when INZ is satisfied that IDme is competently conducting the matches.

Who will use IDme and access biometric information?

Ministry staff with access to IDme will have appropriate access role profiles and there will be appropriate security controls in place to identify who accessed information, what information was accessed and when. The system allows for correction of any mismatches if they occur.

NZ Police will have limited and restricted access in the capacity of providing ongoing fingerprint expertise. This sharing of data with NZ Police is appropriately governed by the MoU between the Ministry and NZ Police.

A function of IDme is the ability to conduct an ad hoc search based on biometrics. Risk Managers, Verification Officers and other approved roles can perform biometric searches to qualify risk. This will enable staff to verify higher risk identities. Only a subset of staff will be trained to perform Biometric searches within the permitted roles.

Due to the time pressure of border facilitation, use of IDme will enhance the turnaround time to more quickly and efficiently match the results of identity information captured.

What is the impact of IDme?

The implementation of IDme will not impact the scope of identity information collected or used. There will be an increase in the volumes of identity matches performed, consequently an increase in confidence making identity decisions and assurances that potential immigration or identity fraud are being detected earlier and more often.

New business processes and roles have been defined within the Ministry to take account of the operational changes. Staff will be trained in new processes and skills.

The impact upon the privacy of individual clients is potentially enhanced through using face images when performing searches based on all holdings. The additional information used in the search provides increased assurances of correct matching to of identities.

What parts of the Immigration Act 2009 are being enabled?

The table below provides a summary of the sections identified as being affected by this initiative.

Sections 100 and 104 of the 2009 Act, although provided for and mandated, are not fully activated yet. The provisions are in place and biometric information is collected on an ad hoc and case by case basis by requesting a photo of an individual. When these provisions are to be applied systematically, this document will be updated.

Section	Section Description	Client Group affected		
		Face	Finger-print	
60	Biometric information may be required from visa applicant.	X	X	All visa applicants
99	NZ citizen may confirm citizenship before arrival in NZ	X	X	All NZ citizens on arrival
100	Collection of biometric information from proposed arrivals.	X	X	All non NZ travelers
104	New Zealand citizens photographed on arrival.	X	X	All NZ citizens
111	Collection of biometric information.	X	X	Applicant for entry permission
120	All non-New Zealand citizens leaving New Zealand to allow biometric information to be collected.	X	X	All non NZ travelers
149	Powers of refugee and protection officers (and their agents).	X	X	Refugee and Asylum claimants
288	Requirement to allow collection of biometric information	X	X	All non NZ nationals

289 to 291	An immigration officer may apply to a court for an order compelling the collection of biometrics if necessary (sections 289 to 291).	X	X	Persons liable for deportation or turnaround
305 & 306	Enables Ministry to exchange information, including biometric information	X	X	All passengers and crew

Privacy risk assessment

The table below provides a summary of the key privacy risks identified and the mitigation strategies in place to respond to these risks.

Risk	Initiative specific risk(s)	Mitigation(s)
G3	Unnecessary expense incurred because systems are not designed from the beginning to include privacy considerations.	Incorporate 'privacy by design' into the IDme solution, including: reporting for information access requests; testing environments and in particular user acceptance testing; back up and disaster recovery environments; and training. Ensure a PIA is undertaken (consistent with legislative obligations) for this project prior to their design/build phase and add as an appendix to this PIA.
G4	Authorisation to access biometric information too widely approved.	Maintain adequate controls around granting authorisation to access biometric information. Design audit processes into all systems used to store or process biometric information to control user accounts, access rights and security authorisations. Base access rights to biometric information on the need to know (essential business justification). Roles for access have been defined and restricted within Ministry and NZ Police.
G5	Inadequately managed collaboration and information sharing with other agencies putting biometric information at risk	Individual PIA conducted with each overseas FCC partner for information sharing. Measures taken to ensure that information sharing agreements do not compromise the Ministry's ability to meet its statutory obligations. MOU agreement between NZ Police and the Ministry which covers the only external use of IDme by NZ Police.

Risk	Initiative specific risk(s)	Mitigation(s)
		Measures are in place to prevent unauthorised use or disclosure of biometric information.
G6	Inadequately managed outsourcing does not adequately protect biometric information	Fingerprints collected and stored by NZ Police staff acting on behalf of the Ministry for immigration purposes will be transitioned to the Ministry. Fingerprints will be managed and stored by IDme database in INZ system. Future agreements with outsourcing providers will cover biometrics collected and delivered to INZ. All outsourcing providers will be required to delete any biometrics collected upon the successful secure transfer of data to INZ. Measures will be included to prevent unauthorised use or disclosure of biometric information.
H1	Biometric information unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification	Ensure that all implementations of the biometric provisions in the Immigration Act 2009 are in line with the statutory authority. Limit collection of biometric information to what is needed (essential business justification) to support current decisions. Fingerprints of high risk clients are collected to verify identity and identify potential immigration and identity fraud. Increased volumes of fingerprint and facial biometric checking will be enabled and search capability provided. This will be managed through business rules, operational policy and specifically high matching thresholds. Inconsistent matches are manually resolved. The use of automated matching to determine matches is considered privacy protective. Alternative processes would be more vulnerable to subjective assessments of interest rather than an objective and consistent measurement of the similarity of two examples of a physical biometric characteristic.

Risk	Initiative specific risk(s)	Mitigation(s)
H2	Staff make arbitrary 'requests' for biometric information	Maintain guidelines in operational policy, business processes and staff training / awareness for requiring biometrics from specific people. Business rules and operational policy will determine ad hoc search criteria. Ad hoc requests will be made by access controlled role profiles and access will be logged for audit trail. Staff will follow operational policy and business rules when requesting ad hoc searches. Train staff in the application of the Ministry's Code of Conduct and the exercise of it in situations where professional judgment is required.
H3	Biometric information not collected directly from the person concerned	Maintain privacy protective processes for handling biometric information collected from third parties (for example, through information sharing and / or other service level agreements / contracts). Some fingerprint information collected by INZ for use is done so directly from the person concerned. INZ is authorised under the Immigration Act 2009 to exchange information with equivalent authorities in other countries for immigration purposes by virtue of s.305 and 306 in the Immigration Act 2009.
H4	People not adequately informed about the purposes of collection of biometric information	Ensure that people are appropriately notified in a relevant manner whenever biometric information is collected from them. The INZ website contains detailed information about biometric collection and data sharing with FCC partners. A multilingual leaflet is currently given to all subjects fingerprinted by INZ explaining why we are collecting their fingerprints and how their biometrics will be handled. It should accurately reflect the applicable age for the collection of biometric information, how NZ citizen's biometric images are being

Risk	Initiative specific risk(s)	Mitigation(s)
		retained. Build an acknowledgement of biometric collection in the biometric enrolment and verification processes. For investigation cases, individuals are informed before collection, not after the event. Communications will be reviewed for future changes.
H5	The manner in which biometric information collected is unfair or intrusive.	Include appropriate responses in operational policy, business processes and staff training/awareness to cultural and physical considerations when collecting biometric information.
H6	The right of people outside the country who are not New Zealand citizens or residents to access and request correction of their biometric information	For sharing of matching capability with FCC partners, the Protocol requires participating countries to abide by all legal requirements within their own countries, including those relating to privacy. All INZ clients can request a copy of their biometric information from INZ. This same right is mirrored across FCC partners. The IDme system has been built with privacy in mind and enables look up and extract functionality for information requests from individuals – this is conducted by Privacy Officers and Identity Services.
H7	The Ministry is unable to respond effectively to requests for personal information or to investigations by the Privacy Commissioner (and others) because of inadequate system design	Maintain oversight and review mechanisms. Design biometric systems with the ability to respond to review agencies requests and the Privacy Commissioners investigations. IDme provides functionality for Identity Services Analysts and Privacy Officers to look up requests directly in IDme to facilitate client requests.
H8	Biometric information incorrectly associated with a	Maintain processes / check to ensure that biometric information is not associated with

Risk	Initiative specific risk(s)	Mitigation(s)
	person	a person record by mistake. Identity Resolver and Face Analyst roles will receive training on facial resolution skills. New specialist forensic tools and supporting training for resolving complex fingerprint biometric exceptions will be available for specialist Fingerprint Analysts.
H9	Inaccurate or incorrect biometric data is used to make a decision about a person	Develop processes for handling false negatives and false positives when matching biometrics. IDme levels of accuracy in fingerprint matching are extremely accurate. Include biometric information in the processes for permitting comment on and rebuttal of potentially prejudicial information. All applicants are informed of information that might harm their case (often referred to as "potentially prejudicial information" or PPI) and given a reasonable opportunity to respond to harmful information.
H10	Biometric information retained longer than necessary	Apply to the Chief Archivist, Archives New Zealand, for a formal disposal authority.
H11	Biometric information used for non-immigration purposes	The Protocol has assigned 'Search Codes' which dictate what may be searched and what may not. This also controls what information is released if a match occurs. The information received for immigration purposes will be used exclusively for immigration and identity purposes.
H12	Disclosure of biometric information without reasonable grounds. Article I.	Maintain specific guidelines on the release and disclosure of biometric information in to operational policy, business processes and staff training. Ensure staff understanding of their responsibilities through training, awareness

Risk	Initiative specific risk(s)	Mitigation(s)
		and other support materials. Standard Operating Procedures have been drafted. Training will be in eModules or paper based and will not involve identifiable "real" biographic or biometric information.
H13	Unnecessary assignment of unique identifiers	Continue the current process of assigning unique identifiers to people that are not biometric templates. IDme will issue a unique ID for internal use only.
S1	Loss of biometric information	Ensure an adequate security environment for biometric information. Appropriate security plans are in place for technical environments, including: production, development, back up, test and training environments. Test information will be secured appropriate and deleted on completion. Compliance with several Government Security Standards is required, in addition to achievement of MBIE Security Accreditation. Apply appropriate encryption of biometric information when it is transferred between agencies where agreements are in place. Maintain contingency plans to address any security breaches. Comply with the Privacy Commissioner's Privacy Breach Guidelines and the Ministry's Privacy Event process.
S2	Unauthorised access to biometric information	Compliance with several Government Security Standards is required, in addition to achievement of MBIE Security Accreditation. When external third parties are involved in the technical development, build, testing and implementation of the enabling technology for IDme, the Government standards for IT and Security are adhered

Risk	Initiative specific risk(s)	Mitigation(s)
		to. Assurances have been obtained from the IDme team within the Ministry that the appropriate technical and security standards required to address the privacy risks of third party involvement have been adhered to. This refers also to the procurement and contractual risks identified in G3. Should third party involvement extend to the capture of biometric and biographic information, this appendix should be updated to address that situation, for example, Biometric Enrolment Centres or IDme Enrolment Stations. IDme has undertaken a rigorous security risk assessment process and will be required to pass a formal security accreditation process to ensure that appropriate physical and technical security standards are in place. This will provide assurance that the required protection to fingerprints is in place after the holdings have been migrated from NZ Police to IDMe. INZ is required under the Protocol and the MOU to take care to protect the information against loss, misuse, and unauthorised disclosure. Information will be encrypted by an internationally accepted protocol and appropriate handling instructions are applied. All fingerprint information will be securely deleted from the secure file server once the match cycle has ended. Only specified employees of INZ will be permitted access to the information and all access will be logged and audited.

Date finalised: 13 May 2016
Version number: V1.1