



Privacy Impact Assessment

Collection and Handling of Biometrics at Department of Labour



Author

Department of Labour

Acknowledgement

The Department of Labour acknowledges the internal business units and external agencies interviewed who provided information about their collection and handling of biometric information.

Auckland Regional Manager
Border and Investigations
Compliance Operations
Data Warehouse
Fraud Branch
Intelligence
Internal Audit
IT Security
London Branch
Office of the Privacy Commissioner
Pacific and Auckland Branches
Project and Integration Support
Records and Documents
Refugee Quota Branch
Refugee Status Branch
Resolutions, Government Relations Unit
Settlement, Protection and Attraction Unit
Strategic Programmes, Service Support
Visa Services and Operational Support
Wellington Branch
Department of Internal Affairs
New Zealand Customs Service
New Zealand Food Safety Authority
New Zealand Police
New Zealand Trade and Enterprise
Ministry of Agriculture and Forestry
Ministry of Foreign Affairs and Trade
Ministry of Justice

Disclaimers

The Department of Labour has made every effort to ensure that the information contained in this report is reliable, 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 Department accepts no liability for any decisions made in reliance on them. The Department may change, add to, delete from or otherwise amend the contents of this report at any time without notice.

The material contained in this report is subject to Crown copyright protection unless otherwise indicated. The Crown copyright protected material may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material being reproduced accurately and not being used in a derogatory manner or in a misleading context. Where the material is being published or issued to others, the source and copyright status should be acknowledged. The permission to reproduce Crown copyright protected material does not extend to any material in this report that is identified as being the copyright of a third party. Authorisation to reproduce such material should be obtained from the copyright holders.

ISBN 978-0-478-36056-1

September 2011

© **Crown copyright 2011**

Department of Labour
PO Box 3705
Wellington
New Zealand
www.dol.govt.nz

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES	6
STRUCTURE OF THE PRIVACY IMPACT ASSESSMENT	7
EXECUTIVE SUMMARY AND SUMMARY OF RISKS AND MITIGATIONS	10
1. BACKGROUND, INTRODUCTION AND OVERVIEW	17
1.1 Biometric provisions in the Immigration Act 2009	17
1.2 Privacy governance within the Department	18
2. IDENTIFICATION OF THE NATURE AND SCALE OF THE PROBLEM	20
2.1 Effective and efficient immigration system	20
2.2 Identity fraud	21
2.2.1 Cost	21
2.2.2 Extent.....	21
3. ASSESSMENT OF EXISTING IDENTITY OPTIONS	23
3.1 Using biographic information only	23
3.2 Interviews	23
3.3 Document analysis.....	24
4. SCOPE OF THE PRIVACY IMPACT ASSESSMENT.....	25
5. PROCESS AND INFORMATION FLOWS.....	26
5.1 Information collection.....	26
5.2 Results.....	27
5.2 Information flows	28
6. ANALYSIS OF GUIDING PRINCIPLES	36
6.1 Justification for the use of biometric technologies for identity related purposes.....	36
6.2 The use of biometric technologies for identity related processes must be lawful and appropriately authorised	37
6.3 Collaboration with other agencies	41
6.4 Consideration of end users.....	42
6.5 Appropriateness of the biometrics used	43
6.6 Relevant international obligations	46
6.7 Stewardship – systems and processes.....	46
7. ANALYSIS OF IMPLEMENTATION PRINCIPLES	47
7.1 Information to end users and consultation with end users and stakeholders	47
7.2 Establishment of processes and procedures	48
7.3 Management of the life cycle of biometric information	48
7.4 Establishment of procurement processes	48
7.5 Standards for interoperability	49
7.6 Legal information sharing and matching	49
8. RISK ASSESSMENT – ANALYSIS OF IMPACTS	50
8.1 Governance risks	50
8.2 Handling practices risks.....	56
8.3 Security risks	60

9. PRIVACY ENHANCING RESPONSES	62
9.1 Privacy by design.....	62
9.2 Privacy-enhancing technologies	62
9.3 Security responses and other privacy protective tools	63
10. ON GOING EVALUATION, REVIEW AND MONITORING	66
11. CONCLUSION	67
APPENDIX 1 – ABBREVIATIONS USED.....	68
APPENDIX 2 – PRIVACY RISK MITIGATIONS ALREADY IN PLACE	69
APPENDIX 3 –MATRIX OF INITIATIVES BY SECTION	73
APPENDIX 4 – FACE BIOMETRICS	74
APPENDIX 5 – FCC PROTOCOL STAGE 2.....	79
APPENDIX 6 – FCC PROTOCOL STAGE 3.....	82
APPENDIX 7 – FCC FOREIGN CRIMINAL ALERTS	86
APPENDIX 8 – REFUGEE STATUS BRANCH	91
APPENDIX 9 – INVESTIGATIONS AND QUOTA REFUGEES.....	94

LIST OF TABLES AND FIGURES

Table 1:	Summary of privacy risks and mitigations	11
Table 2:	Privacy risks and mitigations.....	13
Table 3:	Business units interviewed.....	27
Table 4:	Agencies interviewed	28
Figure 1:	Existing biometric information flows.....	29
Figure 2:	Future biometric information flows.....	33

STRUCTURE OF THE PRIVACY IMPACT ASSESSMENT

The Department of Labour's (the Department'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 Department has completed a privacy impact assessment (PIA).

The Department consulted the Office of the Privacy Commissioner (OPC) on the terms of reference (TOR) for this PIA. Through ongoing consultation, the PIA report structure was agreed to.

The topics and issues for analysis in this PIA were sourced from the *Privacy Impact Assessment Handbook*,¹ *Guiding Principles for the Use of Biometric Technologies for Government Agencies*,² *Good Practice Privacy Guidelines for the use of Biometric Technologies*,³ *Trusted Computing and Digital Rights Management Principles and Policies*⁴ and *Trusted Computing and Digital Rights Management Standards and Guidelines*.⁵

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

As the Department advances its biometrics programme, various initiatives will require activation of legislative provisions. The appendices document those initiatives, their 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 this PIA to act as a reference tool, ensuring each initiative is assessed separately to address specific biometric information processing functions.

¹ *Privacy Impact Assessment Handbook*. Wellington: Office of the Privacy Commissioner, 2007. ISBN 0-478-11703-5.

² *Guiding Principles for the Use of Biometric Technologies for Government Agencies*. Wellington: Department of Internal Affairs, April 2009. ISBN 978-0-478-29487-3.

³ *Good Practice Privacy Guidelines for the use of Biometric Technologies*. Wellington: Department of Internal Affairs, September 2008.

⁴ *Trusted Computing and Digital Rights Management Principles and Policies*. Wellington: State Services Commission, September 2006. ISBN 978-0-478-30301-8.

⁵ *Trusted Computing and Digital Rights Management Standards and Guidelines*. Wellington: State Services Commission, July 2007. ISBN 978-0-478-30315-5.

Executive summary and summary of risks and mitigations

This provides a summary of the PIA and describes future implementation of the biometric provisions of the 2009 Act.

Table 1 (a summary of privacy risks and mitigations) lists relevant sections from the 2009 Act, the actions the Department proposes to take under those provisions and the main privacy risks identified as specific to each provision.

Table 2 (privacy risks and mitigations) lists all the biometric-specific privacy risks identified and possible ways to mitigate those risks. The risks are broken down into three groups: governance risks, handling risks and security risks.

Chapters 1–3

These chapters cover the background, context and issues for identity information management faced by the Department, how biometrics are proposed to be used and an examination of the options available.

Chapter 4

This is a short description outlining what the PIA covers and what it does not cover.

Chapter 5

This covers the research process for the PIA and its results. It describes how the information was collected, the interview process and people interviewed and a summary of the results of the interviews. It includes diagrams that show the known and expected future biometric information flows within the Department and explanatory text for those diagrams.

Chapters 6 and 7

These examine the Department's 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.

Note: This section does not address all risks to personal information. Some risks are already addressed by the Department's operational policies and procedures, and these may only require minor updating. These risks are identified with their existing policies and procedures in an appendix at the end of the document.

Chapters 9 and 10

Chapter 9 addresses general approaches to enhanced privacy responses by using tools such as privacy by design and privacy-enhancing technologies. Chapter 10 discusses the need for on going routine monitoring and review.

Chapter 11

This chapter highlights 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 being implemented by the Department.

These are followed by appendices covering specific powers and uses of biometrics, which will be maintained, as required, under section 32, subsection 3, of the 2009 Act.

EXECUTIVE SUMMARY AND SUMMARY OF RISKS AND MITIGATIONS

The Department is required to establish confidence in and verify the identity of people wishing to travel to, enter or stay in New Zealand. The Department's challenge is to accomplish that while improving the effectiveness and efficiency of its processes. Biometrics are a critical enabler for the Department 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 2009 Act contained provisions that permit the Department to collect biometric information on a mandatory basis. It requires the Department to conduct and maintain a PIA prior to implementing biometric provisions.

Interviews were conducted with internal staff and external stakeholder agencies. Existing and proposed biometric information flows were analysed and documented. Privacy risks and their possible mitigations were identified and documented.

Alternatives to biometrics considered in the PIA include collection of more biographic information, increasing the use of interviews of 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.

Table 1 below represents the end state model for the collection and handling of biometric information by the Department, which will be implemented in phases. Basing this PIA on the end state allows the privacy impacts and mitigations to be identified holistically at the outset and prior to any implementation. This will enable the Department to design its policies, procedures and products to take account of this PIA.

This PIA does not address the disclosure of biometric information under the relevant provisions in Part 8 of the 2009 Act as the Department 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.

Note: Risks in the Table 1 are referred to by a code (G1, H1, S1) where the letter indicates whether the risk is a governance, handling or security risk. The number is for the specific risk within each group. They are also given short names to help convey the basic nature of the risk. Table 2 lists all the risks in more detail and their possible mitigations.

Table 1: Summary of privacy risks and mitigations

Section of Act and proposed action	Main identified risks
60 Biometric information may be required from visa applicant. <ul style="list-style-type: none"> • Require all foreign nationals⁶ 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. 	G6 – use of agents H1 – unnecessary collection H4 – informed collection H5 – manner of collection G6 – use of agents H1 – unnecessary collection H2 – arbitrary requests H4 – informed collection H5 – manner of collection
96 Responsibilities of carriers departing from another country to travel to New Zealand. <ul style="list-style-type: none"> • (Advance Passenger Processing) Airlines to collect an in person photograph and/or fingerprints from all foreign nationals checking in to board a flight to New Zealand. 	G6 – use of agents H1 – unnecessary collection H4 – informed collection H5 – manner of collection
100 Collection of biometric information from proposed arrivals. <ul style="list-style-type: none"> • All foreign nationals to be required to provide an in person photograph and/or fingerprints where requested. 	G6 – use of agents H1 – unnecessary collection H2 – arbitrary requests H4 – informed collection H5 – manner of collection
104 New Zealand citizens photographed on arrival. <ul style="list-style-type: none"> • All New Zealand citizens to be required to provide an in person photograph. 	G6 – use of agents H1 – unnecessary collection H4 – informed collection H5 – manner of collection
111 Applicant for entry permission to allow collection of biometric information. <ul style="list-style-type: none"> • 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. 	G6 – use of agents H1 – unnecessary collection H4 – informed collection H5 – manner of collection
120 Foreign nationals leaving New Zealand to allow biometrics to be collected. <ul style="list-style-type: none"> • 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. 	G6 – use of agents H1 – unnecessary collection H4 – informed collection H5 – manner of collection

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.

Section of Act and proposed action	Main identified risks
<p>149 Powers of refugee and protection officers (and their agents).</p> <ul style="list-style-type: none"> • 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. 	<p>G6 – use of agents H1 – unnecessary collection H4 – informed collection H5 – manner of collection G6 – use of agents H1 – unnecessary collection H2 – arbitrary collection H4 – informed collection H5 – manner of collection</p>
<p>288 Immigration officer may require biometric information to determine compliance with the 2009 Act.</p> <p>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:</p> <ol style="list-style-type: none"> 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. 	<p>H1 – unnecessary collection H2 – manner of collection H4 – arbitrary collection H5 – informed collection</p>
<p>289 An immigration officer may apply to a court for an order compelling the collection of biometrics if 291 necessary (sections 289 to 291).</p> <p>Section 291 also provides further ability to apply for a compulsion order.</p>	<p>G6 – use of agents H1 – unnecessary collection H2 – arbitrary collection H4 – informed collection H5 – manner of collection</p>

Table 2: Privacy risks and mitigations

Governance risks	Mitigations
G1 No formal/centralised oversight of personal information management or privacy risk.	<ul style="list-style-type: none"> • 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 Departmental '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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Incorporate 'privacy by design' for all new biometric/personal information management systems in the Department. • 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 are able to 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. (Note: this is also a security risk.)	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Include privacy considerations in collaborative undertakings with other agencies. • Ensure that information sharing agreements do not compromise the Department'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 Department.)	<ul style="list-style-type: none"> • 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 Department'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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 make arbitrary 'requests' for biometric information.	<ul style="list-style-type: none"> • Maintain guidelines in operational policy, business processes and staff training/awareness for requiring biometrics from specific people. • Train staff in the application of the Department'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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Continue the Department's <i>Privacy Act Policy 2005</i>, which says that, 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	Due to inadequate system design, inability to respond to: <ul style="list-style-type: none"> • requests for access to information, or • requests for correction of information, or • Privacy Commissioner's investigations. 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.
H11	Biometric information used for non-immigration purposes.	<ul style="list-style-type: none"> • Ensure staff training/awareness in permissible uses of the information. • Build auditing and security capability into any future ICT system. • Review the Department's Code of Conduct to include specific guidance on the handling of biometric information.
H12	Disclosure of biometric information without reasonable grounds.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Continue the current process of assigning unique identifiers to people that are not biometric templates.
H14	Widespread use of biometric templates as unique identifiers.	<ul style="list-style-type: none"> • Do not share biometric templates with other agencies as unique identifiers.

Security risks	Mitigations
S1 Loss of biometric information.	<ul style="list-style-type: none"> • 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.⁷
S2 Unauthorised access to, use, disclosure and modification of biometric information.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.

⁷ <http://www.privacy.org.nz/privacy-breach-guidelines-2/?highlight=data%20breach%20notification>

1. BACKGROUND, INTRODUCTION AND OVERVIEW

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.

The 2007 Office of the Auditor-General's identity audit⁸ highlighted areas for improvement in immigration identity information management. Particular focus was on significant weaknesses with the Department's lack of ability to use biometrics. That report challenged the Department to devise a way to permanently associate a person with an identity that can be consistently used across immigration transactions.

Biometrics is key 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. Biometrics may be defined as "*the science of measuring an individual's physical or behavioural characteristics*"⁹

Biometric information is defined in section 4 of the 2009 Act 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. Department to undertake privacy impact assessment

(1) The Department must complete a privacy impact assessment in respect of the collection and handling of biometric information under this Act to–

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

⁸ 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>

⁹ Guiding Principles for the use of Biometric Technologies for Government Agencies, Cross Government Biometrics Working Group, Wellington, 2009

- (b) examine how any detrimental effects on privacy might be lessened.
- (2) The Department must consult the Privacy Commissioner—
 - (a) on the terms of reference developed for the assessment; and
 - (b) when completing the assessment.
- (3) The Department 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 Department must ensure the current privacy impact assessment is—
 - (a) available on the Department’s Internet site; and
 - (b) available or readily obtainable for inspection, free of charge, at—
 - (i) offices of the Department; and
 - (ii) New Zealand government offices overseas that deal 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.

Biometric provisions are contained within the 2009 Act, which mirror the immigration information life cycle. Specifically, these are referenced in the summary of risks and mitigations 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.¹⁰ The initiatives that will use these powers are documented in the appendices attached.

1.2 Privacy governance within the Department

The Department’s management of privacy issues is decentralised with responsibility devolved to each business unit which has ‘ownership’ of personal information. This is set out in a Legislative Compliance Handbook,¹¹ which states that all groups, particularly managers, are responsible for the oversight of privacy issues. Those privacy issues are said to carry a ‘medium risk’. The handbook is primarily targeted towards the management of information requests rather than personal information management practice.

¹⁰ 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>

¹¹ <http://intranet/strategies/internal-assurance/legislative-compliance/documents/legislative-compliance-handbook.doc>

The Department is required¹² to have (a) nominated privacy officer(s) whose responsibilities include the encouragement of, and ensuring compliance with, the Privacy Act 1993. Business units have people identified as privacy officers who are primarily involved in the management of privacy requests. The Deputy Chief Executive, Legal and International is the Chief Privacy Officer having oversight of all cross Departmental privacy issues.

Legal Services is responsible for the delivery of the Departmental 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.

The Department has a *Privacy Act Policy*¹³ dealing with the management of requests for information that fall under the Privacy Act 1993. The 72 page policy manual focuses on the process for information requests, providing explicit instructions and template letters.

Other aspects of privacy compliance appear in other policies dealing with security, retention of information and other subjects.¹⁴

The question of cross Departmental privacy governance is identified as a risk at G1.

¹² Section 23 Privacy Act 1993.

¹³ <http://intranet/support/commguides/pages/privacy-act-policy.aspx>

¹⁴ Most, if not all, of those policies can be found at:
<http://intranet/tools/searchcenter/Pages/results.aspx?k=information%20policy&s=All%20Sections>

2. IDENTIFICATION OF THE NATURE AND SCALE OF THE PROBLEM

The Department'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 Department to improve management of identity information and to use biometrics more effectively. The Department is also expected to respond to the drive to improve efficiency and effectiveness throughout the public service.

In the Department's 2010/2011 Statement of Intent,¹⁵ it 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 biometrics is a key facilitator for service improvement and future cost management by enabling increased automated processing of low risk immigration applications¹⁶ 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 Department's behalf.

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

- Permit faster and more effective processing of immigration applications.
- Enable the early identification and prevention of immigration and identity fraud.
- Facilitate processing at the border, including automation and improved border security.
- Strengthen the Department's ability to protect people from identity theft and the misuse of their travel documents and/or visas by others.

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

Biometric systems at the border will be implemented to improve facilitation and security. International experience has demonstrated that biometric processes can

¹⁵ *Department of Labour Statement of Intent 2010/11–2013/14.*
<http://www.dol.govt.nz/publications/general/soi2010/index.asp>

¹⁶ For example, the widespread use of online applications.

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.¹⁷ Reliable information about the cost and extent of identity fraud in New Zealand, however, is limited.¹⁸

2.2.1 Cost

The best estimates rely on scaling down figures from comparable countries. For example, a recent article¹⁹ 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.²⁰

Another recent article on the KPMG Fraud Barometer²¹ claimed a total of \$76 million was defrauded in New Zealand between July and December 2009 with a total for the year of \$100 million. The barometer (as is true of criminal law here) does not distinguish identity fraud from other frauds, but crimes such as fraudulent 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 theft.²² The Identity Theft Assistance Centre reported that identity theft affected 4.8 percent of the United States population in 2009.²³

2.2.2 Extent

The Department 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

¹⁷ *Immigration Act review Discussion Paper*. 2006. Section 11.

<http://www.dol.govt.nz/actreview/document/index.asp>

¹⁸ *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>

¹⁹ *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>

²⁰ General figures on economies from *CIA World Fact Book*.

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

²¹ *Fraud Barometer – June 2010*. New Zealand: KPMG, June 2010.

<http://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Fraud-barometer/Pages/June-2010.aspx>

²² *Consumer Sentinel Network Data Book January–December 2009*. Washington: Federal Trade

Commission, February 2010. <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf>

²³ <http://www.identitytheftassistance.org/pageview.php?cateid=47>

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 Department obtained some quantitative data following the introduction of biometric matching for onshore claims for refugee status, implemented upon the completion of the first PIA in 2010. A total of 10% of all cases checked using biometrics revealed identity fraud, immigration fraud or concealed criminality. These represent cases the Department would not have found using traditional biographic checking processes.

3. ASSESSMENT OF EXISTING IDENTITY OPTIONS

The Auditor-General's report on identity management highlighted the inadequacy of systems within the Department at that time. Those systems could not ensure that refugee status is granted only to genuine claimants nor could the Department 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 Department was to use biographic information only, it would remain over reliant on identity documentation, names and date of birth in order to identify people. This is information that fraudsters can easily change. 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 have to intensify.

Increased amounts of biographic information could potentially be easily useable, both by the Department 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 natural limit on its wider use.

Extra biographic information would be less effective than biometric information and potentially increase the chance of misidentification. It would be completely useless for 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.

Interviews have one major disadvantage: 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 border to facilitate the speedy processing of low risk travellers. They would be excessive for tourists and most other temporary visas.

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 Department's records systems. Transliteration of foreign-language names into English can be inconsistent.

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

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 Department 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 Department and other agencies that rely on Immigration for authoritative identity information and identity verification services.

4. SCOPE OF THE PRIVACY IMPACT ASSESSMENT

The scope of this PIA was to assess the Department's current and future practices with respect to the collection and handling of biometric information.

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 persons 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 Department's responsibility to manage the regulatory development and operational policy associated with the highlighted risks and to implement suggested mitigations.

The 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 Department 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.

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

5. PROCESS AND INFORMATION FLOWS

This section provides, as recommended in the *Privacy Impact Assessment Handbook*,²⁵ a 'careful and accurate description' of the biometric information flows within the Department. They show the situation today and in an ideal future state when all the biometric provisions of the 2009 Act have been implemented. The flow descriptions and diagrams show how biometric information is collected, circulates within the Department and is shared with external agencies.

5.1 Information collection

Internal information gathering

Information was collected from existing policy and procedures manuals, project plans and supporting documents for proposed initiatives, and face to face interviews conducted with relevant internal personnel. These interviews covered two aspects: existing and planned personal information collection and handling. They took place in Wellington, Auckland and London, and involved one on one or group interviews.

External information gathering/consultation

Because there is information sharing with third party agencies with an interest in biometric information, discussions also took place with relevant external stakeholders. They include the Department of Internal Affairs (DIA), New Zealand Customs Service (Customs), New Zealand Police (Police), Ministry of Foreign Affairs and Trade (MFAT), New Zealand Transport Agency (NZTA), Ministry of Agriculture and Forestry (MAF), New Zealand Food Safety Authority (NZFSA) and Ministry of Justice (MoJ).

Methodology

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 OPC was received and the questionnaires amended accordingly.

Subsequent to the first publication of this PIA, the document has been updated to reflect changes in the Department, the immigration system and the wider environment within which immigration operates.

²⁵ *Privacy Impact Assessment Handbook*, p.9.

5.2 Results

Tables 3 and 4 show the business units and external agencies interviewed and their collection and handling of biometric information, either as a primary handler or where the biometric information is secondary to their purposes.

Table 3: Business units interviewed

Business unit (internal)	Known biometric collection and/or handling	Primary or secondary handler²⁶
Settlement Services	<ul style="list-style-type: none"> • Nil 	N/A
Records and Documents	<ul style="list-style-type: none"> • AMS • Department of Labour Warehouse Portal 	Secondary
Strategic Programmes	<ul style="list-style-type: none"> • Biometric data not within scope 	N/A
Project and Integration Support	<ul style="list-style-type: none"> • AMS • Image database • Identity Report 	Secondary
Border Operations	<ul style="list-style-type: none"> • Fingerprints (from November 2011) • Photographs (compared manually) • Ability to upload electronic photograph to AMS • Fingerprints taken by Police on behalf of the Department (ink) 	Primary
Refugee Status Branch	<ul style="list-style-type: none"> • Fingerprints • Photographs (compared manually) • Ability to upload electronic photograph to AMS • (Also collect medical information but not as biometric information) 	Primary
Fraud Branch	<ul style="list-style-type: none"> • Fingerprints (from November 2011) • Photographs (compared manually) • Ability to upload electronic photograph to AMS 	Secondary
Compliance Operations	<ul style="list-style-type: none"> • Fingerprints (from November 2011) • Photographs (manually compare) • Ability to upload electronic photograph to AMS • Fingerprints taken by New Zealand Police on behalf of the Department (ink) • AMS 	Primary
Auckland Regional Manager	<ul style="list-style-type: none"> • Nil at present 	N/A
Pacific and Auckland Branches	<ul style="list-style-type: none"> • Photographs (compared manually) • Ability to upload electronic photograph to AMS • AMS • DNA data in some circumstances • Fingerprints in some circumstances (from November 2011) 	Primary
Refugee Quota Branch	<ul style="list-style-type: none"> • AMS 	Primary

²⁶ 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 handler²⁶
	<ul style="list-style-type: none"> • Fingerprints (from November 2011) • Photographs (compared manually) • Ability to upload electronic photograph to AMS • DNA data in some circumstances 	
Resolutions, Government Relations Unit	<ul style="list-style-type: none"> • Not collected for own purposes but may be used 	Secondary
Visa Services and Operational Support	<ul style="list-style-type: none"> • Not collected for own purposes but may be used 	Secondary
Information Management	<ul style="list-style-type: none"> • Nil 	N/A
Data Warehouse	<ul style="list-style-type: none"> • Image database 	Secondary
Wellington Branch	<ul style="list-style-type: none"> • Fingerprints in some circumstances (from November 2011) • Photographs (compared manually) • Ability to upload electronic photograph to AMS • AMS 	Primary
London Branch	<ul style="list-style-type: none"> • As above 	Primary
Intelligence	<ul style="list-style-type: none"> • ICE • AMS 	Primary
Internal audit	<ul style="list-style-type: none"> • Not collected for own purposes but may be used 	Secondary

Table 4: Agencies interviewed

External agency (including formal agents of the Department)	Known biometric processing	Primary responsibility or agent²⁷
DIA	<ul style="list-style-type: none"> • Photographs 	Primary
Customs	<ul style="list-style-type: none"> • Photographs (SmartGate) 	Primary – acting under the 2009 Act
Police	<ul style="list-style-type: none"> • Fingerprints: custodian/agent for collection/forensic expertise • Photographs • DNA 	Agent Primary for their own purposes
MAF and NZFSA	<ul style="list-style-type: none"> • Nil 	N/A
NZTA	<ul style="list-style-type: none"> • Nil 	N/A
MFAT	<ul style="list-style-type: none"> • Photographs (as an agent) 	Agent
MoJ	<ul style="list-style-type: none"> • Nil 	N/A

5.2 Information flows

The OPC requires that any PIA contains a careful, accurate and detailed description of the flows of personal information.²⁸ It is recommended that these

²⁷ 'Primary' indicates that the agency is responsible for the collection and management of the information, rather than the Department. 'Agent' indicates that the agency acts as an agent for the Department in some circumstances.

information flows be portrayed diagrammatically to clearly illustrate how data is collected or obtained, how it circulates internally, how it is disseminated beyond the Department and who has access to it.

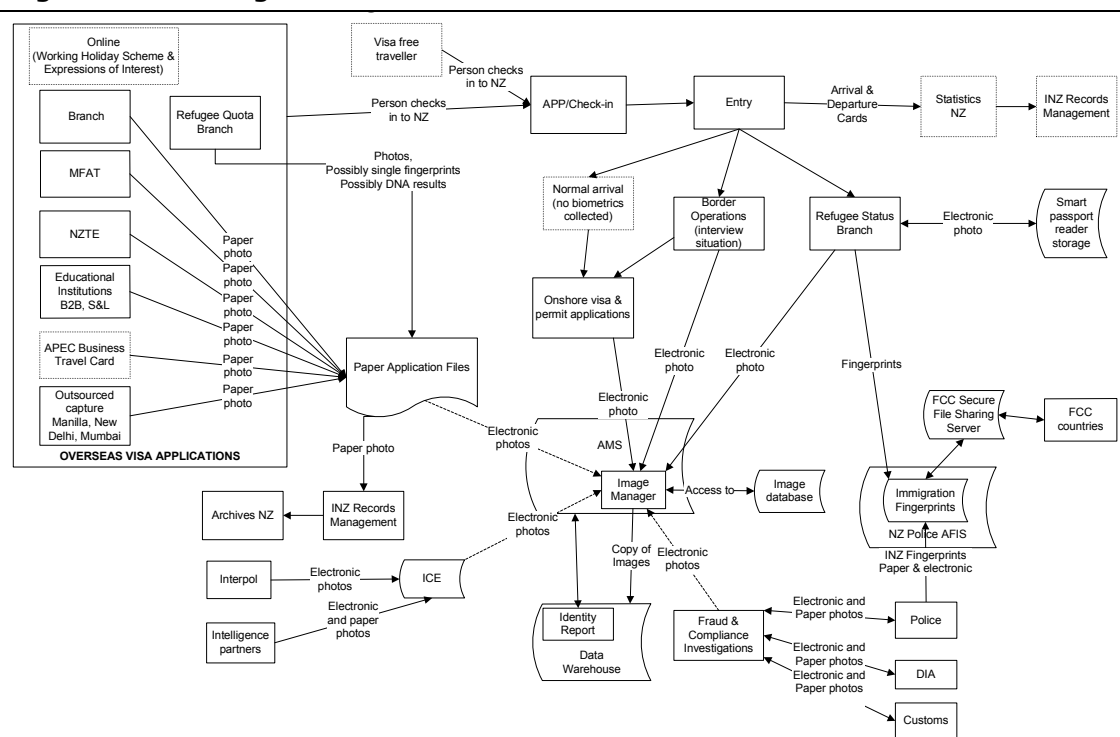
There are two distinct streams of information flows within the Department, current and prospective, as outlined below.

5.2.1 Current information flows

Biometric information is collected and used as a vital component of the identity establishment processes for people wishing to enter New Zealand. The broader identity information collection includes biographic information such as name and birth information found in a passport but also includes, amongst others, familial relationships, educational and work experience, New Zealand and foreign Police background checks and medical information.

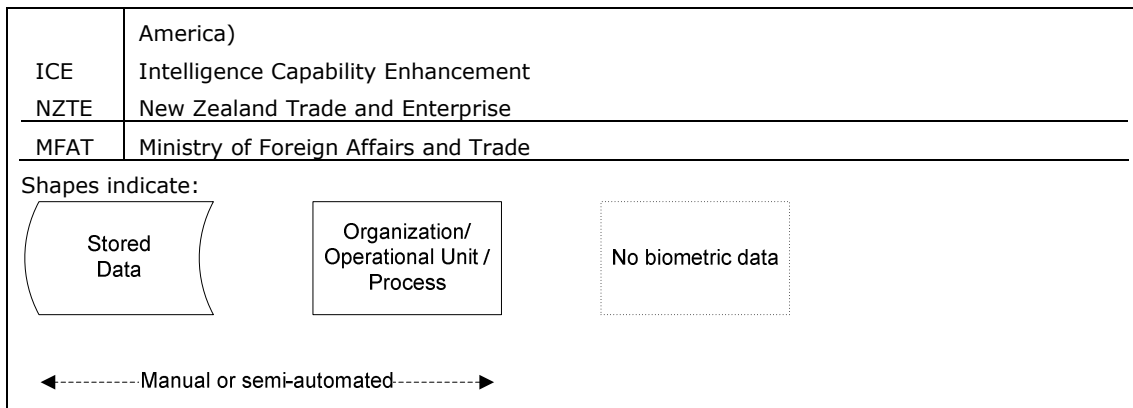
The current uses of biometrics are shown in the Figure 1.

Figure 1: Existing biometric information flows



Key	
Abbreviations used in diagram:	
AFIS	Automated Fingerprint Identification System
AMS	Immigration Application Management System
APEC	Asia Pacific Economic Cooperation
APP	Advance Passenger Processing
Branch	Department of Labour, Immigration Group Branch Office
FCC	(FCC) Conference (Australia, Canada, New Zealand, United Kingdom, United States of

²⁸ *Privacy Impact Assessment Handbook*. Wellington: Office of the Privacy Commissioner, 2007. ISBN 0-478-11703-5.



Current biometric information processes are either manual or semi automated. For example, hard copy photographs are scanned to provide a digital image. From November 2011 immigration staff will collect photographs directly from passports.

No biometric facial recognition ICT system exists within the Department. Biometric systems are not currently used for automated searching of face images against databases.

Currently, Refugee Status Branch collects live fingerprints from people; these fingerprints are processed – and any matches resolved – in a dedicated immigration system provided by NZ Police. Limited automated matching of fingerprints is carried out by the Police on behalf of the Department. All matches indicating identity fraud are confirmed by a fingerprint expert before any action is taken. From November 2011, fingerprints will be collected more widely by the Department. These uses are covered in detail in the appendices to this document.

All immigration fingerprints, whether taken by NZ Police or the Department, are stored on a segregated immigration database housed at NZ Police.

Boxes with dotted outlines indicate sources of information that do not currently include biometric information. They are included in this diagram to facilitate comparison with the future flows diagram (Figure 2).

Biometric information is collected as follows:

- 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. Visa applications require two photographs of the person applying.
- Applications may be made offshore or onshore, directly to the Department, or through an MFAT post, or through another approved lodgement agent.
- 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.
- Some MFAT posts have direct access to AMS including biometric information available through the Identity Report software application.

- Application collection (including paper photos) and basic data entry is done by third party providers 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, fingerprints (from November 2011) and occasionally DNA to substantiate familial relationships. DNA testing is done by an external contractor. The Department 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.
- Border and onshore asylum claimants are required to provide photographs and fingerprints.
- There are passport readers at Auckland and Christchurch 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.
- From November 2011, all immigration locations will begin to use a smart passport reader, enabling the capture of the photograph, which will be stored on immigration systems.
- The Police take fingerprints in some cases on behalf of Refugee Status Branch and Compliance Operations using ink on paper, which is subsequently scanned for entry into the immigration database within the Police Automated Fingerprint Identification System (AFIS).
- Some applications will contain fingerprints because Police check reports from other countries may contain them. These fingerprints are not currently used by the Department.

Once the Department 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.

Biometric information is stored as follows:

- AMS is the primary storage mechanism for the electronic information required to manage immigration case files:
 - 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 become hidden from view. 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.
 - AMS records are copied to the Data Warehouse each night.
- Digital photographs and scanned copies of information such as passport biographic pages are stored in a separate server (AMS image database).

- Photographs are copied from that server each night to the Data Warehouse.
- Information from the passport readers is initially stored on the computer to which each is attached and transferred into the image database. The introduction of smart passport readers in November 2011 will provide an automated mechanism for capturing photographs directly from the passport.
- ICE holds biometric information acquired from law enforcement partners.
- Refugee Quota Branch has a separate database for children's information.
- Fingerprints are stored in the immigration fingerprint database (AFIS), housed at NZ Police

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:

- 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.

Retention of Government records is subject to the Public Records Act 2005. The Department has not applied to Archives New Zealand for a Public Records Act authority to cover AMS as a whole. It is required to keep summary data held in AMS indefinitely. The Department is in the process of implementing an electronic records and document management system.

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

Biometric information is handled internally as follows:

- 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.
- Quota refugees arriving are compared with their photograph on record.
- Refugee Status Branch uses photographs and fingerprints to verify the identity of people who claim asylum on arrival in New Zealand.

- Compliance, Border and Fraud may use photographs and fingerprints to verify the identity and/or background of particular high risk people they are processing.
- Immigration Profiling Branch has access to AMS and therefore the image database because they process applications referred to them. Their focus for risk in these cases is on areas/countries of risk rather than the individual's personal risk profile.
- The Resolutions Team handles statutory complaints, revocations and deportations. They work with the paper files, which can include photos.
- Intelligence and Investigations have access to ICE, which contains images of faces. Investigations' primary focus is the original paper application, including its photo, as a fraudulent application.
- Biometric information transfers between ICE and the photo database are done by intelligence officers only.

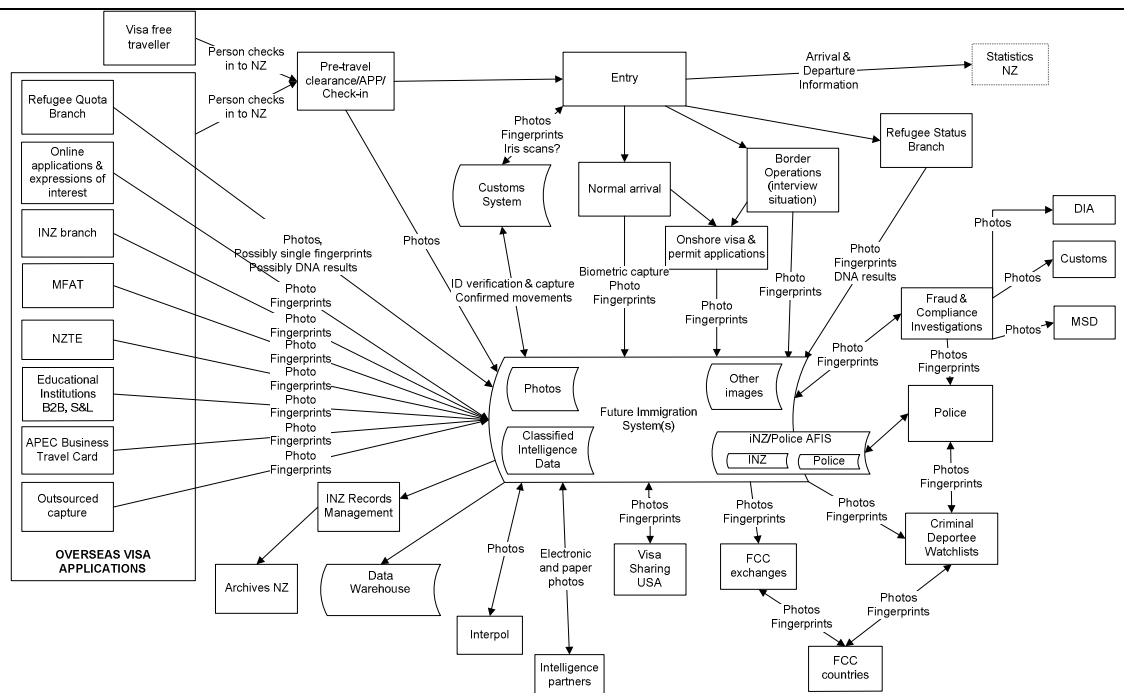
Biometric information is disclosed (shared with):

- Five Country Conference (FCC) partners (fingerprints via the FCC Protocol and photographs where required during specific requirements).
- Law enforcement agencies (Police, Interpol, SIS, Customs, DIA, Corrections).

5.2.2 Future (ideal state) information flows

Figure 2 shows the information flows for an ideal state some time in the future when all the biometric provisions covered by this PIA have been implemented.

Figure 2: Future biometric information flows



Key	
Abbreviations used in diagram:	
AFIS	Automated Fingerprint Identification System

AMS	Immigration Application Management System
APEC	Asia Pacific Economic Cooperation
APP	Advance Passenger Processing
Branch	Department of Labour, Immigration Group Branch Office
FCC	Five Country Conference (FCC) (Australia, Canada, New Zealand, United Kingdom, United States of America)
ICE	Intelligence Capability Enhancement
NZTE	New Zealand Trade and Enterprise
MFAT	Ministry of Foreign Affairs and Trade

Shapes indicate:

←----- Manual or semi-automated ----->

In the future, biometric information will be collected from a wider range of people. Direct electronic collection will be increasingly used in place of hardcopy collection.

Biometric information will be collected as follows:

- People who apply for a visa will be required to provide a 'passport grade' photograph.
 - That requirement may be met through the photograph on the application form, an electronic image with an online application, the biographic page on a passport or in an e-chip passport.
 - Where requested, foreign nationals may be required to provide an in person photograph and/or fingerprints.
- Airlines may be required to collect an in person photograph and/or fingerprints from all foreign nationals checking in to board a flight to New Zealand.
- New Zealand citizens arriving in New Zealand will be required to provide an in person photograph.
- 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.
- Collection will be done electronically wherever possible. For example:
 - applications are expected to become an online process – that process may use trusted digital photograph intermediaries / outsourcers to collect biometric information

- arrival and departure information will be collected electronically through border systems (Advance Passenger Processing, NZ Customs, overseas partner agency systems or airline Systems)
- fingerprints will be collected electronically using scanners – this will include third party visa application centres that collect information on the Department’s behalf
- the Department may introduce voice recognition capability as a way of authenticating people who wish to access the status of their application or similar customer services.

Biometric information will be stored in fewer systems than at present.

Biometric information will be stored as follows:

- 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.
 - The Immigration system will be linked to the NZ Customs system to transfer immigration information collected by them.
 - Information that requires separation, such as that in the Intelligence system, may remain outside the central immigration system or become a segregated database within central immigration system.
- Eventually, any remaining paper application records will be scanned into and managed by an electronic records management system that complies with the Public Records Act 2005.

Some extensions to the current information sharing activities with the FCC partners are planned.²⁹

Biometric information will be shared as follows:

- The FCC exchanges will be extended to include information about criminal deportees and formal intelligence exchanges of information.
- In addition, the current information exchanges will be extended in these ways:
 - The number of fingerprints sent by any one country to another will be increased.
 - In order to respond to that increased volume, the processing will move increasingly to an automated model.
 - Checks on a broader range of case types will be implemented such as high risk visa applications or trusted traveller enrolments.
 - It is expected that sharing of information about visa applicants will be initiated.

²⁹ 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/>. These arrangements are not covered in this PIA.

6. ANALYSIS OF GUIDING PRINCIPLES

The Cross Government Biometrics Group (CGBG), of which the Department is a member, developed guiding principles for the use of biometric technologies, published in April 2009.³⁰ It is intended for use by government agencies to inform decision making when considering biometric technologies for identity related business purposes.

The guiding principles express high level principles for agencies to consider when researching, planning and deploying biometric technologies. They are supported by a set of implementation principles (see chapter 7) that set out operational considerations. By taking these 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.

6.1 Justification for the use of biometric technologies for identity related purposes

The first guiding principle from the CGBG requires that agencies need to justify their decision to use biometric technologies. Specifically, they are advised to 'evaluate the need to use biometric technologies' and 'ensure that it is the most appropriate and cost effective solution'.

As described in chapters 1–3, the Department has done exactly that. The process included extensive public consultation. The proposed use of biometrics was discussed in section 11 of the Immigration Act review discussion paper.³¹ The Department received nearly 4,000 responses to that discussion paper, of which 102 related to the biometrics provisions.³²

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. For example, biometric

³⁰ *Guiding Principles for the Use of Biometric Technologies for Government Agencies*. Wellington: Department of Internal Affairs, April 2009. ISBN 978-0-478-29487-3

³¹ *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>

³² A summary of those responses is available at http://www.dol.govt.nz/actreview/summary/summary-immigration-h1_12.asp#_toc152047222

information about New Zealand citizens would not be retained unless a discrepancy was noted and the information was required for evidence.

Cabinet agreed that the Bill (now the 2009 Act) would enable:³³

- *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 for identity related processes must be lawful and appropriately authorised

The second guiding principle requires that, when government agencies use biometric technologies, 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.

6.2.1 Privacy Act 1993

Principle 1 – Purpose of collection of personal information

This principle provides that personal information should not be collected by the Department unless it is collected for a lawful purpose connected with a function or activity of the Department 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 Department 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 Department to carry out its responsibilities under the 2009 Act is a matter to be taken into consideration and is addressed at H1.

Principle 2 – Source of personal information

This principle requires that the Department 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 Department or its agents, including the actual provision of a passport and/or photo by a person.

³³ *Cabinet Policy Committee POL (06) 380, 17 November 2006.*

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

There are three major exceptions. The first is information received from the information exchanges conducted under bilateral agreements with other agencies (including those overseas). The Department 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).³⁴

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.³⁵

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.

Principle 3 – Collection of information from subject

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

- the fact that information is being collected
- the purposes for collection
- the intended recipients
- the contact details of the agency collecting the information and the agency that will store it
- the law under which the information is collected
- whether the supply is voluntary or mandatory
- the 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 Department will also publish information on its internet site relating to the collection and handing of biometric data. Existing practices in response to these risks that will be continued and updated to accommodate biometrics that are listed in Appendix 2.

This is a matter to be taken into consideration and is addressed at H4.

Principle 4 – Manner of collection of personal information

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

³⁴ <http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement/>

³⁵ Covered by section 96–100 of the 2009 Act.

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).

The Department's existing practices that comply with this principle will be continued and updated to accommodate biometrics that are listed in Appendix 2.

This is a matter to be taken into consideration and is addressed at H5 and H2.

Principle 5 – Storage and security of personal information

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

The Department's Code of Conduct³⁶ requires all employees to treat personal and confidential information with utmost care and to protect it from unauthorised 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.³⁷

The Department's existing practices that comply with this principle will be continued and updated to accommodate biometrics are listed in Appendix 2.

The Department's Removable Media Security Policy has been updated in 2011 to only allow the use of encrypted, Department 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 at G4, G5, G6, S1, S2 and S3.

Principle 6 – Access to personal information

This principle provides that, where the Department 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 Department and not merely to New Zealand citizens and people in New Zealand.

The Department 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 Department's existing practices that comply with this principle will be continued and updated to accommodate biometrics are listed in Appendix 2.

³⁶ *Department of Labour Code of Conduct*. Wellington: Department of Labour, May 2008.

<http://intranet/hrinfo/conduct/code-of-conduct/Pages/home.aspx>

³⁷ <http://intranet/tools/searchcenter/Pages/results.aspx?k=information%20policy&s=All%20Sections>

There are some procedural risks associated with this principle, addressed at H14.

Principle 7 – Correction of personal information

This principle provides that the Department 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 Department 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 Department's existing practices that comply with this principle will be continued and updated to accommodate biometrics are listed in Appendix 2.

There are some procedural risks associated with this principle, addressed at H14.

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

This principle states that the Department 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.

This is a matter to be taken into consideration and is addressed at H8 and H9.

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

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

Retention is a matter to be taken into consideration and is dealt with at H1 and H10.

Principle 10 – Limits on use of personal information

This principle provides that the Department 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 Department must be necessary for its functions or activities and people must be aware of those purposes. The Department 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 at H11 and S2.

Principle 11 – Limits on disclosure of personal information

This principle states that the Department 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 Department 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 at H12 and S2.

Principle 12 – Unique identifiers

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

The Department 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 Department 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 at H13 and H14.

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.

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

The Department is responsible for providing authoritative foreign national identity information to all government agencies.³⁸ 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*,³⁹ 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 Department is also bound by existing government policies regarding major ICT projects. Those include State Services Commission guidelines on ICT projects,⁴⁰ government standards⁴¹, the government procurement regime,⁴² the Gateway process (mandatory for all projects over \$25 million) and the Treasury's Capital Asset Management regime⁴³ and Better Business Cases for Capital Proposals.⁴⁴

The Department's participation in collaborative initiatives under the Joint Border Sector Governance Group will also be subject to the *Guiding Principles for the Use of Biometric Technologies*⁴⁵ developed by the Cross Government Biometrics Group of which the Department 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. That 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.

³⁸ <http://intranet/strategies/initiatives/workforceprojects/identity-and-biometrics/Pages/IdentityManagementStrategy.aspx>

³⁹ <http://www.dia.govt.nz/About-us-Our-Organisation-Directions-and-Priorities-for-Government-ICT>

⁴⁰ *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>

⁴¹ *E-Government Interoperability Framework*. Wellington: State Services Commission: 2008. <http://www.e.govt.nz/standards/e-gif-3.3>

⁴² http://www.med.govt.nz/templates/StandardSummary_43461.aspx

⁴³ <http://www.treasury.govt.nz/publications/guidance/mgmt/capitalasset>

⁴⁴ <http://www.infrastructure.govt.nz/publications/betterbusinesscases>

⁴⁵ *Guiding Principles for the Use of Biometric Technologies for Government Agencies*. Wellington: Department of Internal Affairs, April 2009. ISBN 978-0-478-29487-3.

In April 2006, a public discussion paper was released covering all aspects of the Immigration Act review.⁴⁶ Officials held public meetings in May and June 2006 to outline the proposals, which were attended by more than 650 people. The Department 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.⁴⁷

Cultural considerations include the Department 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 Department. The process flows identified at sections 5.2.1 and 5.2.2 describe how the end user (the person who will interact with the system) is to enrol, verify or identify themselves in terms of biometric information.

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 are appropriate and proportional to Departmental 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 Department intends to use both face and fingerprint biometrics.

⁴⁶ <http://www.dol.govt.nz/actreview/index.asp>

⁴⁷ http://www.dol.govt.nz/actreview/summary/summary-immigration-h1_12.asp

This combination provides the ideal combination of ease of collection via existing processes with high accuracy and high compatibility with overseas and domestic partners' capabilities. They will form the core of the Department's use of biometrics.

6.5.1 Fingerprints

Currently, the Department collects fingerprints from some clients. Their fingerprints are searched and stored in the immigration fingerprint AFIS database. The Police may also collect fingerprints on behalf of the Department for some cases, typically where the person has been in formal detention and served with a deportation liability notice by an immigration officer.

Fingerprints will be collected from refugees⁴⁸ 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.

Since June 2010, fingerprints collected for immigration purposes are stored separately from fingerprints collected for Police purposes.

The Immigration AFIS system provided by Police 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.

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.

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.

⁴⁸ Or be included in their identity documents.

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 arrangements with the Police raise governance risks identified at G6.

6.5.2 Face recognition

The Department does not have automated face recognition capability but is assessing systems for implementation.

Customs currently operates SmartGate. SmartGate allows New Zealand and Australian citizens who have e-chip passports 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.

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 almost always return a single matching candidate. This is why the Department uses fingerprints as its primary method for establishing identity. 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 Department 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 level of assurance. It is, essentially, what customs and immigration officers have done manually for a long time.

It is likely that the first applications of automated facial recognition in the Department will be where immigration clients use an automated system or in an enrolment required 'trusted travellers' system.

The use of joint systems at the border for face recognition raises governance risks that are identified at G3, G5 and G6.

6.5.3 Iris recognition

The 2009 Act includes iris scans in its definition of biometric information. At this time, the Department 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. These state that these obligations could include treaties and international agreements, UN conventions and those from relevant organisations such as the International Air Travel Association (IATA).

New Zealand is bound by a number of international treaties and has entered into a number of international agreements to which it must comply. The Convention Relating to the Status of Refugees⁵⁰ (the Refugee Convention) is included as a schedule of the 2009 Act, and it includes a process for determining New Zealand's immigration related obligations under the Refugee Convention, the International Covenant on Civil and Political Rights⁵¹ and the Convention Against Torture.⁵²

New Zealand has commitments as a member of the Five Country Conference (FCC). It is also a member of the International Civil Aviation Organization⁵³ and the Biometrics Institute.⁵⁴

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 highlighted as a risk at G1. 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 Department.

A strategic approach to the overall management of personal information, including biometrics is required, and options are outlined at page 65.

⁵⁰ <http://www.ohchr.org/english/law/refugees.htm>

⁵¹ <http://www.ohchr.org/english/law/ccpr.htm>

⁵² <http://www.hrweb.org/legal/cat.html>

⁵³ <http://www.icao.int/> – this organisation sets standards for passports and the information contained in them, especially machine-readable travel documents.

⁵⁴ <http://www.biometricsinstitute.org/>

7. ANALYSIS OF IMPLEMENTATION PRINCIPLES

The *Guiding Principles for the Use of Biometric Technologies for Government Agencies*⁵⁵ are expressed in a general way so that they can be useful for all government agencies and remain durable. The implementation principles support the guiding principles and identify the key operational matters to address when proceeding with the use of biometric technologies.

7.1 Information to end users and consultation with end users and stakeholders

As described above, the consultation process undertaken in April 2006 incorporated a variety of 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:

- 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 departments
- 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.

The Department has already developed a *Policy Framework for Collection and Handling of Biometric Information under the 2009 Act*, 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 all business units.⁵⁶

Application forms, arrival cards and a variety of information media (for example, pamphlets and websites) should advise end users and other interested parties of the ways in which biometric information will be collected and handled by the Department.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.

⁵⁵ *Guiding Principles for the Use of Biometric Technologies for Government Agencies*. Wellington: Department of Internal Affairs, April 2009. ISBN 978-0-478-29487-3.

⁵⁶ <http://intranet/strategies/initiatives/workforceprojects/identity-and-biometrics/Pages/ImmigrationAct-BiometricProvisions.aspx>

⁵⁷ <http://www.immigration.govt.nz/migrant/general/generalinformation/Identitymanagement>

⁵⁸ <http://www.immigration.govt.nz/migrant/general/generalinformation/operationalmanual>

7.2 Establishment of processes and procedures

In all instances where biometric information is handled, operational processes will need to be established to manage:

- all means by which biometric data is collected, converted, stored, compared, decisions are made about it or 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
- 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

According to the *Guiding Principles for the Use of Biometric Technologies for Government Agencies*, the Department must apply all relevant legislation and standards for the management of biometric information it collects.

This PIA will require updating and 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 Department manages a systematic process to conduct regular reviews and be able to ascertain and assess any of the changes as outlined in G8.

7.4 Establishment of procurement processes

In keeping with existing government procurement policies and guidelines,⁵⁹ when procuring biometric technologies, the Department will:

- undertake detailed scoping and definition of requirements in consultation with relevant agencies and stakeholders (where relevant)
- investigate opportunities for collaborative procurement
- investigate the option of 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.

As mentioned above, collaborative procurement and system development raise governance risks identified at G5 and G6.

⁵⁹ Government procurement policy framework, policies, mandatory rules, Auditor-General guidance and other material can be found at http://www.med.govt.nz/templates/Page_43367.aspx

7.5 Standards for interoperability

The Department aims to operate using internationally agreed standards for biometric information. For example, where there are relevant ISO/IEC JTC-1 standards,⁶⁰ those would be employed. There are other standards that are relevant.

For example, while not international standards, National Institute of Standards and Technology⁶¹ standards for exchanging fingerprint information are internationally accepted and used in the Five Country Conference (FCC) exchanges.

The Department is also a member of the Biometrics Institute,⁶² 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),⁶³ the International Civil Aviation Organisation (ICAO),⁶⁴ the International Labour Organisation (ILO)⁶⁵ and the Organization for the Advancement of Structured Information Standards (OASIS).⁶⁶

7.6 Legal information sharing and matching

All information matching or sharing of biometric data between the Department and any other agency will have legislative authority and/or the necessary agreements in place to ensure compliance with the Privacy Act 1993. Several provisions exist in the 2009 Act to regulate information sharing and matching (see sections 294–306).

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 <http://www.biometricsinstitute.org/index.cfm>

⁶³ The International Telecommunications Union is the relevant UN agency <http://www.itu.int/en/pages/default.aspx>

⁶⁴ International Civil Aviation Organisation http://www.icao.int/icao/en/m_about.html

⁶⁵ International Labour Organization <http://www.ilo.org/global/lang--en/index.htm>

⁶⁶ Organization for the Advancement of Structured Information Standards <http://www.oasis-open.org/home/index.php>

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 can be broken down into:

- governance
- handling practices
- security

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 Department. This assessment revealed that there was no comprehensive oversight of privacy matters within the Department. In particular, compliance is decentralised with no direct management by any one person or persons. Policies, instructions and guidance are generally targeted only towards the administration of information requests.

As well as specific risk mitigations, this section also provides options for the Department's consideration of an enterprise privacy strategy.

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

The Departments Business Services Group is responsible for effective privacy protection of personal information and oversees a coherent integrated strategy for managing the personal information it collects and uses. That is to ensure consistent practice and to manage the risk of personal information leaks, complaints to the Privacy Commissioner and public embarrassment.

Recommended mitigations:

- Review the privacy governance group which has the responsibility for policies and oversight of handling practices for personal information within the Department.
- The review will ensure effective responsibility for privacy issues, including a comprehensive consolidated personal information management strategy and reporting structures for privacy issues.
- The group contributes to Departmental '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 Department 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 Department is developing a privacy framework.

Recommended mitigation:

- Develop a comprehensive privacy policy that accommodates all aspects of the information management life cycle and all information privacy principles. This work is underway.

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 Department 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.

Recommended mitigations:

- Commit to incorporate 'privacy by design' for all new biometric and other personal information collection and handling systems in the Department.
- 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:

- 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 Department shares biometric information with other government agencies, both in New Zealand and overseas. When the agreements underlying those arrangements are not adequately drafted, the Department 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 mitigation:

- Include privacy considerations in collaborative undertakings with other agencies.
- Ensure that information sharing agreements do not compromise the Department'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 Department as well as contracts with the private sector.)

The Department 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 Department exposed to non-compliance with its statutory obligations including privacy responsibilities.⁶⁷

Recommended mitigations:

- 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 Department'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 Department should continue with the existing process for review and amendment of this PIA (or have a procedure for assessing the requirement to

⁶⁷ 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.
<http://www.e.govt.nz/policy/trust-and-security/government-use-of-offshore-ict-service-providers>

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.

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.⁶⁸ 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 Department needs to establish a strategy that reflects its values and statement of intent. Following is a guide to determine the scope of the strategy. It identifies four alternative approaches, ranging from narrow to broad:

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 Department 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 Department'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 Department 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

⁶⁸ *Privacy Impact Assessment Handbook*. Version 2.0. Wilmslow, UK: Information Commissioner's Office, June 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

overview of Departmental 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 Department'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 Department'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 Department's philosophy, mindset 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 Department'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 (FCC) Conference 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 Department's administrative efficiency, the management of waste and fraud and an integrated view of people across business units and even across the Department'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 Department 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 Department 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, 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 Department needs to consider with respect to both current and future information handling activities. Some of these require the establishment of processes to integrate with operating procedures. Awareness raising/training is of particular concern.

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 Department has statutory authority for the mandatory collection of biometric information under the 2009 Act. It is possible that specific implementations may not be in accord with that statutory authority.

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.

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.

H2 Staff make arbitrary 'requests' for biometric information

The 2009 Act permits the Department 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 Department 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 Department'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 Departmental employees or agents are inappropriate in their interactions with people when collecting biometric information, the Department 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:

- The Department's *Privacy Act Policy 2005* says that, 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 Department 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 are 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.

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 Department'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 Department 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. While proprietary technology militates against this, currently, iris scans all rely on one algorithm (mathematical process) and are particularly susceptible to use as an index mechanism.

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'⁶⁹ 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 Department moves towards collection of electronic biometric information, security becomes more important because the information becomes more portable and accessible than when kept solely in paper files.

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.⁷⁰

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.)

⁶⁹ http://ec.europa.eu/justice/policies/privacy/index_en.htm

⁷⁰ <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 Department takes reasonable precautions to protect the personal information it collects. It also requires that the Department 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 Department 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.⁷¹ 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.
- the ‘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.
- records of information correction requests and their outcome.
- records of any complaints made to the Chief Privacy Officer/Resolutions team.
- records of any complaints made to the Privacy Commissioner.

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:

- 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

⁷¹ *Privacy by Design*. Wilmslow, UK: Information Commissioner’s Office, November 2008. ICO/PBD/1108/1K.

business goals and privacy considerations addressed at every stage of the system's life cycle.⁷²

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.⁷³

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 Department 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 Department 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 Department 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 Department 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

⁷² 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>

⁷³ *Acceptable Use of Departmental Technology*. Wellington: Department of Labour, 20 October 2008. <http://intranet/support/security/information/Pages/acceptable-use.aspx>

generally. The overarching policy is the Department's Code of Conduct,⁷⁴ which addresses, at a high level, employees' responsibilities towards personal information and related responsibilities such as use of the Department's computer network.

Examples of more specific policies and guidelines are:

- Code of Conduct.⁷³
- Information Security Policy.⁷⁵
- Information Security Classification and Handling Policy.⁷⁶
- Physical and Environmental Security Policy.⁷⁷
- Acceptable Use of Departmental Technology.⁷⁸
- *Removable Media Security Policy*⁷⁹ and the Mobile Device Security Standard.⁸⁰
- general guidelines for all ICT users, managers, ICT managers and ICT operational staff.⁸¹
- privileged account authentication,⁸² cryptography⁸³ and firewall⁸⁴ standards.

⁷⁴ *Department of Labour Code of Conduct*. Wellington: Department of Labour, May 2008.

<http://intranet/hrinfo/conduct/code-of-conduct/Pages/home.aspx>

⁷⁵ Information Security Policy. Wellington: Department of Labour, 2 March 2010.

<http://intranet/support/security/information/policy-standards/Documents/High-Level-Information-Security-Policy-Draft.doc>

⁷⁶ Information Security Classification and Handling Policy. Wellington: Department of Labour, 23

November 2009. <http://intranet/support/security/information/policy-standards/Documents/High-Level-Information-Security-Policy-Draft.doc>

⁷⁷ *Physical and Environmental Security Policy*. Wellington: Department of Labour, 23 November 2009.

<http://intranet/support/security/information/policy-standards/Documents/physical-environmental-policy.doc>

⁷⁸ *Acceptable Use of Departmental Technology*. Wellington: Department of Labour, 20 October 2008.

<http://intranet/support/security/information/Pages/acceptable-use.aspx>

⁷⁹ *Removable Media Security Policy*. Wellington: Department of Labour, October 2008.

<http://intranet/support/security/information/policy-standards/Pages/removable-media-security-policy.aspx>

⁸⁰ *Mobile Computing Device: Configuration and Usage Standard*. Wellington: Department of Labour, 26

March 2010. <http://intranet/support/security/information/policy-standards/Documents/mobile-device-standard.doc>

⁸¹ <http://intranet/support/security/information/guidelines/Pages/home.aspx>

⁸² Privileged Accounts: Authentication Standard. Wellington: Department of Labour, 26 March 2010.

<http://intranet/support/security/information/policy-standards/Documents/privileged-account-authentication.doc>

⁸³ Cryptography Standard. Wellington: Department of Labour, 26 March 2010.

<http://intranet/support/security/information/policy-standards/Documents/cryptography-standard.doc>

⁸⁴ Firewall Standard. Wellington: Department of Labour, 26 March 2010.

<http://intranet/support/security/information/policy-standards/Documents/firewall-standard.doc>

These policies address current best practice in information security, specifically address the Department's handling of personal information and incorporate current best practices including encryption of any personal information when it is sent outside Departmental 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 Department'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 Departmental systems.

General security recommendations

1. Adopt the principle in the *Information Security Policy* 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 Departmental systems.
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 Department 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 (and best international practice suggests) that the Department reviews 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 Department 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 Department.

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 Department should consider:

- Within wider privacy governance systems manage Department wide privacy issues/risk including having assigned owners, accountability and closure steps and dates.
- how the identified risks will be appropriately 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.
- future management needs to be addressed – does/will the Department have a policy to require significant future changes to the system to be subject to a PIA?
- that this PIA is only relevant for as long as the fundamental assumptions upon which it based remain unchanged – if any parts of the system or processes are redesigned after completion of the PIA or if external circumstances change, what will happen?

11. CONCLUSION

This PIA is the first step in the Department's progress to implementing the biometric provisions in the 2009 Act. It is the first step to meeting the compliance obligation in section 32(3) of the 2009 Act. It 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 Department 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 Department will be increasingly collecting biometric information about everyone who enters or leaves the country, some security processes may require review and updating, and these are identified as security risks.

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

1. Maintain a governance group to provide comprehensive oversight of all Departmental privacy risks, to include a Chief Privacy Officer.
2. Develop comprehensive strategy and policy to manage all elements of information processing in the Department, including biometrics.
3. Create a risk register in which to log all privacy risks and assign accountability for them.
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 Department information is being handled by third parties.

APPENDIX 1 – ABBREVIATIONS USED

(the) 2009 Act	Immigration Act 2009
AFIS	Automated Fingerprint Identification System
AMS	Immigration Application Management System
APEC	Asia Pacific Economic Cooperation
APP	Advance Passenger Processing
Corrections	Department of Corrections
Customs	New Zealand Customs Service
(the) Department	Department of Labour
DIA	Department of Internal Affairs
EDRMS	Electronic Document and Records Management System
FCC	Five Country Conference (FCC)
FMR	False match rate
FNMR	False non match rate
ICAO	International Civil Aviation Organisation
ICE	Intelligence Capability Enhancement
ICT	Information and communication technology
IGMS	Immigration Global Management System (as planned)
ILO	International Labour Organisation
ITU	International Telecommunications Union
JBMS	Joint Border Management System
NZTE	New Zealand Trade and Enterprise
OECD	Organisation for Economic Cooperation and Development
MAF	Ministry of Agriculture and Forestry
MFAT	Ministry of Foreign Affairs and Trade
MoJ	Ministry of Justice
MOU	Memorandum of Understanding
NZFSA	New Zealand Food Safety Authority (now subsumed by MAF)
NZTA	New Zealand Transport Authority
NIST	National Institute of Standards and Technology (United States of
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
PIT	Privacy-invasive technology
PIA	Privacy impact assessment
PIRA	Preliminary impact and risk assessment
Police	New Zealand Police
RIA	Regulatory impact analysis
SAML	Security Assertion Mark up Language
SSC	State Services Commission
SIS	Security Intelligence Service
TOR	Terms of reference
UNHCR	United Nations High Commissioner for Refugees
UI	Unique identifier
UK	United Kingdom of Great Britain and Northern Ireland
UKBA	UK Border Agency
UNHCR	United Nations High Commissioner for Refugees
US	United States (of America)

APPENDIX 2 – PRIVACY RISK MITIGATIONS ALREADY IN PLACE

The Information Management Division Information Strategic Plan includes an action around developing a privacy framework for the Department which will 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 Department's operational 'business as usual' and are updated where appropriate to incorporate biometric privacy considerations.

Principle 3

All applicants complete a formal application to enter or remain in New Zealand – there are differing versions depending on the different status applied for.⁸⁵ All forms give indicative information about the processing of the information provided, including photographs.

All travellers to New Zealand 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 Department 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.

SmartGate⁸⁶ 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.

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*.

⁸⁵ <http://www.immigration.govt.nz>

⁸⁶ <http://www.customs.govt.nz/Border+sector/Trans-Tasman+travel/Q+and+As/Smartgate.htm>

There is already information relating to the exchange of biometric data under the Five Country Conference (FCC) Protocol on the Departments public web site.

Principle 4

The Department 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 Department 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 *Guidelines for All Users*⁸⁷, which states that users must:

- understand their personal responsibility as an information system user
- ensure that, when entering or leaving Departmental 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 Department has processes in place to manage access to and security of all personal information. Those processes have evolved to encompass the current reliance on paper-based primary documentation and are supported by automated systems (AMS and the associated Identity Report). These provide access to key information about applicants required for application processing.

Physical protection for paper documents includes the use of locked filing rooms for applications in branches and clear desk policies for officers handling personal information.

⁸⁷ *Guidelines for all users*. Wellington: Department of Labour, updated December 2010, <http://intranet/support/security/information/guidelines/pages/user-guidelines.aspx>

The current limited handling of biometric information is, in part, controlled by those existing processes and, in part, by newly devised and evolving processes. 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.

Internal compliance and policing of these policies is undertaken by a dedicated Internal Audit unit that, amongst other things, monitors system usage and, where necessary, acts on cases where use or access may be deemed unnecessary, suspicious or otherwise untoward.

Where fingerprints are shared with FCC partners, new 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 will require review and revision/replacement as the Department moves towards implementation of its future systems.

This principle further requires that the Department 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 Department'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 Department's information adequately.

Principles 6 and 7

The Department 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. That right applies to anyone whose information is held in an accessible form by the Department. Specifically:

*In immigration matters, where the Department has made a decision on a person's application for a permit or a visa, the Department'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.*⁸⁸

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 Department relies on Police experts to assess any apparent match between a sample fingerprint and fingerprints in the immigration fingerprint

⁸⁸ *Privacy Act Policy 2005*. Wellington: Department of Labour, October 2005. Section A.3
<http://www.dol.govt.nz/PDFs/privacyactpolicy.pdf>

database. At this time, the Department does not have such expertise internally and intends to continue to utilise Police experts for the foreseeable future.

It is Departmental policy that applicants are informed of any 'potentially prejudicial information' that the Department may hold and that they are given an opportunity to respond to or explain the circumstances behind that information.⁸⁹ 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 Department 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.⁹⁰

⁸⁹ *Immigration Operational Policy Manual*. Section A 1.5 Fairness. Wellington: Department of Labour, Updated 29 November 2010. <http://www.immigration.govt.nz/opsmanual/i8083.htm>

⁹⁰ <http://intranet/support/mydesk/managingrecords/pages/home.aspx>

APPENDIX 3 –MATRIX OF INITIATIVES BY SECTION

Biometric Initiatives	PIA Appendix	Immigration Act Section										
		60	96	100	104	111	120	149	288	289	290	291
Face Biometrics	4	x				x	x	x	x			
FCC Protocol Stage 2	5							x				
FCC Protocol Stage 3	6	x						x	x			
FCC Foreign Criminal Alerts	7						x		x			
RSB Enrolment	8							x				
Investigations and Quota Refugees	9	x				x	x		x	x	x	x

APPENDIX 4 – FACE BIOMETRICS

Background

Immigration New Zealand (INZ) and the New Zealand Customs Service are upgrading passport readers to improve the speed and accuracy of data entry, passport verification and automate 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.

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.

Passport images will be collected from:

- All foreign nationals; and
- Persons who claim to be New Zealand Citizens where their identity is in doubt. INZ will not store images where New Zealand Citizenship is proven.

Passport readers at INZ connect to the Department of Labour's (the Department) secure network. Primary line systems connect to Custom's secure network and applications. The face biometrics and bio page images are stored in the INZ Image System and linked to the client's immigration identity number in the INZ Application Management System (AMS).

NZ Citizens Face Images

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

If a visa holder becomes a citizen, INZ will retain the images for immigration purposes but no further images will be kept once citizenship is granted.

Face Biometrics of Children

Images of children under 10 years of age are not stored unless the passport is under investigation.

Future Uses of face biometric images

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

This will be 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.

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*	
60	Biometric information may be required from visa applicant.	Yes	All visa applicants, including at the border
104	New Zealand citizens photographed on arrival.	No	N/A
111	Applicant for entry permission to allow collection of biometric information.	Yes	All non NZ Travellers
120	Foreign nationals leaving New Zealand to allow biometrics to be collected.	Yes	All non NZ Travellers
149	Powers of refugee and protection officers (and their agents).	Yes	All non NZ nationals
288	Immigration officer may require biometric information to determine compliance with the 2009 Act.	Yes	All non NZ nationals

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.

Initiative specific risk(s)	Mitigation(s)
Authorisation to access biometric information is too widely approved	Access to biometric information only available to approved INZ staff.
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).

Initiative specific risk(s)	Mitigation(s)
	Information sharing agreements with other government agencies include measures to prevent unauthorised use or disclosure of biometric information.
Inadequately managed outsourcing does not adequately protect biometric information	<p>Passport images are captured by INZ staff, by Customs Officers at the border who are delegated as Immigration Officers under by s465 of the Act, and/or by automated systems (i.e. Smartgate).</p> <p>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.</p>
Biometric information unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification.	<p>Ensure that all implementations of the biometric provisions in the Act are in line with the statutory authority.</p> <p>Limit collection of biometric information to what is <u>needed</u> (essential business justification) to support current decisions.</p>
Staff make arbitrary requests for biometric information.	<p>Passports and client photographs are required by <u>all</u> foreign nationals during immigration application processes. Staff will not have discretion that can be abused.</p> <p>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.</p>
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.
People not adequately informed about the purposes of collection of biometric information.	<p>Privacy information is provided through INZ customer information channels (forms, arrival / departure cards, web and leaflets).</p> <p>The DoL biometric PIA is published on our public web site (www.immigration.govt.nz).</p>
The manner in which biometric information collected is unfair or intrusive.	<p>The Department collects and will continue to collect biometric data in a sensitive and culturally appropriate manner.</p> <p>The Department has procedures for handling cultural and physical considerations.</p>
The right of people outside the country who are not New Zealand citizens or residents, to access and request correction of their biometric information.	Continue the Department's <i>Privacy Act Policy 2005</i> which says that 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.

Initiative specific risk(s)	Mitigation(s)
The Department 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 Department already has procedures in place for requests for personal information.
Biometric information incorrectly associated with a person.	<p>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.</p> <p>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.</p>
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.
Information kept longer than is necessary.	<p>Passport and face images retained for the natural lifetime of the individual (or 50 years).</p> <p>If the immigration officer determines that the person is a NZ citizen, the image will be deleted by the immigration officer.</p> <p>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.</p>
Biometric information used for non immigration purposes.	Staff will be trained to ensure awareness in permitted uses of biometric information.
Disclosure of biometric information without reasonable grounds.	Staff will be trained to ensure awareness in permitted uses of biometric information.
Unnecessary assignment of unique identifiers.	Continue the current process of assigning unique INZ identifiers to people and records.
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.
Loss of biometric information.	All information will be kept and handled securely according to the Department's ICT security procedures.
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.

Initiative specific risk(s)	Mitigation(s)
	All information will be kept and handled securely according to the Department's ICT security procedures.
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 Department's ICT security procedures.

Date finalised: 8 August 2011

Version number: V1.0

APPENDIX 5 – FCC PROTOCOL STAGE 2

Current implementation approach

The Five Country Conference (FCC) Protocol is currently in operation. Four PIAs for implementation of the Protocol have been developed in consultation with the OPC, one each between Immigration New Zealand and the border / immigration authorities of the United States, the United Kingdom, Australia and Canada. Since April 2011, INZ has been sharing data with all four partners.

Immigration NZ has set up an immigration fingerprint capability with NZ Police in their Automated Fingerprint Identification System (AFIS). The Immigration fingerprint database is fully segregated from the criminal fingerprint database. This system is used by INZ to run the FCC Protocol.

Stage Two of the Protocol can manually share up to 3,000 fingerprint requests per year per country with a three day response time.

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 AFIS in order to detect identity and immigration fraud. If there is no match following a check, the fingerprints are destroyed by the receiving country.

If there is a successful match, further information is shared bilaterally.

Section

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

Section	Section Description	Biometric type		Client Group affected
		Face	Finger print	
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	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. Face or other biometrics are not used. The initial use of pseudonymous fingerprints to determine if the agencies involved share an interest in an individual is considered

Risk	Initiative specific risk(s)	Mitigation(s)
		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.
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' will be 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. DoL 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	DoL published a formal notification to advise of the implementation the FCC Protocol. This notification is placed on the DoL website and other relevant communication channels. A bilingual 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.
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	AFIS are extremely accurate particularly using all ten fingerprints (which the Protocol does). 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

Risk	Initiative specific risk(s)	Mitigation(s)
		reasonable opportunity to respond to harmful information.
H10	Biometric information retained longer than necessary	All Protocol fingerprints are automatically deleted after the search has been completed
H11	Biometric information used for non immigration purposes	<p>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.</p> <p>The information that New Zealand receives from FCC partners will be used exclusively for immigration and nationality purposes in both countries.</p>
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	<p>Immigration fingerprints are stored according to the same physical and technical security standards as criminal fingerprint data</p> <p>DoL 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 handled in New Zealand as required by a "restricted" classification. All fingerprint information will be securely deleted from the secure file server once the match cycle has ended.</p> <p>Only specified employees of DoL 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.</p>

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)

Version number: V1.0

APPENDIX 6 – FCC PROTOCOL STAGE 3

Current implementation approach

INZ is currently designing stage three of the FCC Protocol. The main component of stage three is the development of a real time data sharing platform which can be used to securely share data with FCC partners.

Background

Stage Three of the FCC Protocol will provide automation to the existing stage two process and enable larger numbers of fingerprints to be processed more quickly (30,000 per year per country with a two hour response time).

Stage Three is designed to be used for a greater range of clients; though is still intended only to check high risk applicants or subjects of immigration investigations. Low risk clients will not be checked via the Protocol.

The Stage Three platform will be used for other approved FCC data sharing initiatives in future and will not be restricted to fingerprint biometric sharing.

Section

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

Section	Section Description	Biometric type		Client Group affected
		Face	Finger print	
60	Biometric information may be required from visa applicant.	X	X	High risk visa applicants
104	New Zealand citizens photographed on arrival.			
111	Applicant for entry permission to allow collection of biometric information.	X	X	Border passengers under investigation
149	Powers of refugee and protection officers (and their agents).	X	X	Asylum claimants
288	Immigration officer may require biometric information to determine compliance with the 2009 Act.	X	X	Compliance and Fraud clients

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	<p>Individual PIA conducted with each overseas FCC partner.</p> <p>Measures taken to ensure that information sharing agreements do not compromise the Department's ability to meet its statutory obligations.</p> <p>Measures in place to prevent unauthorised use or disclosure of biometric information.</p>
H1	Biometric information unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification	<p>Only fingerprints of high risk clients are collected for checking via the Protocol. Face or other biometrics are not used.</p> <p>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.</p>
H2	Staff make arbitrary 'requests' for biometric information	<p>Only fingerprints of high risk clients are collected for checking via the Protocol.</p> <p>Definition of 'high risk' will be defined by INZ business rules and operational policy.</p>
H3	Biometric information not collected directly from the person concerned	<p>All biometric information collected for use in the Protocol is done so directly from the person concerned.</p> <p>DoL 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</p>
H4	People not adequately informed about the purposes of collection of biometric information	<p>DoL published a formal notification to advise of the implementation the FCC Protocol. This notification is placed on the DoL website and other relevant communication channels.</p> <p>A bilingual leaflet is given to all subjects fingerprinted by INZ explaining why we are collecting their fingerprints and how their biometrics will be handled. This will be reviewed for Stage 3, as Stage 2 only relates to asylum claimants.</p>
H5	The manner in which biometric information collected is unfair or	Include appropriate responses in operational policy, business processes and staff

Risk	Initiative specific risk(s)	Mitigation(s)
	intrusive.	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	<p>The Protocol requires participating countries to abide by all legal requirements within their own countries, including those relating to privacy.</p> <p>All INZ clients can request a copy of their biometric information from INZ. This same right is mirrored across FCC partners.</p>
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	AFIS are extremely accurate particularly using all ten fingerprints (which the Protocol does). 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 are automatically deleted after the search has been completed
H11	Biometric information used for non immigration purposes	<p>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.</p> <p>The information that New Zealand receives from FCC partners will be used exclusively for immigration and nationality purposes in both countries.</p>
H12	Disclosure of biometric information without reasonable grounds.	Not applicable for this project
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

Risk	Initiative specific risk(s)	Mitigation(s)
S2	Unauthorised access to biometric information	<p>Immigration fingerprints are stored according to the same physical and technical security standards as criminal fingerprint data.</p> <p>DoL 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 handled in New Zealand as required by a "restricted" classification. All fingerprint information will be securely deleted from the secure file server once the match cycle has ended.</p> <p>Only specified employees of DoL 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.</p>

Date finalised: 8th August 2011

Version number: V1.0

APPENDIX 7 – FCC FOREIGN CRIMINAL ALERTS

Current implementation approach

Biometric (face and fingerprints), biographic and criminality information will be received from, and sent to, FCC partners on foreign nationals removed from FCC borders who have committed serious criminal convictions.

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 of 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:

- 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; or
- who has, at any time, been removed, excluded, or deported from another country.

Fingerprints and face will be collected and sent to INZ by FCC partners on persons with serious criminal convictions who have been deported from their borders. Bi-lateral MOUs between FCC Partners will ensure that data is not loaded for New Zealanders or citizens or permanent residence class visa holders.

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

INZ will receive, match and store fingerprints on the INZ AFIS, housed at NZ Police. Fingerprint match results will be provided to INZ for auditing and investigation purposes.

INZ will send FCC partners biographic, criminality information and biometrics (fingerprints and face) of foreign nationals (excluding nationals of the receiving country) who have been deported for criminal reasons, and have been imprisoned for 12 months or more, or 5 years and greater (Immigration Act 2009).

Background

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 Department 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 Department and other agencies – the Department is the authoritative source of identity information for foreign nationals.
- conduct international identity checks with partner countries under the Five Country Conference (FCC).

Section

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 foreign national convicted for 12mths or more or more than 5 years
288	Immigration officer may require biometric information to determine compliance with the 2009 Act.	X	X	Any foreign national convicted for 12mths or more or more than 5 years

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 authorizations. • 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.	<ul style="list-style-type: none"> • Include privacy considerations in collaborative undertakings with NZ Police and FCC Partners. • Ensure that information sharing agreements do not compromise the Department's ability to meet its statutory obligations. • Require measures to prevent unauthorised use or disclosure of biometric information by FCC partners and NZ Police.
H1	Biometric information is unnecessarily or excessively collected and retained, including multiple types of biometric information (multi modal) collected without adequate justification.	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 Department's Code of Conduct and the exercise of it in situations where professional judgment is required.

Risk	Initiative specific risk(s)	Mitigation(s)
H3	Biometric information not collected directly from the person concerned.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Ensure FCC bi-lateral MOU's contain expectations of partners to adequately 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.
H8	Biometric information incorrectly associated with a person.	<ul style="list-style-type: none"> • All inbound fingerprints from FCC partners will be labeled with the AMS identity number in AMS prior to being stored in the AFIS; • All outbound fingerprints, face and biographics will be manually checked for matching accuracy before being sent to FCC partners. • 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.	<ul style="list-style-type: none"> • Processes for handling false negatives and false positives when matching biometrics will be developed.
H10	Biometric information retained longer than necessary.	<p>Business rules will be developed to:</p> <ul style="list-style-type: none"> • ensure biometrics are not retained for longer than the natural life of an individual; 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 nationality 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.
H13	Unnecessary assignment of unique identifiers.	Continue the current process of assigning a unique INZ identifiers to people and records.

Risk	Initiative specific risk(s)	Mitigation(s)
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 Department'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 Department'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 NZ Police and the Department's ICT security procedures.

Date finalised: 8th August 2011

Version number: V1.0

APPENDIX 8 – REFUGEE STATUS BRANCH

Current implementation approach

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 FCC partner databases under the FCC Protocol. Face images are collected and stored but not used as a biometric for matching purposes.

Background

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

- assist in identity establishment – biometric enabled identity management enables the Department 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 Department and other agencies – the Department is the authoritative source of identity information for foreign nationals.
- conduct international identity checks with partner countries under the Five Country Conference (FCC).

Section

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	
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)
G6	Not applicable in this instance.	RSB will be collecting the prints.
H1	Applicants lack a real choice about providing	The 2009 Act provides statutory authority for the collection of biometric information. This

Risk	Initiative specific risk(s)	Mitigation(s)
	biometric information.	information is necessary to enable the Department to undertake its statutory responsibilities. It will be used to help establish and verify the identity of the passenger. Passengers 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.
	Excessive collection was not identified as a specific risk as the proposed collection was limited and the rationale for the limitations described in full.	<p>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 Department 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. Advice was also sought from the Police on how fingerprints develop as children grow and at what age fingerprints become useful for automatic comparisons.</p> <p>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, the fingerprinting would be undertaken in the presence of the Police or a representative from Child, Youth and Family.</p>
H2	Not applicable in this instance.	See explanation in H1 – all claimants aged 14 years or over will be fingerprinted.
H4	People will not know what is happening with their information.	<p>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 Department'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 Department's use of authorised information matching. A translated brochure is available for asylum claimants and their representatives explaining the collection and handling of biometric information.</p>
H5	Not applicable in this instance	See explanation in H1 – all claimants aged 14 years or over will be fingerprinted.

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 personal information.	The Department's <i>Privacy Act Policy 2005</i> says that, 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	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 are 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 information will be securely stored in an immigration fingerprint database hosted within the Police Automated Fingerprint Identification System (AFIS). Access will be restricted to approved staff. It is not possible to access the fingerprint database through the Department's Application Management System (AMS). Criminals who are fingerprinted separately by Police will not have their fingerprints searched against the immigration fingerprint database.
H14	Widespread use of a common unique identifiers (UIs).	All people are assigned a unique identifier for all their dealings with the Department. 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 Department's ICT security procedures.

Date finalised: 09/11/2010

Version number: V1.0

APPENDIX 9 – INVESTIGATIONS AND QUOTA REFUGEES

Background

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

How will fingerprints be stored and searched?

Fingerprints collected will be searched and stored in the immigration fingerprint database and may also be searched via the Five Country Conference⁹¹ (FCC) Protocol.

Will face biometrics be used?

Face images (photographs) may be taken and manually compared, no face biometric matching will be conducted at this stage.

Who will be fingerprinted?

This initiative applies to the following case types:

- Border investigations of passengers of interest.
- Compliance investigations.
- 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).
- Persons seeking resettlement in New Zealand under the UNHCR Refugee Programme (Quota Refugees).

How will the fingerprints be used?

The use of biometrics in this initiative 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).

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.

- No fingerprints will be collected from New Zealanders

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 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 NZ under another identity.
- to facilitate the identification and deportation of those who use false identities in order to try to prevent their deportation.
- 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	High risk visa applicants.
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 whom 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.

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.

Initiative specific risk(s)	Mitigation(s)
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 Department of Labour (Labour) 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 Department's security procedures.
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.
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.
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 Department'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 Department'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.
The manner in which biometric information collected is unfair or intrusive.	See explanation in H1 and H2.
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 Department's <i>Privacy Act Policy 2005</i> says that, 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.
Adverse action taken against a person without that person given the	All potentially prejudicial information will be presented to the person for their comment or rebuttal, before an application is decided.

Initiative specific risk(s)	Mitigation(s)
opportunity to explain or challenge potentially prejudicial information.	
A perception that biometrics are 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.
The information will be used for purposes unrelated to an immigration determination.	The information will be securely stored in an immigration fingerprint database hosted within the Police Automated Fingerprint Identification System (AFIS). Access will be restricted to approved staff. It is not possible to access the fingerprint database through the Department's Application Management System (AMS). Criminals who are fingerprinted separately by Police will not have their fingerprints searched against the immigration fingerprint database, unless specifically authorised to do so via a Memorandum of Understanding between INZ and New Zealand Police.
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 Department's ICT security procedures. All biometric information collected will be encrypted before transmission.

Date finalised: 8 August 2011

Version number: v1.1

