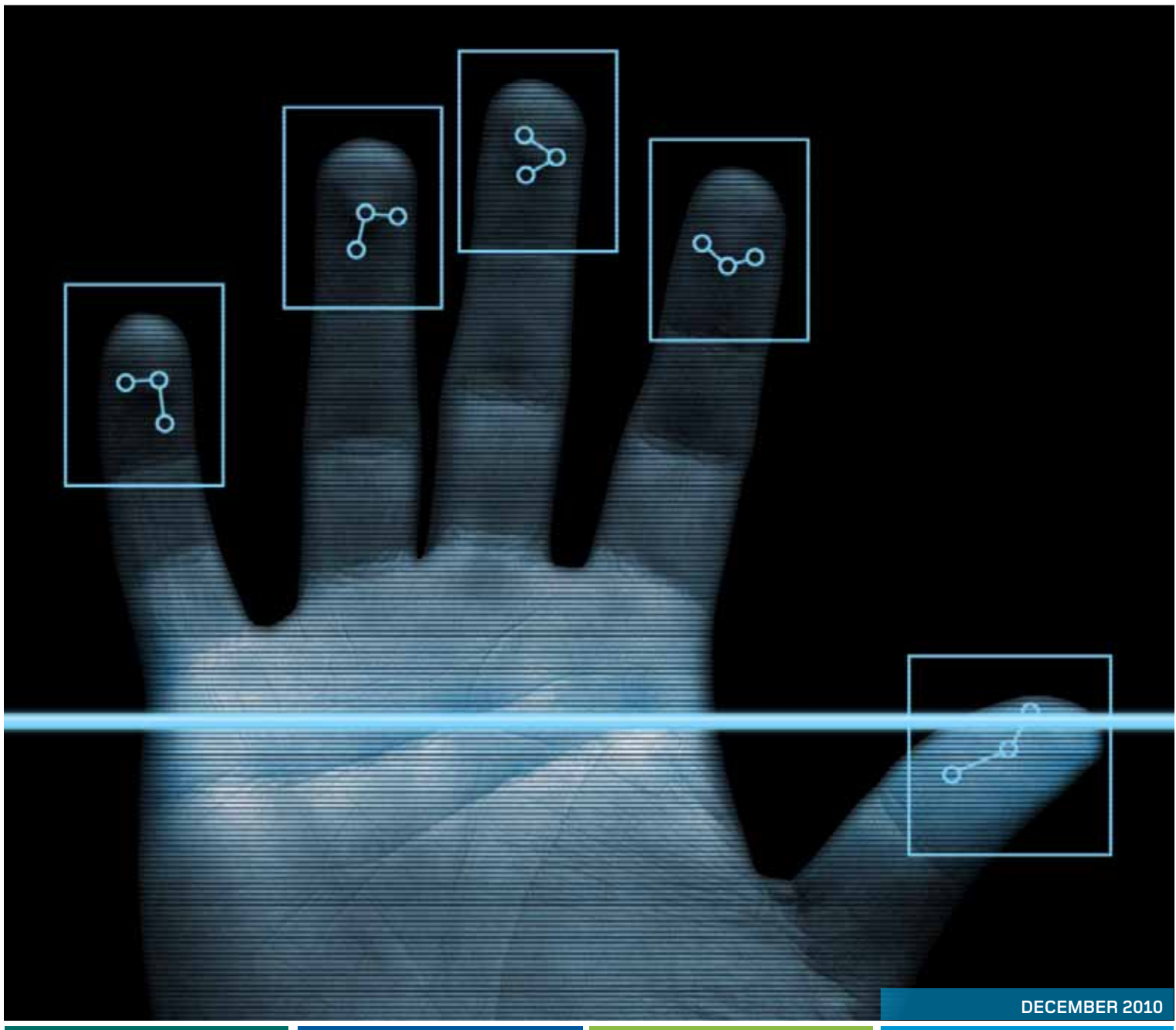


Privacy Impact Assessment

For the collection and handling of biometric information from asylum claimants



Contents

| | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------------------------------------------------------------------------------------|-----------|
| A. Introduction and overview | 2 | Principle 9 – Agency not to keep personal information for longer than necessary | 11 |
| Background: identity management for refugee and protection purposes | 2 | Principle 10 – Limits on use of personal information | 11 |
| B. Description of the project and information flows | 3 | Principle 11 – Limits on disclosure of personal information | 11 |
| Statutory authority to collect biometric information | 3 | Principle 12 – Unique identifiers | 11 |
| Information Flows | 4 | D. Privacy Risk Assessment | 12 |
| Collection of biometric information | 5 | E. Conclusion | 13 |
| Face recognition biometrics | 5 | | |
| Fingerprint biometrics | 6 | | |
| Rationale for collecting fingerprints from asylum claimants aged 14 and over..... | 6 | | |
| Process for collecting fingerprints from asylum claimants and persons subject to an investigation about their refugee or protection status | 6 | | |
| C. The privacy analysis | 7 | | |
| Principle 1 – Purpose of collection of personal information | 7 | | |
| Principle 2 – Source of personal information | 8 | | |
| Principle 3 – Collection of information from subject..... | 8 | | |
| Principle 4 – Manner of collection of personal information | 8 | | |
| Principle 5 – Storage and security of personal information | 9 | | |
| Principle 6 – Access to personal information | 9 | | |
| Principle 7 – Correction of personal information | 9 | | |
| Principle 8 – Accuracy, etc, of personal information to be checked before use..... | 10 | | |

A. Introduction and overview

This privacy impact assessment (PIA) has been prepared in conjunction with a proposal to Cabinet to bring into effect, by Order in Council, the provisions of the Immigration Act 2009 (the 2009 Act) that provide statutory authority for the collection and use of biometric information by Refugee and Protection Officers. This will enable the Department of Labour (the Department) to continue collecting biometric information by way of fingerprints from asylum claimants¹ aged 14 or over.

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

- assist in identity establishment – biometric-enabled identity management enables Immigration New Zealand (INZ) to be sure that the client has not already made an immigration application under another identity
- ensure reliable identification of clients in subsequent transactions both with INZ and other agencies – the Department is the authoritative source of identity information for non-New Zealand citizens
- conduct international identity checks with partner countries under the Five Country Conference (FCC).

This PIA covers the collection of biometric information in the form of fingerprints from asylum claimants aged 14 or over. Fingerprints are currently collected from asylum claimants who make their claim at the border (approximately 10%). The collection of fingerprints from all claimants is an extension of current practice. This PIA does not cover biometric related activities such as the use of facial recognition technologies or the collection of other biometric information such as iris scans.

Background: identity management for refugee and protection purposes

Effective identity management is critical to a well functioning immigration system. Identity fraud is the most common type of immigration prosecution. It is a major challenge for the Department which is responsible for processing immigration applications from all over the world.

The Department needs to be able to detect identity fraud to maintain the integrity of the immigration system and to effectively assess the legitimacy of asylum claims. Identity fraud is damaging because it can displace or delay genuine applicants and means the Department cannot assess an applicant's bona fides or eligibility to enter or remain in New Zealand. Public safety issues arise when fraudulent identities are used to conceal a criminal or extremist background. Identity fraud also imposes costs on the Crown, for example, when false identities are used to access government funded services or to fraudulently sponsor family members for residence.

Asylum claimants represent particular identity challenges and risk for the Department. Many have little or no documentation and any documentation held is not normally able to be validated with the issuing State. Successful claimants generally go on to live in New Zealand and may seek citizenship. There is an expectation that INZ will be able to reliably identify them. The use of biometrics reduces the risk of the asylum system being abused as well as the potential for down-stream costs to the Crown arising from identity fraud.

1. Asylum claimants, in this PIA, refers to persons who apply for recognition as refugees (s 129), as protected persons under the Convention Against Torture (under s 130) or as protected persons under the Covenant on Civil and Political Rights (under s 131).

The Office of the Auditor General's identity audit² highlighted areas for improvement in immigration processes, particularly focussing on significant weaknesses within the Department in identity management and 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 are seen to be key to effectively confirm identity and prevent the fraudulent use of multiple identities in the immigration system.

The weaknesses of traditional means of managing identity crime have led governments around the world to increase their use of biometrics to complement biographic identity checks used in immigration and border processes. Fingerprinting of asylum claimants for identification and background checks is standard practice in the United States (US), Canada, United Kingdom (UK), Australia and across the EU.

2. Controller and Auditor-General, Performance Audit Report, *Department of Labour: Management of immigration identity fraud*. June 2007. ISBN 0-478-18188-4

B. Description of the project and information flows

Statutory authority to collect biometric information

The Department has had statutory authorisation to collect biometric information in the form of fingerprints and photographs of refugee status claimants since October 1999³. Section 129H (1) (e) of the 1987 Act states that a refugee status officer “[i]n carrying out his or her functions” under Part 5 of the 1987 Act may: *“Require the claimant to provide or allow the taking of such fingerprints or photographs of the claimant as are reasonably necessary for the purpose of ascertaining or confirming the claimant’s identity or nationality.”*

This power can also be used when refugee status officers are determining whether to cease or cancel recognition of a person as a refugee⁴. Statutory authorisation under the 1987 Act, however, lapses at 2 am on 29 November 2010 when the 1987 Act is repealed and the substantive provisions of the 2009 Act come into force.

S 149(1)(e) of the 2009 Act, enables a Refugee and Protection Officer *“In carrying out his or her functions under this Part in relation to a claimant or to a person whose recognition as a refugee or a protected person is being investigated, a refugee and protection officer may ... e) require the person to allow biometric information to be collected from him or her.”* This power relates to asylum claimants⁵.

Section 31 of the 2009 Act allows Refugee and Protection Officers, or people acting on their behalf, to collect biometric information. Section 30 of the 2009 Act allows Refugee and Protection Officers to use this biometric information for specified purposes, for example, to verify a person’s identity.

The general biometric powers in the 2009 Act, including provisions relating to Refugee and Protection Officers’ collection power, do not come into force on 29 November 2010 (s 404 Immigration Act 2009, cl 2(2) Immigration Act 2009 Commencement Order 2010). Instead, these provisions will come into force by Order in Council at a date to be determined.

To enable the collection and use of biometric information in the form of fingerprints from December 2010 onwards, it is proposed that the relevant provisions of the 2009 Act come into force in December 2010 by Order in Council.

Information Flows

The diagram on the following page has been developed for the broader PIA underway to evaluate the complete set of biometric provisions under the 2009 Act. The process related to the collection of limited biometric information from asylum claimants is highlighted in green.

Collection of biometric information

The Department currently collects fingerprints from approximately 10 percent of all asylum claimants. That 10 percent are the people who make their initial claim at the border and are fingerprinted by the New Zealand Police (Police) on the Department’s behalf.

The remaining 90 percent of claimants enter the country normally and subsequently make an asylum claim. Typically, they are not fingerprinted but some form of photograph is collected either by photographing the person or copying one from an existing travel document. This has led to inconsistency in identity checks, as international checks through the Five Country Conference⁶ or Interpol can only

3. Protection under the Convention Against Torture and the Covenant on Civil and Political Rights is an addition to immigration legislation in the Immigration Act 2009.

4. Sections 129L(1)(a) to (c), 129M(b) and 129H(1)(e) of the 1987 Act.

5. Asylum claimants are persons who apply for recognition as refugees (s 129), as protected persons under the Convention Against Torture (under s 130) or as protected persons under the Covenant on Civil and Political Rights (under s 131)

6. The Five Country Conference (FCC) consists of the immigration authorities of New Zealand, Australia, Canada, the UK and the USA. Identity and background checks of asylum claimants can be made between FCC partners under the FCC Protocol using fingerprints

age at 14 is consistent with practice in other comparable jurisdictions such as Australia, Canada, the United States (US), Germany, Switzerland, Sweden and the EU 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.

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.

Process for collecting fingerprints from asylum claimants and persons subject to an investigation about their refugee or protection status

INZ has a dedicated immigration fingerprint database which will be the central storage point for the data collected. This database is hosted in, but segregated from, the Police's Automated Fingerprint Identification System (AFIS). Responsibility for the security of data lies with

the Police. Immigration data is stored under the same security controls that apply to access and use of the Police's database of criminal fingerprints.

The immigration fingerprint database is isolated from the Police's criminal database, but shares the same search engine and match resolution processes. A dedicated immigration process searches and registers immigration fingerprints within the immigration fingerprint database⁷.

The RSB will be equipped with a biometric enrolment station, built to the Department's ICT standards, and only authorised RSB staff will have access. It will be secured using appropriate levels of windows access credentials and client side antivirus and malware protection software to safeguard against any data repudiation attacks.

Following collection, the record will be encrypted and transferred to the Police system. There it will be searched against the INZ fingerprint holdings. If there is no match, the system will generate a new record. If there is a match, the result goes into a work queue for a fingerprint expert to manually verify.

7. This system is also used for FCC international immigration fingerprint checks. In this case, a separate 'FCC' work queue is used which searches and then deletes the probe fingerprints rather than registering them.

C. The privacy analysis

Principle 1 – Purpose of collection of personal information

The information will be collected and used to help establish and verify the identity of asylum claimants and persons subject to a subsequent investigation about their status. This information is necessary for the Department to carry out its responsibilities under the Immigration Act 2009.

To assist in identity verification, fingerprints collected will be matched against the Immigration Fingerprint Database to ensure the applicant is not already known to INZ under another identity. Fingerprints will not be matched against the Police criminal fingerprint database, but will be matched against FCC partner agencies as part of the High Value Data Sharing Protocol.

If fraud is suspected or established, the information may be provided to the INZ Fraud Branch or the Police or another government agency as per s151 of the 2009 Act.

Principle 2 – Source of personal information

The information will be collected directly from the asylum claimant, or protected person whose case is under investigation, by a Refugee and Protection Officer or from documents presented by the claimant under section 149(1)(e) of the Immigration Act 2009⁸.

Principle 3 – Collection of information from subject

All entrants to New Zealand complete an arrival card on entry that states that the biographic information collected is for immigration purposes. There is a formal Privacy Statement on the arrival card 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.

In relation to claims for asylum, an appropriately translated brochure has been developed and will be provided to all claimants. It states that all claimants must allow fingerprints to be taken if this is requested by a Refugee and Protection Officer and explains how this information will be stored and used⁹.

All asylum claimants also complete a 'Confirmation of Claim to Refugee and Protection Status' form. This form includes a declaration authorising INZ to share information with other New Zealand Government agencies and overseas government agencies in safe third countries.

Principle 4 – Manner of collection of personal information

Biometric data will continue to be collected in a sensitive and culturally appropriate manner. For example, veiled women will be provided with private facilities and female officers to verify identity (face to passport) or to capture a photograph. Otherwise, collection will occur in a private room with only an Officer and the individual present. An interpreter may be provided if required. People are able to bring their lawyer or a support person if they wish.

Principle 5 – Storage and security of personal information

The Department has systems in place to control physical access to and provide security for all paper immigration application files.

Electronic information including biometric information is also protected from unauthorised access and misadventure. Access to the image

8. (1) In carrying out his or her functions under this Part in relation to a claimant or to a person whose recognition as a refugee or a protected person is being investigated, a refugee and protection officer may – (e) require the person to allow biometric information to be collected from him or her.
9. *Immigration Fingerprint and Photograph Checks* is available from the Department. While the leaflet states that face images may be used biometrically, this process will not commence until the broader privacy impact assessment has been completed.

database is mediated by a special software application known as the identity report that can only be accessed through the Application Management System (AMS). It is not possible to access the fingerprints database through AMS. Access is restricted to approved Police fingerprint staff, via the same security processes (such as logins and auditing) that apply to the Police.

Direct access to the image database is restricted to approved Departmental staff on a 'need to see' basis (ie who deal with INZ clients) and it has no connection with external systems. Access to the image database is recorded and audited.

When biometrics information is being transferred it is treated as if it were classified as "Restricted" although it is formally classified as "In-Confidence"¹⁰.

Principle 6 – Access to personal information

The Department already meets the requirement in the recent amendment to section 34 of the Privacy Act 1993¹¹. The Department's internal policies cover the right of access and correction to all people about whom it has made a decision on immigration matter. 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.*¹²

If an individual is refused access to personal information, the letter they receive notes 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 7 – Correction of personal information

As described above, the Department upholds the rights of access to and correction of personal information under the New Zealand Privacy Act.

In particular, the Operations Manual advises that *"In all responses to information requests, the requestor must be advised of the right under Principle 7 to request correction of personal information; and to request that there be attached to the information a statement of the correction sought but not made."*¹³

It further states that¹⁴ all "... officers must act on the principles of fairness and natural justice when deciding an application." Fairness is defined as including whether the claimant is informed of information that might harm their case (often referred to as "potentially prejudicial information" or PPI) and whether the applicant is given a reasonable opportunity to respond to harmful information.

In the case of a disputed correction, a note would be placed in AMS outlining the situation. If necessary, the fingerprints would be destroyed or corrected. However, this is expected to be an extremely unlikely occurrence.

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

The Department's standard processes are designed to meet the requirement that information used in making immigration decisions is *"accurate, up to date, complete, relevant, and not misleading."*

The Operations Manual includes the following criteria in its definition of fairness, whether

- an application is given proper consideration
- only relevant information is considered
- all known relevant information is considered.

10. New Zealand ICT Security Manual (NZSIT 402:2008)

11. Section 34: substituted, on 8 September 2010, by section 5 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113).

12. *Privacy Act Policy 2005 section A.3* <http://www.dol.govt.nz/PDFs/privacyactpolicy.pdf>

13. In part A7.65 Right to request correction of information

14. Part A 'Fairness and Natural Justice'.

It advises officers 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; ...”.

Section 127 of the 2009 Act requires refugee and protection officers to act in a manner that is consistent with the Act or the Refugee Convention. Refugee and protection officers are also subject to the requirements of fairness and natural justice as outlined in New Zealand’s Bill of Rights Act. The Immigration (Refugee and Protection Status Processing) Regulations 2010 also outline certain mandatory steps that refugee and protection officers must take when assessing a person’s refugee or protection status.

In terms of the accuracy of the biometric matching, the fingerprint searching algorithm used by Police is recognised as being extremely accurate. It is the same algorithm trusted and used by Police in serious criminal cases. As an added precaution, however, all automatic matches would be validated by one of the Police’s fingerprint experts. Photographs would also be compared if appropriate.

Principle 9 – Agency not to keep personal information for longer than necessary

The Department keeps paper files on applicants for the natural life of the applicant or possibly longer if there are familial links or links to other individuals that need to be maintained. Once a physical file has no operational value, it is passed to Archives New Zealand as material of historical value.

Electronic records are kept indefinitely to ensure that links between individuals can be maintained. Biometric data will be retained for the natural life of the individual to support delivery of immigration services as they are required by the client.

Principle 10 – Limits on use of personal information

The biometric information collected from asylum claimants and persons subject to an investigation about their status would be used to assist in determining their refugee status. It would also establish their identity for any future immigration applications.

Principle 11 – Limits on disclosure of personal information

The Department discloses the information only as required or permitted by law.

Confidentiality provisions regarding refugee and protection claims are set out in section 151 of the 2009 Act. Details of a claim, including the fact that a claim has been made, can only be disclosed in certain prescribed circumstances. The claimant’s safety is the priority consideration.

Principle 12 – Unique identifiers

Immigration New Zealand has functioning systems for assigning a unique identifier to each client within its systems. Identifiers are assigned at the beginning of the immigration process, when an identity is created in AMS. It is based on the information the applicant provides INZ at that time, but may be updated if new facts come to light as part of the identity establishment process. The Department does not share these unique identifiers with any other agency other than when authorised under the Act. For example, s 294 of the 2009 Act provides for the disclosure of information for the purpose of information matching to identify the immigration status of persons sentenced to imprisonment or a community based sentence.

15. Natural life is currently defined as death or 80 years of age, whichever comes first. This policy will be clarified as part of the Department’s broader work to support the extension of biometric enabled identity management.

D. 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. [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: "Immigration Fingerprint and Photograph Checks".

| Summary of Privacy Risks & Mitigations | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk | Mitigation(s) |
| Applicants have a lack of real choice about providing biometric information as part of their asylum claim. | The 2009 Act provides statutory authority for the collection of biometric information from asylum claimants. This information is necessary to enable the Department to undertake its statutory responsibilities. It will be used to help establish and verify the identity of asylum claimants. Applicants 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. |
| The information will be used for purposes unrelated to refugee determination. | The information will be securely stored in an immigration fingerprint database hosted within the Police's 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. |
| 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 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 s.34 of the Privacy Act as amended on 8 September 2010. |
| 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 will be verified by a Police fingerprint expert. All potentially prejudicial information will be presented to the individual for their comment or rebuttal. |
| Adverse action being taken against an individual without that person being given the opportunity to explain or challenge potentially prejudicial information. | All potentially prejudicial information will be presented to the individual for their comment or rebuttal. |
| 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. |
| The extra step of converting the XML files to NIST format adds vulnerability | The system used to convert the files is built to a higher data security specification than standard DoL machines, and the room in which it is housed has extremely limited access rights. Transferral of fingerprint data from INZ to NZP will be encrypted. The system will be upgraded in 2012 to use XML, rendering the current conversion step unnecessary. |
| Information will be kept beyond the business requirements of the Department. | All formal applications for residence are kept indefinitely as records of historical interest and ultimately are transferred to Archives New Zealand. |

| Summary of Privacy Risks & Mitigations | |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk | Mitigation(s) |
| Widespread use of a common Unique Identifier (UI) | All individuals are assigned a unique identifier for all their dealings with INZ. That UI is not used by any other agency. |
| Individuals 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.</p> <p>It is available on the Department's website at http://www.immigration.govt.nz/migrant/stream/live/visa/ and in the Immigration Policy Manual http://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: "Immigration Fingerprint and Photograph Checks".</p> |

E. Conclusion

Statutory authority for the collection of limited biometric information from refugee status claimants is provided by the 1987 Act. This proposal would enable the Department to collect limited biometric information from all asylum claimants under the 2009 Act.

Biometric information assists the Department to verify an individual's identity and process their claim for asylum. The collection of this information will also enable the Department to participate in bilateral FCC data-sharing arrangements. Separate privacy impact assessments have been completed for the exchange of information with Australia and the UK.

The Department has developed the necessary processes and procedures to ensure the secure collection and storage of biometric information from asylum claimants. All information will be kept and handled securely according to the Department's ICT security procedures. An information pamphlet has been developed to explain the process for collecting and handling of biometric information to asylum claimants.

