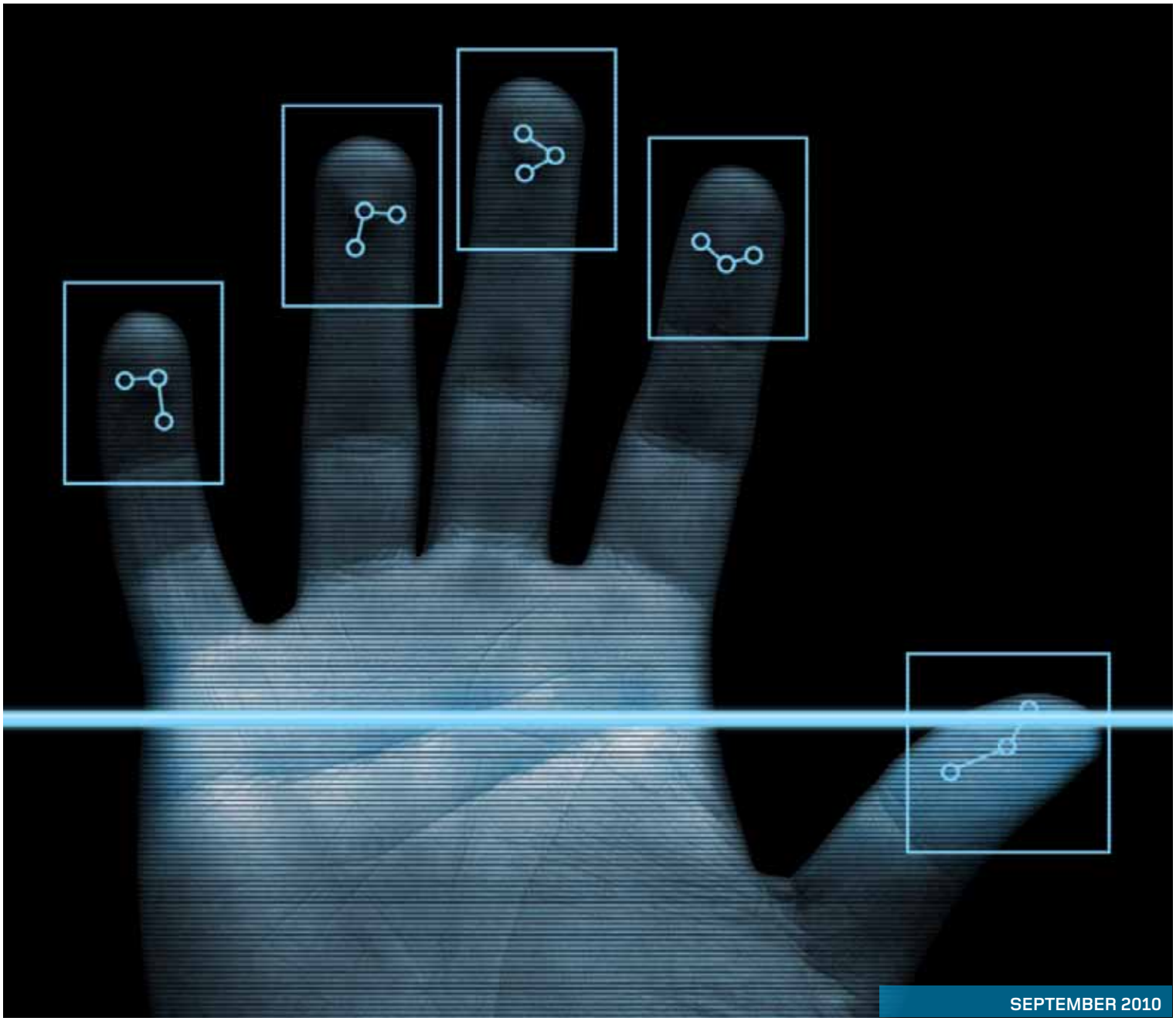
Privacy Impact Assessment

For Exchange of Information between the New Zealand Department of Labour and the United Kingdom Border Agency, as part of the Five Country Conference High Value Data Sharing Protocol



SEPTEMBER 2010

Agencies Involved

- **NZ Department of Labour (DoL) – Immigration New Zealand**
  NZ Sponsor
- **New Zealand Police**
  NZ data custodian
- **UK Border Agency**
  UK Sponsor
- **Immigration and Asylum Fingerprint System**
  UK data custodian

Contents

Executive Summary & Summary of Risks

A. Background

New Zealand and other countries are increasingly concerned about identity fraud being used to circumvent immigration and border controls.

The fraud may be used, for instance, to hide a criminal record or to take advantage of immigration processes that are seen to be vulnerable. For example, individuals use a false identity to claim refugee protection when they already hold residence or citizenship in a safe jurisdiction.

Governments are now working together to exchange information about high risk situations to reduce the impact of these types of fraud. One group includes New Zealand, Australia, Canada, the United Kingdom, and the United States of America - the Five Country Conference (FCC).

The High Value Data Sharing Protocol (The Protocol) is designed to allow the FCC countries to share information about high risk individuals applying to the immigration authorities of those countries.

Given the legal and operational differences in the five countries, it was decided that all sharing of information would take place as bilateral exchanges under the umbrella Protocol. Each bilateral exchange would be operated under a Memorandum of Understanding (MOU) between each pair of countries.

B. Benefits

The proposed exchanges are expected to deliver the following benefits:

- Improved integrity of New Zealand's immigration system. This will happen through the improved early detection of fraudulent identity and immigration claims, and the ability to close previously open files regarding absconders who may have covertly left New Zealand to an FCC partner country.
- Improved public safety through earlier detection of persons using false identities to hide criminal histories or terrorist backgrounds.
- Cost savings from the:
  - earlier detection of fraudulent identities and applications,
  - prevention of fraudulent secondary migration, and
  - prevention of fraudulent use of public services (e.g., benefit payments, health care, legal aid, public housing, police, courts and custody costs)
- Improved international reputation through maintaining parity and interoperability with modern immigration capabilities and ability to participate in security arrangements
- Enhanced ability to:
  - detect and analyse immigration trends
  - respond to and manage trends in the future.

C. The exchanges

Under the bilateral arrangement there is a cap of 3,000 match requests that can be made by each country per year. Under future arrangements, this may be increased to 30,000 (refer to sections 5.5.2 and 5.5.3) and FCC participants have agreed to review their privacy impact assessments before such an extension.

The overall FCC programme scale varies depending on the participants. In this bilateral exchange with UKBA, exchanges are expected to be small in terms of numbers of cases exchanged as outlined below.

The records of known nationals of any FCC country are excluded from these exchanges. No fingerprints of any known FCC national will be sent for pseudonymous matching.

The scale of the programme is expected to change with time.

In stage 2, (which this PIA refers to) the exchanges will be limited to enquiries on 3,000 cases per year per participating country as processing will be largely manual.

In stage 3, (Note: this PIA will be updated for stage 3) that maximum will increase to 30,000 cases per year from each of the other

participating countries and will be dependent on the development of a real-time automated identity checking system.

Initially, it is expected that New Zealand will send up to 3,000 fingerprints per year to UK for matching. They will be sent in batches of up to 50 records with the maximum permitted being 50 records in a week.

However, those limits under the protocol may never be reached. Cases will be selected for sending to UK according to two priority levels:

'A' - national security, asylum, fraud, compliance and detention cases where there are doubts over identity

'B' - individuals who have been granted leave to remain in NZ, but where doubts remain over identity.

In order to be sent for matching, the cases will also have to meet one or more of these criteria:

Immigration cases where identity of the individual is unknown or uncertain;

Immigration cases where the individual's whereabouts are unknown; and/or

Immigration cases where there is reason to suspect that the person has been encountered by more than one of the countries participating in the Protocol.

D. Purpose

The information that New Zealand receives from the UK will be used exclusively for immigration and nationality purposes in both countries. From the MOU clause 1.3, those are; "*…the consideration, regulation and enforcement of whether, and on what basis, any person may enter or remain in the territory of one of the Participants.*" The information is necessary in order for DoL to carry out its responsibilities under both the 1987 and 2009 Immigration Acts.

E. Notice

DoL is publishing a formal notification to advise of the implementation the FCC Protocol. This notification will be placed on the DoL website and other relevant communication channels.

Summary of Privacy Risks & Mitigations		
	Risk	**Mitigation(s)**
1	The right of people outside the country who are not New Zealand citizens or residents, to access and request correction of their personal information.	DoL'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.
2	Automated decision making and absence of human judgement.	All apparent matches will be assessed by a fingerprint expert before any action is taken.
3	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.
4	Information collected for one country's immigration purposes will be used by another country.	The disclosure of immigration information to another country and the use of another country's immigration information are explicitly permitted by statute. The FCC protocol and the MOU provide additional safeguards for the personal information subject to the exchanges.
5	DoL will be using information collected from its partner agencies in the FCC rather than directly from the individuals.	DoL has explicit statutory authority to collect and use this information.
6	The biometric information is compromised by a lack of security in storage or transmission.	All transfers of information will be protected by encryption. All information will be kept securely according to DoL standard procedures.
7	Information will be kept beyond the business requirements of DoL.	The Protocol and MOU restrict retention of information under these arrangements and require destruction of unmatched records used in the match process.
8	Widespread use of a common Unique Identifiers (UIs)	None of the participating agencies will assign UIs already assigned by another agency. Special UIs will be created to identify the fingerprints during the initial pseudonymous matching process so that existing UIs are not used for that process.
9	Individuals will not know what is happening with their information.	Information about the Protocol including Frequently Asked Questions will be published on the DoL website. Notification of the implementation of the Protocol will also be published on the website.
10	"Fishing" in government records	The Protocol targets only "high value" situations where identity documents are absent or there is reason to be concerned about a claimed identity.
11	Inaccurate information transmitted through multiple agencies' systems	Both the Protocol and the MOU require that the information exchanged be accurate and as complete and up-to-date as possible and that when errors are discovered, the other parties are notified.

1. Background

New Zealand and other countries are increasingly concerned about identity fraud being used to circumvent immigration and border controls.

The fraud may be used, for example, to hide a criminal record or to take advantage of immigration processes that are seen to be vulnerable. For example, individuals use a false identity to claim refugee protection when they already hold residence or citizenship in a safe jurisdiction.

Immigration fraud is damaging for two reasons. Firstly, fraudulent immigration claims displace or delay applications and claims by genuine applicants. This is particularly damaging for asylum candidates, many of whom are in difficult or dangerous situations. Secondly, once individuals obtain NZ residence – and potentially citizenship – through fraud, it is difficult, time-consuming and expensive to fix this.

Governments are now working together to exchange information about high risk situations to reduce the impact of these types of fraud. One group includes New Zealand, Australia, Canada, the United Kingdom, and the United States of America - the Five Country Conference (FCC).

The High Value Data Protocol is designed to allow the FCC countries to share information about high risk individuals applying to the immigration authorities of those countries.

Given the legal and operational differences in the five countries, it was decided that all sharing of information would take place as bilateral exchanges under an umbrella Protocol. Each bilateral exchange would be operated under a Memorandum of Understanding (MOU) between each pair of countries.

New Zealand is preparing to start information exchanges under the protocol with the United Kingdom. This PIA informs the MOU between the two responsible agencies.

The signing of the MOU is scheduled for later in 2010. Exchanges of information are scheduled to commence after the execution of the MOU.

There is a broader PIA in progress on the privacy impacts of biometrics collected and handled, generally, for immigration purposes[1]. The wider PIA will also be made public and may result in amendments or updates to this PIA.

1.2 The Issue

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.

Biometric information is explicitly defined in the Immigration Act 2009 as:

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

Biometrics are useful when people arrive undocumented or with false or suspicious documents. They are also useful when people try to prevent their correct identification by DoL.

Biometrics can help in the:

- early detection and prevention of immigration fraud,
- reduction of public safety risk by identifying individuals with criminal or adverse immigration histories, and
- reduction in the time and cost of dealing with immigration fraud downstream[2].

The immigration system is a significant contributor to the economic development of New Zealand. It is also a means for meeting

1. Immigration Act 2009, s.32
2. Other agencies directly affected by immigration fraud include Police, Housing, Health, Education and Ministry of Social Development

New Zealand's obligations under international agreements, such as the 1951 Convention Relating to the Status of Refugees and 1967 Protocol Relating to the Status of Refugees.

DoL is expected to assess immigration and asylum cases for legitimacy and to prevent abuses of the system. The proposed information exchanges with the UK involve high risk cases with the objective of maintaining the integrity of the immigration system.

1.3 Benefits of the Exchanges

The proposed exchanges are expected to deliver the following benefits to both countries:

- Improved integrity of New Zealand's immigration system. This will happen through the improved early detection of fraudulent identity and immigration claims, and the ability to close previously open files regarding absconders who may have covertly left New Zealand to an FCC partner country.
- Improved public safety through earlier detection of persons using false identities to hide criminal histories or terrorist backgrounds.
- Cost savings from the:
  - earlier detection of fraudulent identities and applications,
  - prevention of fraudulent secondary migration[3], and
  - prevention of fraudulent use of public services (e.g., benefit payments, health care, legal aid, public housing, police, courts and custody costs)
- Improved international reputation through maintaining parity and interoperability with modern immigration capabilities and ability to participate in security arrangements
- Enhanced ability to:
  - detect and analyse immigration trends
  - respond to and manage trends in the future

A final objective is to develop a statistical base on which to assess the value of different forms of data sharing. Preliminary statistical results and two case examples are available from the trials conducted by other FCC participants.

1.3.1 New Zealand experience to date

In July 2010, DoL successfully exchanged their first live fingerprint match requests under the Protocol with the Department of Immigration and Citizenship (DIAC) in Australia.

Additional information shows that:

- Approximately 130 false identities are detected at the border each year. This does not include false identities detected by DoL offshore or onshore.
- The number of people who successfully entered or departed New Zealand using false identities is (obviously) unknown
- Since August 2005, 257 false identities have been referred to the Police for inclusion in the Identity Protection Register
- Identity fraud is the most common type of immigration prosecution
- Numerous cases where persons have concealed 'safe third country' citizenship to obtain refugee status in New Zealand
- 29 cases of cancelled refugee status (serious fraud proved) involved identity fraud

1.3.2 Anticipated cost avoidance

Improved detection and prevention of attempted fraudulent entry to New Zealand is expected to reduce the costs of managing cases at the border and removals. Those costs can be significant.

Each case of refugee fraud conservatively costs DoL NZ$28,550. Additional Crown costs accrue from services provided by government, for example legal aid, health, education, housing and welfare. These additional downstream costs are not available.

There are reputational costs and public trust costs to having known criminals remain in New Zealand or leave with and misuse a fraudulently obtained New Zealand passport.

1.4 Alternatives to the Exchanges

The only other agencies that hold comparable information to that held by DoL are the partner immigration authorities in the other FCC

3. 'Fraudulent secondary migration' occurs when a principal applicant successfully acquires NZ residence through identity fraud and as a result helps other claimed family members to also migrate.

countries. Each country shares a desire to:

- maintain a secure border
- be better informed about those who remain illegally in their countries
- be better informed about those without a legal basis to remain in the country who have left other countries, voluntarily or by deportation/removal.

The Auditor General's report on identity management in DoL[4] highlighted the inadequacy of existing systems. Those systems cannot ensure that asylum and refugees status are granted only to genuine claimants, nor can DoL associate each individual with a consistent identity used across all immigration transactions. The report noted the absence of consistent routine use of biometrics to ensure reliable, consistent, person-to- identity verification.

FCC countries will use pseudonymous fingerprints only for matching. That will allow identification of individuals in each agency's records without disclosing any other personal information about that individual. In particular, no biographic information and no photographs will be disclosed with the fingerprints. That will only occur after a match of sufficient quality is made through the pseudonymous fingerprints and which warrants further disclosure.

Alternatives considered by the FCC would have required more disclosure of personal information in order to establish a shared interest in an individual. The current solution was decided upon as the least privacy-intrusive.

1.4.1 Alternative 1 - Using biographic information only

If DoL was to use biographic information only, the amount of information required from individuals would be greatly increased. The type of information and the amount of detail about each type of information would have to be augmented.

If this were the case, increased amounts of biographic information would be easily useable by many other agencies and for many other purposes. However, biometric information requires specialised equipment and specialised training of the human operators in order to be useful. This provides a natural limit on its wider use.

The increased amounts of information collected would increase the potential for scope creep and requests from other agencies for the information for purposes unrelated to immigration.

In addition, all extra biographic information would be less effective than biometric information and increase the chance of misidentification. It would be completely useless for people who arrive in New Zealand with no travel documents or 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[5].

1.4.2 Alternative 2 – Using photographs of people's faces

Another alternative considered was the use of pseudonymous photographs. Photographs are widely collected and available on travel documents and are a normal part of an immigration application to ensure that the person who enters a country is the same as the person who applied for entry.

However, photographs of people's faces (digital or otherwise) are easily viewed and recognised. In contrast, the specialised equipment and training required to identify a person from their fingerprints is not widely available. Face images (photographs) were therefore considered to pose more risk to privacy than fingerprint images.

Face recognition biometrics are also less accurate than fingerprint biometrics when run against large databases, with a correspondingly greater chance of error or ambiguity in the identification of matches.

4. Controller and Auditor General, Performance Audit Report, Department of Labour: Management of Immigration Identity Fraud. June 2007. ISBN 0-478-18188-4
5. Many cultures do not use the Western calendar, and other cultures do not necessarily place the same emphasis on date of birth as do our records systems. Transliteration of foreign-language names into English can be inconsistent.

2. General Privacy Concerns

2.1 Adequacy of Privacy Protection

The UKBA has produced a Privacy Impact Assessment for their own purposes for the exercise of this Protocol, see http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/. It has analysed the adequacy of privacy and data protection regimes in Australia, US and Canada, with an assessment of New Zealand's Privacy Act currently underway.

The Data Protection Act 1998 (DPA), which applies in the UK, establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. The legislation itself is complex and, in places, hard to understand. However, it is underpinned by a set of eight principles. The data exchanges proposed under the Protocol need to comply with, or be exempt from, these principles for the UK to participate in the Protocol.

2.1.1 Analysis of DPA principles

Principle 1 – fair and lawful processing. People whose information may be shared through the Protocol are routinely notified (usually when their fingerprints are initially captured) that their data may be subject to international checks. This principle also provides that personal data may only be processed where one of the conditions in Schedule 2 to the DPA is met, and that sensitive personal data may only be processed when one of the conditions in Schedule 3 is also met. The UKBA has provided assurances that at least one condition in each of these Schedules is satisfied and that personal information will only be processed to the extent that is necessary for the exercise of immigration and nationality purposes.

Principle 2 – obtained for limited purposes and not further processed for incompatible purposes. Immigration and nationality purposes are defined in this context as 'the consideration, regulation and enforcement of whether, and what basis, any person may enter or remain in the territory of one of the participants'. The UKBA has advised that fingerprints will only be checked through the Protocol for direct immigration and nationality purposes. Use of information received in relation to immigration-related benefits would not in itself be a reason to check fingerprints through the Protocol but may be a consequence in view of the information received.

Principle 3 – adequate, relevant and not excessive for the purpose. Data will only be processed to the extent necessary for the legitimate purposes, through a multilayered approach. The UKBA states that it will use the Protocol primarily to check:

- people who are due to be removed from the UK, in particular foreign nationals who are in UK prisons, but where this is not practicable because their identity and/or nationality cannot be confirmed; and
- asylum seekers, where there is a particular reason to do so, for example, because the person's identity is in question or unknown, or because the person is believed to be known to other FCC countries.

The UKBA further advises that there are safeguards to ensure that the operation of the Protocol remains proportionate and does not stray from the purposes for which it was intended:

- it is limited to check on immigration cases
- the purposes for which shared data may be used and the extent to which it may be further disclosed are explicitly defined
- the data that may be shared is defined to ensure that it does not go beyond what is relevant and proportionate for those purposes.

Principle 4 – accurate and up to date. The UKBA is confident that each of the country's fingerprint systems operates to a high degree of assurance. Further, the Protocol arrangements include:

- each country will provide other countries with an Interpretation Guide which explains how to interpret shared information

- all of the data exchange will, in each country, be handled by a central team
- the exchanged information will be, wherever possible, produced automatically from the relevant country's biometric database
- other information exchanged in accordance with the Search Code Guide will be provided in an agreed and understood format, restricted to factual, not subjective information
- each country will have an internal procedure for vetting and clearing any further information which is to be shared on a case by case basis
- arrangements to provide for cooperation between countries' central teams to liaise and correct any data found to be inaccurate

Principle 5 – not kept for longer than necessary. The UKBA states that personal information exchanged under the Protocol may only be retained as set out in it unless the agency that supplied the information has given its prior written approval. The UKBA has advised that it would not give such approval unless satisfied that the information was still relevant and further retention was appropriate.

Principle 6 – processed in accordance with the rights of individuals. The Protocol specifically sets out that no data may be exchanged that may not be disclosed to the individual to whom it relates. The DPA sets out requirements with respect to individuals' entitlement to access information about themselves with which the UKBA is bound to comply. If individuals consider that any of the rights under the DPA have been breached, they can complain to the Information Commissioner for investigation of the matter (see following).

Principle 7 – Security. All of the data exchanges will be conducted securely and using encryption through a Secured File Share Server (SFSS) hosted by the government of Australia. The UKBA advises that the security measures include technical measures in line with ISO17799/BS7799 standards. All data exchanges are bilateral and the SFSS is constructed in such a way that data can only be accessed by the country for which it is intended.

Principle 8 – Not transferred to other countries without adequate protection. The UKBA has assessed and approved the adequacy of data protection in the partner countries (to date, Australia, Canada and the US) with NZ still to be determined, though not considered, at this stage, to be an issue.

Protection/redress for the individual

Individuals affected by the information exchanges have a right of redress under the DPA. This Act gives individuals important rights including the right to know what information is held about them and the right to correct information that is wrong.

The Information Commissioner is the supervisory data protection authority in the United Kingdom. In this role he has a duty to exchange information with the other supervisory authorities in the EEA states and also the European Commission. He also has a duty to help other supervisory authorities investigate complaints about the processing of personal data outside the UK where the data controller is UK based. He has specific duties in relation to certain decisions he may make about the international transfer of personal data.

Further, the Commissioner is responsible for administering the provisions of the DPA and this makes him responsible for:

- promoting good practice in handling personal data, and giving advice and guidance on data protection;
- keeping a register of organisations that are required to notify him about their information-processing activities;
- helping to resolve disputes by deciding whether it is likely or unlikely that an organisation has complied with the Act when processing personal data;
- taking action to enforce compliance with the Act where appropriate; and
- bringing prosecutions for offences committed under the Act (except in Scotland, where the Procurator Fiscal brings prosecutions).

The Information Commissioners' Office (ICO) has legal powers to ensure that organisations comply with the requirements of the DPA. It is important to note that these powers are focused on ensuring that organisations meet the obligations of the Act. In this respect,

any individual who considers that their personal data has been compromised by or they feel adversely affected by the use of their personal data in information exchanges under the Protocol, can make a complaint to the Commissioner for assessment of their grievance, with ultimate determination in UK courts.

Given the rigour of the DPA and the similarity of its principles to the information privacy principles in the New Zealand Privacy Act, personal information will be protected in the UK as well at would be in New Zealand with similar rights of redress and complaint available to individuals.

2.1.2 The Framework of Formal Agreements

The FCC information exchanges are governed by the Protocol, the Hunter Valley Declaration, (neither of which are legally binding treaties) and a series of bilateral memoranda of understanding between pairs of participants[6].

The Hunter Valley Declaration states:

We intend to uphold high standards of privacy and the protection of personal information, in accordance with the privacy legislation of our respective countries.

The draft MOU between New Zealand and the UK includes the commitment to:

2.6 The Participants intend to ensure that the fingerprints exchanged for searching under this MOU are not to contain fingerprint data of known FCC nationals.

This reflects similar conditions in other MOUs between the FCC participants. Consequently, neither UK nor New Zealand citizens would normally be subject to the activities under the Protocol. However, a match might uncover the fact that an individual using a fraudulent identity was also a citizen of an FCC country. That could result in an investigation for immigration fraud.

For example, in a match between US and UK records, a Somali asylum claimant in the UK was found to be a naturalised Australian citizen.

If a similar situation arose in New Zealand, it is possible that a person who received New Zealand citizenship by grant or descent (or the UK equivalents) might be retrospectively investigated for fraudulent acquisition of citizenship. Such a person would be entitled to protection under the New Zealand Privacy Act until after both their citizenship was revoked and they were removed from New Zealand, if either of those actions was eventually taken against them.

2.1.3 Procedural issues

The DoL Immigration Policy Manual provides standard guidelines for immigration officers. They cover the verification of credentials to meet criteria for entry visas (temporary or permanent). Verification ranges from relatively superficial checks to thorough background investigations. It may include the use of specialised expertise such as forensic analysis.

In each area of credential verification, the third tier of investigation is always an in-person interview.

Where potentially prejudicial information exists, *"…applicants will be given the opportunity to comment before a decision is made on the basis of any potentially prejudicial information that they are not necessarily aware of.[7]"*

2.2 The Information Exchanges

The scale of the programme is limited by:

- number of agencies involved,
- number of individuals whose information will be exchanged or
- amount of information that will be disclosed

as described in the following sections.

Under the bilateral arrangement there is a cap of 3,000 match requests that can be made by each country per year under stage 2. Under a future stage 3 arrangement, this may be increased to 30,000 (refer to sections 5.5.2 and 5.5.3) and FCC participants have agreed to review their privacy impact assessments before such an extension.

The costs to DoL are minimal as the initiative uses existing infrastructure and arrangements.

6. Copies of the High Value Data Sharing Protocol and the Hunter Valley Declaration will be provided to the New Zealand Privacy Commissioner with this document.
7. Operational Manual E7.15 http://workforce.dol.govt.nz/toolkit/html/inzmanual/index.htm

The information flows and key decision points are shown in the diagram on page 13.

2.2.1 Number of Agencies

There are two New Zealand agencies involved in this bilateral exchange. The New Zealand Police currently act as custodian for DoL fingerprints and provide the expertise necessary to assess potential matches.

DoL fingerprints are stored in a segregated environment provided by the Police and are isolated from Police records. When match requests are received by DoL from the UK, the matching will be performed against these DoL fingerprints only.

Matching against the Police criminal fingerprint database will not be conducted under the FCC Protocol.

2.2.2 Number of Individuals

The overall FCC programme scale varies depending on the participants. In this bilateral exchange with UKBA, exchanges are expected to be small in terms of numbers of cases exchanged as outlined below.

The records of known nationals of any FCC country are excluded from these exchanges. No fingerprints of any known FCC national will be sent for pseudonymous matching.

The scale of the Programme is expected to change with time.

- In stage 2, (which this PIA refers to) the exchanges will be limited to enquiries on 3,000 cases per year per participating country as processing will be largely manual.
- In stage 3, (Note: this PIA will be updated for stage 3) that maximum will increase to 30,000 cases per year from each of the other participating countries and will be dependent on the development of a real-time automated identity checking system.

Initially, it is expected that New Zealand will send up to 3,000 fingerprints per year to UK for matching. They will be sent in batches of up to 50 records with the maximum permitted being 50 records in a week.

However, those limits under the protocol may never be reached. Cases will be selected for sending to UK according to two priority levels:

'A' - national security, asylum, fraud, compliance and detention cases where there are doubts over identity

'B' - individuals who have been granted leave to remain in NZ, but where doubts remain over identity

In order to be sent for matching, the cases will also have to meet one or more of these criteria:

- Immigration cases where identity of the individual is unknown or uncertain;
- Immigration cases where the individual's whereabouts are unknown; and/or
- Immigration cases where there is reason to suspect that the person has been encountered by more than one of the countries participating in the Protocol.

Even the potential maximum of 30,000 per year in Stage 3, is relatively small in comparison with the numbers of total cases handled by DoL as in 2008/09:

- 1.4 million people granted a temporary permit
- 88,300 permanent and long-term arrivals

New Zealand has a comparatively small number of asylum seekers. In 2008/09, only 246 people sought this status in New Zealand. If all asylum seekers were checked through the Protocol exchanges, it would amount to less than 10% of the cases allowed for matching in Stage 2.

2.2.3 The Amount of Detail Exchanged

Each match progresses through up to 3 processes of information disclosure. These are known in the Protocol as "Tiers". An unsuccessful match request results in a Tier 1 response which simply advises 'no match.'

INITIAL MATCH REQUEST

In the initial match request, fingerprints are encrypted and transmitted from the 'Requesting Country' to the 'Providing Country' with no accompanying identifying information other than a unique identifier (UI) created for the purposes of the match and a search type code.

This has been referred to as pseudonymous or nigh-anonymous information disclosure. The UI is completely separate from any UIs used by the agencies in their own systems and any UIs

that relate to the individual such as a passport number. Prints are usually sent in batches of 50 but may be sent in smaller batches if warranted.

TIER 1

All match requests are run by the Providing Country. If a match occurs, the Providing Country that received and matched the prints against their own records will respond within three (3) days with Tier 1 information that there was a successful match. They will also include as much of the following information as they can obtain within the three days:

- date, location, and reason fingerprinted
- last name, first name, and any other names the person is known by
- date of birth, place of birth, nationality, and gender
- any travel document number(s)
- any photograph(s) held in their files or any other facial images, and/or a scan of the passport bio-data page
- any caveats around information source and usage
- other information as deemed appropriate by the Providing Country

All the fingerprint sets in a batch that did not match, will also be recorded in the Tier 1 information sheet list as a no-match (i.e. the record will give the fingerprint UI plus the NO MATCH indicator).

In all cases where biometric matches are achieved, after receipt of the Tier 1 response sent from the Providing Country, the Requesting Country must also provide back to the Providing Country the standard Tier 1 bio-data elements, to the extent that they are available within its own system or otherwise readily obtainable.

The reasons for this bilateral exchange of Tier 1 information are:

1) So both countries can be assured that they are dealing with the same individual by comparing photographs and biographic data
2) To permit the providing country to confidently remove the individual from any overstayer list and cease compliance activity for that person
3) To verify that the individual is not, in the Providing Country's jurisdiction, the subject of an outstanding arrest warrant (of sufficient severity to warrant extradition proceedings).

TIER 2

If the information available from the Providing Country is incomplete or unavailable within those three days, the providing Country may send a second Tier 2 information response within the next seven (7) days. That second response can include any of the standard data elements listed above that are not available in the biometric system, but are available elsewhere.

In all cases where the match includes a travel document issued by a country of which the person is not a national (e.g. a refugee travel document), confirmation of the type of document, the country of issue of the document and the nationality of the person must be shared under Tier 2.

In all cases where a match is achieved against a watchlist, the reason for the watchlist entry should be shared.

TIER 3

If further information is required, then information sharing moves up to Tier 3. This requires the Requesting Country to send an approved FCC 'Request for Information' form to the Providing Country.

The request for information must include who the request is about (UI, biographic information, etc), what additional information is required from the Providing Country, and why this information is required.

The Providing Country may then provide further information if this is appropriate and permitted under their laws. Note: the Protocol does not require participating countries to guarantee to provide Tier 3 information.

SEARCH CODE LIMITATION

The search code attached to each initial request:

- identifies the reason for the fingerprint being sent for matching, and
- determines the type and amount of information that is sent back.

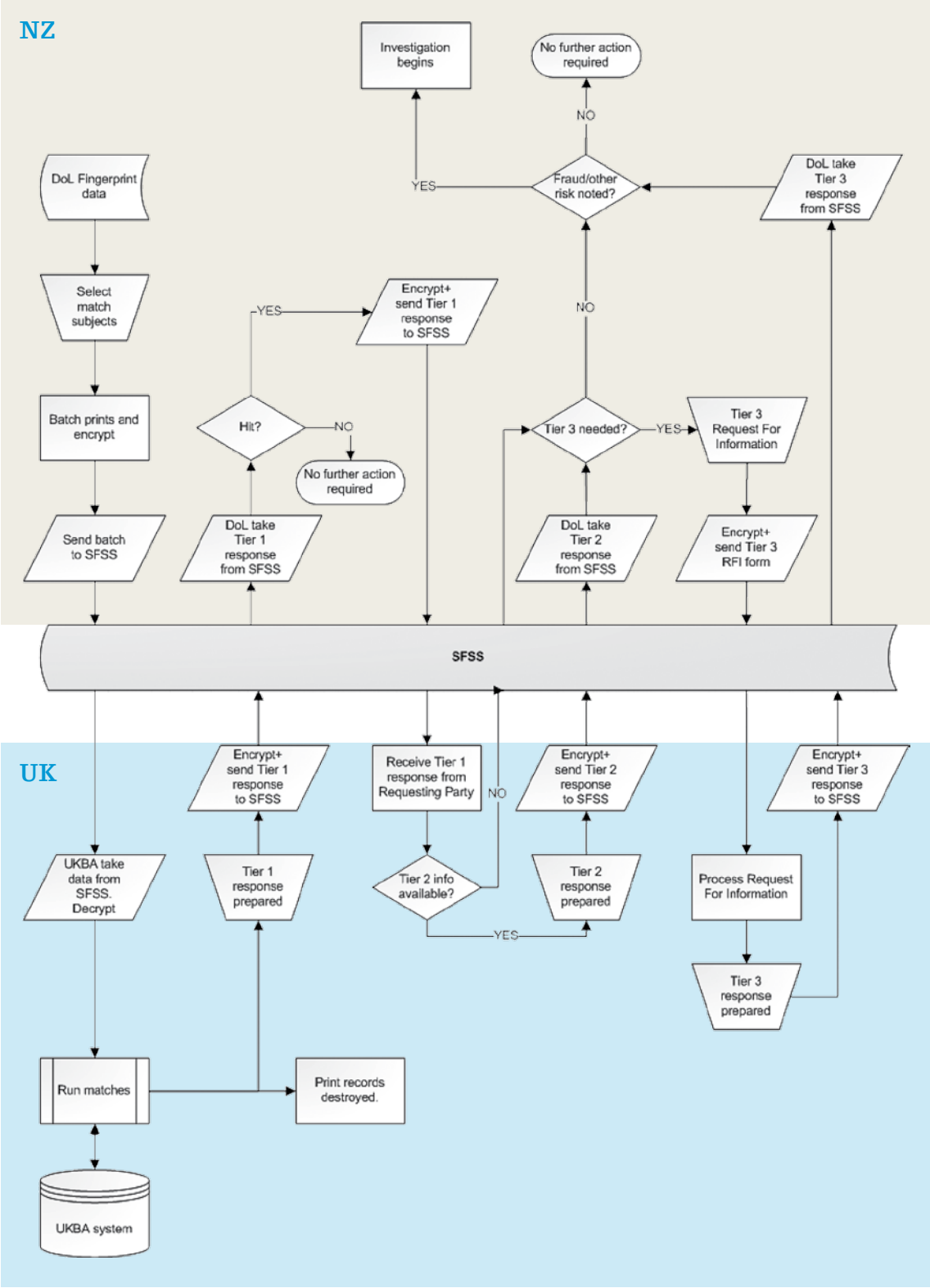
This helps to ensure that only relevant information is returned with each response.

2.2.4 The Cost of implementation

The project leverages off existing Government systems and arrangements between DoL and Police. The cost for New Zealand of implementation of the entire FCC Protocol is approximately NZ$50,000.

2.2.5 The information flows and FCC Protocol data matching & sharing process

Note: this diagram reflects a situation where New Zealand requests information and it is provided by the UK.



3. Compliance with the NZ Information Privacy Principles

3.1 Principle 1 – Purpose of collection of personal information

The information that New Zealand receives from the UK will be used exclusively for immigration and nationality purposes in both countries. From the MOU clause 1.3, those are; *"…the consideration, regulation and enforcement of whether, and on what basis, any person may enter or remain in the territory of one of the Participants."* The information is necessary in order for DoL to carry out its responsibilities under both the 1987 and 2009 Immigration Acts.

3.2 Principle 2 – Source of personal information

Neither country will be receiving the information directly from the individuals concerned. In some cases, the information they receive will not have been collected directly from the individual by the supplying agency. For example, this will be the case where the information relates to criminal activity.

DoL is authorised under both Immigration Acts to exchange information with equivalent authorities in other countries for immigration purposes by virtue of ss.141AA and 141AB of the Immigration Act 1987 and ss.305 and 306 in the Immigration Act 2009.

3.3 Principle 3 – Collection of information from subject

All applicants complete a formal application to enter or remain in New Zealand. All entrants to New Zealand complete an arrival card on entry that states that the information is being collected for immigration purposes.

The arrival card states that the information collection is mandatory, required under the Immigration Act, contact information is provided for immigration information and enquiries, and the New Zealand Customs Service (Customs) is clearly identified as the chief collection agency 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.

In the case of asylum claimants, fingerprint data may be collected by a Refugee Status Officer under ss.129 (H)(1)(e) of the Immigration Act 1987 for the purpose of ascertaining or confirming the claimant's identity or nationality and several sections of the Immigration Act 2009.

New Zealand Police (Police) may collect fingerprint data on behalf of DoL under ss.140(2) of the Immigration Act 1987 for immigration clients who are taken into custody under a Removal Order, foreign criminals who are being deported, or immigration clients, including asylum claimants, who have no appropriate documentation for immigration purposes, or who appear to hold false documents. The equivalent provision for asylum claimants in the Immigration Act 2009 is s.149(1)(e).

For individuals subject to custody under the Immigration Act 2009, the relevant provision is s.333(3) which refers to s.41 of the Corrections Act 2004 permitting the taking of fingerprints.

3.4 Principle 4 – Manner of collection of personal information

DoL's collection of information from UK is authorised by ss.141AA and 141AB of the Immigration Act 1987 and by ss.305 and 306 of the Immigration Act 2009.

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.

3.5 Principle 5 – Storage and security of personal information

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.

Only specified employees of DoL will be permitted access to the information and all access will be logged and audited. Both UK 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.

3.6 Principle 6 – Access to personal information

The Protocol requires participating countries to abide by all legal requirements within their own countries, including those relating to privacy. It also requires the UK and New Zealand to notify their partner if they discover that there are any changes to the information about an individual disclosed in this programme.

At the time of writing this document, DoL went beyond the minimum requirements of the Privacy Act by providing in its internal policies the right of access and correction to people about whom it has made a decision on an immigration matter. That right would apply to anyone subject to this exchange. 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.[8]

However, even if an apparently ineligible individual 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.

3.7 Principle 7 – Correction of personal information

As mentioned above, DoL extends the rights of access to and correction of personal information to people who would otherwise be ineligible under the New Zealand Privacy Act, where the information is collected for immigration purposes.

In addition, the Protocol requires that all countries should notify one another of any data errors discovered.

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

The Protocol and MOU both require that the agencies abide by this principle. Specifically, the Protocol requires that:

6.2.4 Personal information, should, to the maximum extent feasible, be as accurate, timely, relevant, and complete as reasonably necessary to assure the propriety of identification of individuals whose personal information is contained in the system and of actions taken under this agreement with respect to that information.

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

The Protocol and MOU both restrict retention of information exchanged under these agreements. Specifically, the MOU states:

6.14 Subject to paragraph 2.12, each Participant is expected to assess the continued relevance of the information received under this MOU to its immigration and nationality purposes, and to destroy the information securely when it is no longer relevant. In particular:

i. *Data subject case file. Personal information which is retained on an electronic or paper case file relating to the data subject, because*

8. Privacy Act Policy 2005 section A.3 http://www.dol.govt.nz/PDFs/privacyactpolicy.pdf

it has ongoing relevance to that file, may be retained as part of that file in accordance with the domestic laws and data retention policies of the Participant that has received it.

ii. *Watchlists. Personal information relating to:*

a) false identities and travel documents;

b) multiple identities used by the same person; and

c) persons engaged in derogatory activity that would render them inadmissible to the territory of the Participant that has received it may also be retained for as long as it is relevant to that Participant's border controls, up to an initial maximum of ten years from the date of receipt. As part of their ongoing review of watchlist entries, the Participants will discuss the continued relevance of the information and seek approval before ten years on information appropriate for retention for a further period.

iii. *Data held by central Protocol team. Personal information which is otherwise retained, in a central record of information received or otherwise, may be retained for no longer than two years from the date of receipt.*

Any further retention is subject to the prior written approval of the Participant that supplied the information.

3.10 Principle 10 – Limits on use of personal information

There are specific legislative provisions for these exchanges: in the Immigration Act 1987, disclosure overseas is provided for by ss.141AA and 141AB. In the Immigration Act 2009, it is covered by ss.305 and 306.

3.11 Principle 11 – Limits on disclosure of personal information

There are specific legislative provisions for these exchanges: in the Immigration Act 1987, disclosure overseas is provided for by ss.141AA and 141AB. In the Immigration Act 2009, it is covered by ss.305 and 306.

3.12 Principle 12 – Unique identifiers

The UK and New Zealand will only use their own assigned UIs within their own systems – for example client identifiers in the New Zealand Application Management System (AMS) will not be disclosed to the UK.

Special UIs will be created and assigned to identify each set of fingerprints sent or received between the participants. They will only be used for the exchanges and will not be entered into permanent client records.

Once follow-up information is required, the participants will identify the persons of interest by standard biographic data and with photographs. However, the information transferred after the match may include information about travel documents including passports which contain UIs. Those UIs will be stored and used by the participants but will not be assigned by them to the individuals for the purpose of uniquely identifying the individuals.

Both participants already have successfully functioning systems for assigning unique identifiers to clients within their systems. Assigning these additional and questionable UIs would be inappropriate and counter-productive. As some of those "secondary" UIs may be from fraudulently acquired documents, they are unsuitable for use as anything other than a piece of information about the individual.

Fingerprints received by each participant will be processed through that participant's fingerprint analysis systems and the biometrics templates created used to search for matching fingerprints within the receiving participant's records.

Fingerprint information sent under the Protocol will be destroyed after use, unless there is a match. If there is a match, the receiving participant will already hold the individual's fingerprints and the "probe" fingerprint will be kept if needed as evidence or destroyed in the normal course of business.

4. Additional Protections for the Privacy of Affected Individuals

4.1 Informing people likely to be affected

DoL is publishing a formal notification to advise of the implementation the FCC Protocol. This notification will be placed on the DoL website and other relevant communication channels.

During the initial period (from the execution of the MOU until full implementation under the Immigration Act 2009) fingerprint collection will be as authorised or required under the 1987 Immigration Act.

4.2 Security of on-line transfers of personal information

The information transfers for the matches will be through a secure file transfer system hosted by the Australian government. All transmissions will be encrypted. In the event of failure of that system, the Protocol calls for alternate secure encrypted electronic transfers. As a last resort, encrypted electronic files may be transferred physically through diplomatic channels.

The information on the SFSS is contained within a dedicated directory structure. Each bilateral MOU is assigned a separate sub-folder and only registered authorised users from the two relevant FCC participants can access each sub-folder. So, for example, only registered UK and Canadian users can access the UK-Canada folder.

4.3 Technical standards of operation

A copy of a draft Technical Standards Report (TSR) is provided with this document to provide additional background information on how the exchanges will operate.

In the interests of continued transparency of operation, any variations to that TSR before the commencement of operation of the matching programme will be reported to the Privacy Commissioner. Similarly, any changes to the TSR that are agreed to by the agencies after the commencement of the match will also be provided to the Privacy Commissioner.

4.4 Safeguards for individuals affected by the results of the exchanges

The structured and controlled release of information according to the Protocol helps to protect individuals from poorly considered actions being taken as a result of the exchange.

When a match on the fingerprints is made that meets an acceptable standard and has been verified by a fingerprint expert, the requesting agency will receive Tier 1 information. Tier 1 information includes a photo of the individual, if available. That allows the receiving country to compare the more detailed information against its own records. It should help to confirm or disprove whether the individual concerned is likely to be the same person.

DoL has a structured process for assessing information about applicants for entry to this country. It will be applied to all matches under the Protocol. The process has five stages for each type of information assessed and level three is an interview.

Included in this process is a letter outlining all potentially prejudicial information (PPI) available related to the individual's case. That letter invites client comment or explanation which may be done through an interview if appropriate. The case is re-assessed once client comment is obtained, and a final immigration decision is made. If the client is unsatisfied with the outcome, there is a well established administrative review process followed by a formal appeals process.

4.5 Destruction of biometric information

The Protocol requires participating agencies to destroy the exchanged information as soon as the exchange has been performed. This is enforced by the SFSS system, which automatically purges all bilateral folder data seven (7) days after the information has been downloaded by the Providing Country.

The Protocol also requires that the more detailed information received after a successful match should be kept for no longer than 10 years, as follows:

6.2.6 Unless otherwise agreed, the Providing Country should destroy the biometric data received from the Requesting Country straight after matching has been completed.

6.2.7 Unless otherwise agreed and in accordance with all requisite national laws of the Five Countries, returned results (see 8.3.3) should be retained by the Requesting Country for no longer than ten years, as codified in the bilateral memoranda referenced in section 7.

The MOU requires each participant to assess the continued relevance of the information received under the MOU to its immigration and nationality purposes, and to destroy the information securely when it is no longer relevant. It also requires participants to delete information if requested by the providing agency.

4.6 No new databanks or new shared databanks

No new fingerprint databank or register of individuals will be created as a result of this exchange. DoL will retain information received from the UK for as long as it takes to either confirm or deny its validity with respect to the individual whose fingerprints appear to match those in the UKBA's records. The SFSS does not act as a databank and all biometric holdings are self-purged.

If the information is found to be true of an individual in DoL's records, it will be kept according to the requirements under the Immigration Acts (1987 and/or 2009) for the determination of the individual's eligibility for entry or continued stay in New Zealand. If adverse action is required, the information will be kept for as long as the respective Act requires and at least until all appeals are exhausted.

4.7 Operation only under the provisions of the FCC High Value Data Sharing Protocol and the MOU between the UK and New Zealand

No exchanges will be undertaken until after the MOU between DoL and UKBA has been signed. New Zealand and the UK have already signed the Protocol. These two documents, in their practical effects, form the agreement to exchange information

The agencies in this bilateral agreement will not charge each other fees for stage 2 exchanges. The matter of cost sharing for stage 3 has not yet been determined.

4.8 No unreasonable delays in acting on the information received

DoL undertakes to decide if at all possible within 60 days on whether it will take adverse action against an individual and actually carry out that decision within 12 months of operating the exchange.

The time constraints agreed to in the Protocol are specific enough that DoL will have sufficient information to request the client explain the new information within specified time frames or flag that client record if DoL has lost touch with the client.

4.9 Advising individuals about possible adverse action as a result of the exchanges

DoL's standard processes for handling immigration applications of all types will apply. Those processes include informing applicants about PPI held or acquired by the DoL and inviting them to respond with an explanation, comment, or refutation. Typically, that is done through a letter and may include an interview.

4.10 Public reporting on the exchanges

DoL is willing to provide the Privacy Commissioner with an annual report on the results of the FCC Protocol. It may also make this information publically available, for example on its own website. Publication will demonstrate the actions undertaken to ensure the integrity of the border and refugee processes, and to deter potential fraud.

Abbreviations Used

AFIS	Automated Fingerprint Identification System
DoL	NZ Department of Labour
FCC	Five Country Conference
Fingerprints	A representation of fingerprint markings (normally for all ten fingers) which is stored in a specific format that can be used by the AFIS of each country
IAFS	Immigration and Asylum Fingerprint System (UK)
MOU	Memorandum of Understanding between The New Zealand Department of Labour and the United Kingdom Border Agency
PIA	Privacy Impact Assessment
PPI	Potentially Prejudicial Information
The Protocol	High Value Data Sharing Protocol of the Five Country Conference
Providing Country	The Country which receives the initial biometric match request from the Requesting Country and either matches the biometric provided against the specified database, or who provides information to the Requesting Country from the specified databases.
Responsible agencies	NZ Department of Labour & UK Border Agency
Requesting Country	The Country sending to the other Country (the 'Providing Country') either an initial biometric information match request, or request for further information following a successful biometric match
SFSS	Secure File Sharing Server (operated by Department of Immigration and Citizenship (DIAC), Australia)
UI	Unique identifier
UKBA	United Kingdom Border Agency
Watchlist	Personal information relating to: i. false identities and travel documents; ii. multiple identities used by the same person; and iii. persons engaged in derogatory activity that would render them inadmissible to the territory of the Participant that has received it.

newzealand.govt.nz

DOL 11537 NOV 10