参考資料４

アメリカ
(PIA Report)

事例）

国土安全保障省ＰＩＡ報告書

ＰＩＡガイダンス（新バージョン）を適用したＰＩＡ

Privacy Impact Assessment
for the

U.S. Secret Service Counter Surveillance Unit Reporting Database

DHS/USSS/PIA-004

July 27, 2011

Contact Point
Latita M. Payne
Privacy Officer
United States Secret Service
(202) 406-5838

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Secret Service (Secret Service or USSS) has created the Counter Surveillance Unit Reporting (CSUR) Database. CSUR assists Secret Service employees in managing, analyzing, and distributing intelligence information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The Secret Service is conducting this Privacy Impact Assessment (PIA) because CSUR contains personally identifiable information (PII) regarding subjects of protective interest to the Secret Service.

Overview

The Protective Intelligence and Assessment Division of the Secret Service manages the CSUR database. The system is used to report and store information collected by USSS Counter Surveillance Units (CSU) and Uniformed Division Officers.

The Secret Service uses CSUs to identify threats against individuals, events, and facilities protected by the Secret Service. The focus of CSU is persons who are showing undue or unusual interest in a protectee or a protected venue. The officer or agent observes, records, and reports information so pre-attack indicators can be revealed, hostile surveillance can be identified, and anomalies can be investigated. Information is gathered from observation of suspicious activity by officers or special agents who are trained to investigate, research, and follow-up on reported information in order to resolve or provide further details about the situation, subject or activity encountered. Occasionally, information in CSUR originates from an information tip from a concerned citizen. That information will only be transferred into CSUR if trained personnel vet the information and determine it is credible and necessary in the furtherance of the agency's protective mission.

The CSUR database is a central repository of information concerning Secret Service agents' and officers' observations of suspicious activity or surveillance directed against Secret Service protectees, events, or facilities. Real-time or on-the-spot feedback may be provided to the field units if deemed necessary. The Secret Service may also use the information in CSUR to investigate, research, and/or follow up on details in order to resolve or provide a clearer picture of the situation, subject, or activity encountered.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The collection of the information is authorized by the Secret Service's protective authority contained in 18 U.S.C. §§ 3056 and 3056A.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CSUR is covered by DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The certification and accreditation was completed on August 9, 2010, and expires on August 9, 2013.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, NARA has approved the records retention schedule for CSUR.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected in CSUR is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The CSUR database is a central repository of information concerning observations of suspicious activity or surveillance directed against individuals, events or facilities protected by the Secret Service. The CSUR database includes the following information, as applicable:

Incident: location, possible direction of interest (protectee, event, or facility), and a narrative description of the suspicious activity.

Individual's (if available): full name, date of birth, age, sex, nationality, race, height, weight, build, eye color, hair length, hair color, facial hair (if any), clothing, street address, e-mail address, telephone number(s), field photographs, and aliases.

Other identifiers that may be recorded in CSUR include information obtained either from the individual or from law enforcement databases such as NCIC/NLETS, including Social Security number (SSN), drivers license number, FBI number, state

criminal ID number, passport number, alien identification number, any other identifying number, and arrest record.

Vehicles: driver, registered owner, color, type, make, model, year, vehicle identification number (VIN), license plate number, the state that issued the license plate, and the year in which the license was issued or renewed.

Some records may contain an address or phone number obtained through conducting a search of commercially available public records, when such information is not otherwise obtained directly through an investigation.

2.2 What are the sources of the information and how is the information collected for the project?

Information is gathered from observation of suspicious activity by an officer of the USSS Uniformed Division officer (UND) or a special agent. UND officers at the Joint Operations Center (JOC) relay pertinent information to a UND or CSU member to conduct a follow-up field interview, consent search, or other appropriate action.

Information about suspicious activity may also be provided to the USSS by another law enforcement entity or USSS-vetted observations reported by a concerned citizen.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Some records may contain an address or phone number obtained through conducting a public record search, when such information is not otherwise obtained directly through an investigation.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the information submitted will be checked by the appropriate field unit, working with the CSUR Desk. The field units are comprised of USSS agents and officers trained to investigate, research, and follow-up on reported information in order to resolve or provide further details about the situation, subject or activity encountered.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the Secret Service could collect information about individuals who pose no threat, particularly via information from non-law enforcement concerned citizens.

Mitigation: Trained personnel vet reported information and only enter into CSUR that

information which is both credible and necessary in the furtherance of the agency's protective mission.

Privacy Risk: CSUR could over-collect PII.

Mitigation: The Secret Service collects the information necessary to enable positive identification so that; (a) the individual is identifiable during future interactions with the agency; (b) the individual is not erroneously identified as or linked to another individual; and (c) further investigation can be conducted (if necessary). Information is gathered from observation of suspicious activity or an investigation by an officer of the Secret Service UND or a CSU member. Information about suspicious activity may also be provided to the Secret Service by another law enforcement entity or concerned citizen.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information is used to support the Secret Service in accomplishing its protective mission. CSUR assists Secret Service employees in managing, analyzing, and distributing intelligence information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The officer or agent observes, records, and reports information so pre-attack indicators can be revealed, hostile surveillance can be identified, and anomalies can be investigated. Officers and agents may conduct searches of data in CSUR and communicate relevant results to Secret Service field units if deemed necessary.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The Secret Service does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

While CSUR database information will be shared with the participants in the (Nationwide Suspicious Activity Reporting Initiative (NSI) Shared Space Environment) facilitated by DHS Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) via the ISE-SAR Server, there are no other DHS components with assigned roles and responsibilities within the system. Authorized personnel may use the NSI shared space query capability to conduct searches to determine if the subject(s) or

activity has been encountered previously.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access to and inappropriate dissemination of information maintained in CSUR.

Mitigation: The Secret Service has mitigated this risk by implementing primary security standards for CSUR. These include user accountability and validity of identification, user audit logs for significant activity, system time-out after twenty minutes of inactivity, access limited to authorized individuals with a verifiable need to know, account lockout after three bad attempts, and a security warning to users that unauthorized, improper use or access to the system may result in disciplinary action, as well as civil and criminal penalties.

Additionally, trained personnel vet reported information and only enter into CSUR that information which is both credible and necessary in the furtherance of the agency's protective mission. All CSUR users complete annual agency mandated privacy and security training, which stresses the importance of appropriate and authorized use of PII in government systems.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The System of Records Notice DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008) provides notice regarding the collection of information and the routine uses associated with the collection of the information. This PIA provides similar notice to the general public as to the collection and use of information for this purpose. Advanced notice of the collection of information to investigative targets or others involved in the investigation generally is not provided as it would compromise ongoing law enforcement investigations and otherwise impede law enforcement proceedings. The final rule for the Protection Information System of Records officially exempts the system from portions of the Privacy Act.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals have no right to decline to have their information collected, stored, and maintained in this system. However, they may decline to be interviewed or refuse to provide information requested during the course of an interview.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the existence of CSUR and the data it collects and maintains.

Mitigation: This PIA and the USSS Protection Information System SORN serve as public notice of the existence of CSUR, the data it collects and maintains, and the routine uses associated with the information collected. The information is used only for the purpose for which it was provided through the public notice of this PIA.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Information that is collected that becomes part of an investigative case file will be retained for a period that corresponds to the specific case type developed (e.g., judicial, non-judicial, non-criminal).

The retention periods established and/or approved by the National Archives and Records Administration (NARA) for investigative case files may cover periods as short as two years, or as long as 30 years, depending on the type or disposition of the case.

Per USSS Records Disposition Schedule N1-87-10-4 (approved by NARA on 11/22/2010), CSUR information that has no potential historical or archival value and which does not become part of an investigative file is to be deleted "when the agency determines that it is no longer needed for administrative, legal, audit, or other operational purposes." Understanding that the time frames associated with such purposes can vary widely (e.g., a backup of the database which is overwritten on a nightly basis, versus a litigation-related preservation order which may remain in effect indefinitely), it is not practical to assign a specific retention period to this type of data. However, it should be understood that the Secret Service has no interest in preserving such information any longer than is absolutely necessary.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in CSUR will be retained for the timeframes outlined in Question 5.1 to allow the Secret Service to manage, analyze, and distribute intelligence information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The retention period is also consistent with general law enforcement system retention schedules and is appropriate given the Secret Service protective mission and the importance of the law enforcement data to accomplish

this mission.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CSUR database information that meet the DHS Information Sharing Environment (ISE) SAR Functional Standard, as outlined in the DHS ISE SAR PIA,[1] will be shared with the participants in the Suspicious Reporting Initiative via the ISE-SAR Server. USSS will enter ISE SAR data by manually. Personnel may use the NSI query capability to conduct searches to determine if the subject(s) or activity has been encountered previously. Also, PII and/or summary investigative information maintained in CSUR may be shared with law enforcement and/or other federal, state, local government agencies who have a need-to-know.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any information maintained in CSUR may be shared in accordance with the purposes and routine uses specified in the Secret Service's System of Records Notice DHS/USSS-04 (Protection Information System, 73 FR 77733) in support of the Secret Service protective mission.

6.3 Does the project place limitations on re-dissemination?

Currently any information maintained in CSUR that is shared with outside law enforcement organizations, and/or other federal, state, local government agencies that have a verified need-to-know is provided via telephone call. Security warnings and disclaimers requiring that the information be kept in law enforcement channels are orally reinforced during the telephone call.

---

[1] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative* (Nov. 17, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise.pdf.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

When CSUR information is shared with outside law enforcement organizations, and/or other federal, state, local government agencies, an entry is made in the CSUR database record to reflect that the information was shared and with whom it was shared. Information originating from CSUR that is uploaded into ISE SAR may be shared outside of the Department, and records of those disclosures would be maintained by ISE SAR and not CSUR as described in the DHS ISE SAR PIA.[2]

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The privacy risks associated with this external sharing relates to the unauthorized access to and disclosure of the information maintained in CSUR.

Mitigation: The sharing of information described above is in accordance with appropriate routine uses and legally mandated sharing and will be shared only upon verification of need-to-know and in conjunction with adequate warnings regarding improper re-dissemination.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

As a protection information system owned by the Secret Service, DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008) permits CSUR to be excluded from the access and redress provisions of the Privacy Act in order to prevent harm to law enforcement investigations or interests. However, access requests will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA Officer, Communications Center (FOI/PA), 245 Murray Lane, Building T-5, Washington, D. C. 20223, as specified in the Protection Information System SORN.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures are the same as those outlined in Section 7.1.

[2] *Ibid.*

7.3 How does the project notify individuals about the procedures for correcting their information?

The mechanism for requesting correction of information is specified in the DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008), in this PIA, and on the Secret Service's public webpage.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that that an individual may have limited access or ability to correct their information.

Mitigation: Individuals can request access to information about them under the FOIA and Privacy Act and may also request that their information be corrected. The nature of CSUR and the information it collects and maintains is such that the ability of individuals to access or correct their information may be limited by Privacy Act exemptions. The redress and access measures offered are appropriate given the purpose of the system which is to collect, analyze, and store information concerning individuals who may pose a threat to Secret Service protectees, protected facilities, and protected events.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All Secret Service information systems are audited regularly to ensure appropriate use of and access to information. Specifically related to this system, application access is mediated through a two-tier identification and authentication process. Any changes to the hardware or software configuration are subject to review and approval by the USSS Configuration Control Board process to ensure integrity of the application.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Secret Service employees are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors additional guidance.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

DHS physical and information security policies dictate who may access Secret Service computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USSS has agreed to contribute CSUR data to the DHS ISE-SAR Server.

Responsible Officials

Richard K. Elias, Assistant Director,
Office of Operational Intelligence and Information
U.S. Secret Service, Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

ＰＩＡガイダンス（旧バージョン）
を適用したＰＩＡ

Privacy Impact Assessment
for the

Immigration Benefits Background Check Systems

November 5, 2010

Contact Point
Donald Hawkins
USCIS Privacy Officer
United States Citizenship and Immigration Services
202-272-8000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
703-235-0780

Abstract

As part of its benefits adjudication process and as required by law, the United States Citizenship and Immigration Services (USCIS) conducts background checks on petitioners and applicants who seek certain immigration benefits. These background checks consist of four separate checks against systems within Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS). In order to facilitate the collection and transmission of information necessary to complete background check processes, USCIS maintains five information technology electronic systems: the Fingerprint Masthead Notification System (FMNS), the Customer Identity Capture System (CICS), the FD-258 Tracking System - Mainframe (FD-258 MF), the Benefits Biometrics Support System (BBSS), and the Interagency Border Inspection System (IBIS) Manifest. USCIS is conducting this privacy impact assessment (PIA) because FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest collect, use, and share personally identifiable information (PII). This PIA replaces the previously published USCIS PIA for the "Background Check Service (BCS)" which describes planned background check-related systems that were never implemented. Upon publication of this PIA, the BCS PIA will be retired.

Introduction

Title 8 U.S.C. § 1101 et seq. requires background checks to be conducted for certain immigration benefits. The background check process is triggered as soon as the petitioner or applicant (hereafter collectively referred to as "applicants") applies for a benefit. In adjudicating applications for benefits, USCIS conducts four different background checks, two biometric fingerprint-based and two biographic name-based.

After an applicant submits a USCIS application for which a background check is required, USCIS contacts the applicant by mail with an appointment time to have his biometrics taken at a specified USCIS Application Support Center (ASC).[1] At the ASC, USCIS electronically captures the applicant's fingerprints (hereafter referred to as "the 10-prints") and related biographic data.

This PIA replaces the previously published USCIS PIA for the BCS describing planned background check-related systems that were never implemented. USCIS continues to operate five information technology systems in collecting biometrics and processing the background checks: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.[2] USCIS is developing a single system to streamline the

[1] USCIS implemented additional processes in response to the Kendall Frederick Citizenship Assistance Act. Public Law 110-251. The process allows USCIS to accept fingerprints previously submitted by military citizenship applicants at the time of their enlistment or from prior submissions to DHS. The Act applies to only those individuals applying for naturalization within 24 months of military enlistment. This expedites the processing of military applicants applying for citizenship.

[2] Systems used to support case management and application adjudication are covered in separate PIAs available at www.dhs.gov/privacy, most notably the September 5, 2008 *USCIS Benefits Processing of Applicants other than Petitioners for Naturalization, Refugee Status, and Asylum (CLAIMS 3)* and *USCIS Computer Linked Application Information Management System (CLAIMS 4)*.

process and to limit the privacy risks associated with using multiple systems. USCIS will issue a new PIA once the technology has been developed.

Background Check Processes

USCIS uses background check results to assist in determining an applicant's eligibility for a benefit. If the background check result from the FBI or DHS yields an item of law enforcement or national security interest, USCIS may work with DHS Customs and Border Patrol (CBP), the FBI, or other law enforcement entities, such as Immigration and Customs Enforcement (ICE), to determine whether law enforcement actions should be pursued.

The four background checks are:

- two biometric fingerprint-based:
    1. the FBI Fingerprint Check;
    2. the US-VISIT's Automated Biometric Identification System (IDENT) Fingerprint Check;
- two biographic name-based:
    3. the FBI Name Check; and
    4. TECS Name Check.

Five IT systems support the background check processes identified above: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.

1. FBI Fingerprint Check

The FBI Fingerprint Check is conducted on applicants over the age of 14 when the benefit allows them to remain in the United States beyond one year. The FBI Fingerprint Check is a search of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) to identify applicants who have an arrest record. IAFIS[3] is a national fingerprint and criminal history system maintained by the FBI's Criminal Justice Information Services (CJIS) Division. The applicant's fingerprints are processed by the FBI pursuant to an Interconnection Security Agreement (ISA) between the FBI and USCIS.

The FBI electronically sends responses to USCIS indicating whether there is a criminal history response. If there is a criminal history record, FBI also sends the FBI Record of Arrests and Prosecutions[4] (commonly referred to as the "RAP Sheet") to USCIS electronically. The RAP Sheet is stored in BBSS. A hard copy of the RAP Sheet is also sent to the respective service center and is stored

[3] For FBI's related privacy documentation, see the IAFIS and DOJ/FBI Interim Data Sharing Model PIAs at http://foia.fbi.gov/iafis.htm, and http://foia.fbi.gov/idsm.htm, respectively and corresponding SORN for the FBI Fingerprint Identification Records System (FIRS)(JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410 and associated blanket routine uses at 66 FR 33558 and 70 FR 7513-02) which can be found at http://foia.fbi.gov/firs552.htm.

[4] The RAP Sheet is a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, includes information taken from fingerprints submitted in connection with federal employment, naturalization, or military service.

in the applicant's Alien file (A-File).[5] The RAP Sheet includes the name of the agency or institution that submitted the fingerprints to the FBI, the date of arrest and the date the individual's fingerprints were received by the agency submitting the fingerprints, the arrest charge, and the disposition of the arrest if known by the FBI. All arrest data included in a RAP Sheet are obtained from fingerprint submissions, disposition reports, and other reports submitted by agencies having criminal justice responsibilities.

2. IDENT Fingerprint Check

The IDENT fingerprint check is conducted on applicants over the age of 14 when the benefit allows them to remain in the United States beyond one year. IDENT is the official DHS-wide system for the biometric identification and verification of individuals encountered in DHS mission-related processes. The 10-prints are enrolled and stored to check for matches. If there is derogatory information, that information is emailed to USCIS via an encrypted spreadsheet. The spreadsheets, emailed on a weekly basis, may contain information on more than one applicant. IDENT results may include known suspected terrorists and other national security and/or public safety concerns. IDENT search results are stored in IDENT and not stored in BBSS.

3. FBI Name Check

The FBI Name Check is conducted on applicants over the age of 14. The FBI Name Check is a name-based search of the FBI's Central Records System (CRS) and Universal Index (UNI).[6] The CRS encompasses the centralized records of FBI Headquarters, FBI field offices, and Legal Attaché offices. The CRS contains FBI investigative, administrative, criminal, personnel, and other files compiled for law enforcement and national security purposes. The UNI consists of administrative, applicant, criminal, personnel, and other law enforcement files. USCIS sends applicant information (name, date of birth (DOB), country of birth, race, and gender) to the FBI in order to conduct the name check. The secure data exchange between USCIS and the FBI for the purpose of FBI Name Check occurs via zipped and encrypted email.

The UNI is searched for "main files," files where the name of an individual is the subject of an FBI investigation, and for "reference files." Reference files are files where the name being searched is merely mentioned (not as the main subject) in an investigation.

The FBI will respond to the FBI Name Check with either a: "no record," "positive response," or "pending." A no record response means that the FBI has no relevant information based on the name and DOB of the applicant. A pending response means further research is needed before the FBI can provide a final response. For those records with an initial response of pending, the FBI will complete a review of their records and provide a final response of no record or positive response. A positive response means the FBI has information relating to the name submitted. The FBI sends the actual information in a Letterhead Memorandum relating to the positive response separately via encrypted email or over the classified network. The memoranda are stored in the A-File and if the memoranda are classified, then the A-File becomes classified. Records for refugees are stored in FD-258 MF.

[5] DHS/USCIS-001 Alien File (A-File) and Central Index System (CIS) System of Records Notice (72 FR 1755).

[6] DOJ/FBI Central Records System (66 FR 29994)

4. TECS Name Check

The TECS Name Check is conducted on all applicants over 14 years of age. The TECS [7] Name Check query consists of a name-based search of a multi-agency database containing information from 26 different federal agencies. The information in TECS includes records of known and suspected terrorists, sex offenders, people who are public safety risks and other individuals that may be of interest (e.g., individuals who have warrants issued against them, people involved in illegal gang activity, etc.) to the law enforcement community. If there are positive results from the TECS Name Check, the results are stored in IBIS Manifest and may be placed in the A-File.

USCIS Background Check IT Systems

There are five IT systems that support the background check process outlined above: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.

1. FMNS

FMNS is a stand-alone system that runs on a computer desktop at the ASCs. The data in FMNS is automatically deleted 60 days after it is captured. FMNS is only used when the electronic systems for capturing fingerprints, commonly referred to as the livescan device, are not functioning, when the ASC is extremely busy, or if the livescan device is not suitable for capturing fingerprints for example, because of accessibility for accessibility reasons. In these instances a hard copy of fingerprints needs to be printed and submitted. When this occurs, the 10-prints and biographic data are collected on the paper-based FD-258 card. The biographic data is entered into FMNS and printed on the FD-258 card. These cards are mailed to the service centers. The completed FD-258 cards are then scanned and uploaded into BBSS and the electronic fingerprint transmission specification (EFTS) record is forwarded to the FBI where the 10-print criminal background check is conducted.

FMNS maintains FD-258 masthead data, applicant's name, address, DOB, Social Security number (SSN) (if available), Alien Number (A-Number), country of birth, country of citizenship, current address, aliases, gender, race, height, weight, eye color, and hair color. FMNS creates a manifest of FD-258 cards printed and generates letters to notify applicants of the time and place where they need to appear to provide fingerprints.

2. CICS

The CICS application resides on USCIS configured laptops that have a fingerprint scanner and camera. CICS is used to capture biographic, biometric and photo image information in refugee camps and in USCIS overseas offices from applicants seeking immigration benefits from USCIS. CICS transmits applicant data into the BBSS.

3. FD-258 MF

The FD-258 MF record contains biographic data, fingerprint transmission data, and fingerprint response data. This record is stored to assist in the adjudication process. If there is a RAP Sheet, it is not sent to FD-258 MF. As noted above, the RAP Sheet is sent separately and stored in the paper A-File.

[7] DHS/CBP-011 U.S. Customs and Border Protection TECS (73 FR 77778).

4. BBSS

In 1999, USCIS developed BBSS[8] to process fingerprints taken electronically at the ASC and transmits them to the appropriate USCIS SC for processing. BBSS receives fingerprints taken at the ASCs or at refugee camps and USCIS oversees office through CICS and forwards them to one of four USCIS service center where the 10-print records are encrypted and electronically transmitted to the FBI for the FBI Fingerprint Check.

BBSS also facilitates the transfer of biometric and biographic data pursuant to the United Kingdom (UK) Visa Program, which is covered by a separate PIA.[9]

BBSS maintains information on the FBI Fingerprint Check.

5. IBIS Manifest

USCIS developed IBIS Manifest to conduct TECS Name Checks against TECS. The results of the name check search are stored in IBIS Manifest for adjudication purposes. USCIS adjudicators have access to the results in this system to determine an applicant's eligibility for the immigration benefits being sought.

To initiate a name check, adjudicators either wand-in or manually enter the applicant's receipt number into IBIS Manifest. IBIS Manifest uses the receipt number to retrieve the applicant's full name, DOB, A-Number, and benefit form-type from the Citizenship and Immigration Service Centralized Oracle Repository (CISCOR) either via a user interface or through a batch submission process. The applicant's data is then electronically transmitted to TECS to perform a background check. The investigation yields results of either "hit" or "no hit" based on the applicant's full name and DOB. The name check results are received by and stored in IBIS Manifest. A history action code is placed in Computer-Linked Application Information Management System (CLAIMS 3) if there is no derogatory information. If derogatory information is returned, the "hit" result is all that is stored in CLAIMS 3. The adjudicator must log into TECS to view the derogatory information.

Results of Background Checks

Depending upon the nature of the benefit requested, the indicator response will be maintained in the following benefit case management systems:

- CLAIMS 4, for naturalization applications;
- Refugees, Asylum, and Parole System (RAPS), for asylum applications, and
- Marriage Fraud Assurance System (MFAS) for the TECS Name Check.
- Paper copies may also be maintained in the A-File.

[8] In 2000, a new website was added that provides users with the ability to query and view records stored in BBSS.

[9] DHS/UK Visa Project, November 14, 2007 found at:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_ukvisa.pdf

These systems maintain an indication that the background checks have been run for the relevant benefit being requested.

Results of Background checks are maintained as follows:

1. FBI Fingerprint Checks – BBSS maintains copies of the responses to the FBI Fingerprint Check and the FBI RAP Sheets. In certain instances, the RAP Sheets will also be placed in the A-File.
2. IDENT Fingerprint Checks – IDENT maintains the results.
3. FBI Name Check – The no records, pending, or positive response codes are stored. Positive responses are sent to the National Benefits Center (NBC) on Letterhead Memoranda in encrypted format and printed and placed in the A-File. If the response is a national security or public safety issue, the response is maintained in Fraud Detection National Security-Database System.
4. TECS Name Check – This check is stored in IBIS Manifest and may be placed in the A-File. Also, a history action code is placed in CLAIMS 3 if there is no derogatory information.

This PIA covers the IT systems that support the fingerprint process from collection at the ASC or through CICS to completion, when results are received. In order to understand the entire process of background checks, the introduction in this PIA is necessarily more comprehensive. The remainder of this PIA will concentrate only on the five IT systems: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.

Section 1.0 Information collected and maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is collected?

The information collected and stored in FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest includes biographic and biometric data provided by applicants at the ASC (or scanned from FD-258 cards in certain situations), refugee camps and oversees or from the application or petition submitted when seeking a USCIS benefit.

An applicant's 10-prints, photo, signature and an index finger press-print are collected at the USCIS ASCs using livescan machines that interface with BBSS or at refugee camps and oversees using CICS , which is a mobile laptop unit. The 10-prints are stored in IDENT and at the FBI.

FMNS

FMNS collects and temporarily stores the following information for 60 days: applicant's name (first, last and middle), address, reason fingerprinted, DOB, aliases, A-Number, reason for fingerprint, SSN, country of birth, country of citizenship, gender, race, weight, height, eye color, and hair color.

CICS

CICS collects and temporarily stores A-Number, SSN, name, DOB, country of birth, country of citizenship, sex, race, height, weight, eye color, hair color, alias, residence address, city, state, and zip code of person fingerprinted, Originating Agency Identification (ORI) Code, SC ORI Code, destination SC ORI Code, reason fingerprinted, site code, Z-number, a single photograph image, and a full set of 10-print fingerprint images.

FD-258 MF

The data stored in FD-258 MF includes:

Biographic Data: applicant's name (last, first, middle), SSN (if the applicant provides it, as SSNs are not required), two additional SSN fields for applicants who provide more than one (in the case of an applicant fraudulently or accidentally using more than one SSN), street address, city, state, ZIP code, up to five aliases, country of citizenship, DOB, two additional DOBs, sex, race, height, weight, eye color, hair color, country of birth, A-Number.

Fingerprint Data: Transaction Control Number (TCN), fingerprint service requested (criminal background check), date fingerprints were sent to the FBI, miscellaneous number (e.g., Z Number[10]), date/time fingerprints were taken, reason fingerprinted (represented by USCIS form type), ASC site code, ASC machine ID, ASC employee ID, ORI code (i.e., District Office (DO) ORI, SC ORI code), and external system ID (e.g., A-Number for CLAIMS 4, receipt number for CLAIMS 3).

Fingerprint Result Data: TCR, FBI response, date processed by the FBI, date processed by the SC, date processed by FD-258 MF, and FBI Number (number assigned to a record with a RAP Sheet).

While all of the data mentioned above is stored in the FD-258 MF database, only the following information is displayed for the user to view: A-Number, name, service center ORI, DOB, TCN, TCR, country of birth, FBI response, date processed by the FBI, date processed by the service center, date processed by FD-258 MF, and FBI Number.

BBSS

Records in BBSS related to the FBI Fingerprint Check include the following information:

Biographic Data: name (last, first, middle), may include SSN, two additional SSNs in the event that the applicant is using multiple SSNs either fraudulently or accidentally) street address, city, state, ZIP Code, up to five aliases, country of citizenship, DOB, two additional DOBs, sex, race, height, weight, eye color, hair color, place of birth, and A-Number.

Fingerprint Data: TCN - a unique number generated by the live scan device, fingerprint service requested (criminal background check), date fingerprints were sent to the FBI, miscellaneous number (e.g., Z Number), date/time fingerprints were taken, external system ID (e.g., CLAIMS 3, and CLAIMS 4), external system ID, reason fingerprinted (represented by form type), ASC site code, ASC machine ID, ASC employee ID, Local ORI code (i.e., DO ORI), service center ORI code).

[10] A Z Number is a temporary ID number used when no other identifying number is provided.

Fingerprint Result Data: TCR - a unique number assigned to each transaction by the FBI, and the RAP Sheet (where one exists). If there is no match in IAFIS, the FBI's response is "NON-IDENT" which is stored in BBSS and FD-258 MF. If a criminal history record does not exist, the FBI provides USCIS a response (NON-IDENT) indicating that there was not a match on the fingerprints submitted.

The image sets (press-print, photo and signature) captured at the ASCs are transferred through BBSS for use in card production. Images related to cards that have been produced are stored in the Image Storage and Retrieval System (ISRS) which will retire at the end of the fiscal year and be replaced by Customer Profile Management System (CPMS) but the information is not stored in BBSS. [11] This information that passes through BBSS includes the receipt number and the image set.

IBIS Manifest

IBIS Manifest collects and stores the following information: full name (first, middle, and last), aliases, DOB, A-Number, receipt number, benefit form type, and TECS Name Check results ("HIT" or "NO HIT").

1.2 From whom is information collected?

The biometric information provided by the applicant for the FBI Fingerprint Check and the IDENT Fingerprint Check is taken from the livescan application at the ASC. The biographic information is collected from the applicant at the time the fingerprints are taken. Fingerprints are taken at one of USCIS' ASC and sent electronically to one of the USCIS service centers. If the applicant is unable to have their fingerprints taken by one of the electronic livescan fingerprint capture devices, a hard copy fingerprint card (FD-258 card) is used to capture the fingerprints and that hard copy is mailed to one of the service centers. The hard copy FD-258 is scanned into an electronic format at the service center. All fingerprints are encrypted and sent to the FBI electronically. The responses to the FBI Fingerprint Check are encrypted and sent back to USCIS electronically from the FBI and the results are stored in FD-258 MF. The biographic information used for the FBI Name Check and the TECS Name Check is taken from the application/petition submitted by the petitioner or an authorized representative.

In addition, CICS captures biographic, biometric, and photo image information primarily of refugees and beneficiaries of I-730 petitions (V92/93) who are considered for refugee status in the United States in accordance with U.S. Law and international mandates; and also for applicants, petitioners, and beneficiaries applying in USCIS overseas offices for USCIS benefits including eligibility for certain types of non-immigrant and immigrant visas, naturalization, travel documents, waivers, and parole.

The biographic information from the application/petition is entered into one of USCIS' case management systems. The USCIS case management systems include:

- CLAIMS 3, which is used to process applications for benefits other than naturalization, refugee, and asylee status;

[11] For a detailed discussion of ISRS and ICPS, please see *Privacy Impact Assessment for the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum* (September 5, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.

- CLAIMS 4, which is used to process applications for naturalization;
- CISCOR, which is used to consolidate and maintain an exact replica of CLAIMS 3 data;
- RAPS, which is used to process Asylum applications; and
- MFAS, which is used for processing information relating to investigations of marriage fraud.

1.3 Why is the information being collected?

The collection of information is required to conduct the background check required by 8 U.S.C. § 1101 *et seq.* and to produce USCIS issued documents for applicants who have been approved for the respective benefit. The background checks are conducted to determine if information is available from FBI IAFIS, US-VISIT IDENT, FBI Name Check or TECS Name Check that would make the applicant ineligible for the benefit sought. USCIS cannot grant certain benefits unless it collects the information necessary to meet this statutory requirement.

The image set (press-print, photo, and signature) is collected and is put on the UCSIS issued documents including the Permanent Resident Card (PRC), Employment Authorization Document (EAD), Re-Entry Permit (REP), and Refugee Travel Document (RTD).

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The legal authority to collect this information is derived from 8 U.S.C. § 1101 *et seq.* (Aliens and Nationality).

In addition, the U.S. Office of Management and Budget (OMB) approves the format of every public form utilized by USCIS to collect the information in conjunction with requested immigration benefits through the Paperwork Reduction Act process.

USCIS has signed an ISA and MOU with the FBI that set forth the terms and conditions for the transfer and use of information pertaining to background checks and associated with the interaction with BBSS, FMNS and FD-258 MF (via BBSS). USCIS has an MOU with US-VISIT covering the biometric and biographic information sharing. *MOU between U.S. Citizenship and Immigration Service Department of Homeland Security and US VISIT U.S. Department of Homeland Security and Bureau of Customs and Border Protection U.S. Department of Homeland Security for the Purpose of Sharing Relevant Biometric and Biographic Data (Travel Document and Ten-Print Fingerprint Data for the US VISIT Increment 2A Program, December 16, 2005).*

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Privacy Risk: The overarching risks presented by the current USCIS background check processes and systems stems from the very complex and outdated technology used. The main risk is that the technologies will fail.

Mitigation: These risks will not be fully mitigated until USCIS is able to replace these older mainframe systems with an appropriately up-to-date Information Technology (IT) solution. USCIS is in the first year of a five year comprehensive transformation initiative that includes replacing the existing systems with a technical solution that incorporates the latest data security practices. In the interim, USCIS employs standard operating procedures to keep records of background check responses, such as printing responses in hardcopy to be filed in the applicant's permanent A-File record.

Privacy Risk: Misuse and inappropriate dissemination of data.

Mitigation: USCIS has implemented measures to mitigate these risks in the design of FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest by limiting access to these systems to authorized personnel who need this information to make an adjudication decision.

USCIS developed and implemented FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest in accordance with DHS approved security guidelines. Only users who need the information to effectively perform their job functions are granted access to FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest. These authorized users must go through an approval process and can only access FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest through DHS approved equipment. All USCIS adjudicators who use FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest during the adjudication process are required to take the annual security awareness and Privacy Act training.

Privacy Risk: Inherent in the use of multiple systems for background check processing is the unnecessary duplication of data and the risks to control data when it exists in so many instances.

Mitigation: USCIS recognizes this risk and is developing a centralized system for storing and managing all biometrics and background check activity. This new system is part of the broader "Transformation Initiative" mentioned above.

Privacy Risk: Lack of transparency.

Mitigation: Transparency into the background check process is difficult to provide because of the complexity of the processes. By publishing this PIA and subsequent updates, USCIS is attempting to mitigate this by setting out the processes in a clear manner. Additionally, the development and deployment of the centralized system will streamline the process and thus improve transparency of the processes.

Privacy Risk: There is also a risk that the CICS mobile fingerprint units may be lost or stolen.

Mitigation: USCIS has followed DHS and OMB guidelines for encrypting all CICS mobile devices to ensure the data cannot be compromised.

Privacy Risk: Adding the biometrics to the incorrect applicant file.

Mitigation: The information collected is attributed to the correct applicant file by matching fields such as A-Number Integrity checks are conducted at all points of data transfer and matching.

Section 2.0 Uses of the system and the information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The biographical and biometric information collected at USCIS ASCs, refugee camps, and overseas offices and stored in and disseminated by FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest is used to complete the background checks required by USCIS. The results of the background checks are used to determine an applicant's eligibility for a USCIS benefit. If the background checks result from the FBI yields an item of law enforcement or national security interest, USCIS may work with CBP, the FBI, or other law enforcement entities, such as ICE, to determine if law enforcement actions should be pursued.

Additionally, the information in these systems may be used for future law enforcement action if that information, viewed in conjunction with other information not currently known, indicates that a crime may have been committed. If the applicant becomes the subject of a national security or law enforcement investigation, the information in these systems could be provided to law enforcement and the courts in the interest of public safety.

The information processed through BBSS is also used for card production.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest are not used to analyze data in order to assist users in identifying previously unknown areas of note, concern, or pattern.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The information collected from applicants and entered into BBSS (via an electronic interface) and FMNS (via a manual process) is checked for accuracy. BBSS and FMNS have various validation tables, which are used to ensure the information and proper formatting prior to the transmission to the FBI. Data integrity checks are also performed to verify that the system is uploading the correct data. These checks match the A-Number, receipt number, first and last names, DOB, and other biographical information. If incorrect information is used to conduct a background check that results in the return of derogatory information for someone other than the applicant, the applicant has an opportunity during the adjudication

process to provide correct information and have the corrected information submitted to the agency conducting the check (e.g., FBI, US-VISIT/IDENT) for a new search.

In most cases, the refugee applicants in refugee camps have no identification documents when they are initially processed into CICS but if documentation such as a passport is available, then that is used to establish identity. Accuracy of biographic information is dependent on information provided by the refugee applicant. The USCIS Refugee Corps Officer types in the applicant's biographical information, takes a photo, and processes the fingerprints into the CICS application. CICS validates all demographic data to ensure that the data is compliant with the EFTS format defined by BBSS prior to sending a submission. The Refugee Asylum and International Operations (RAIO) Officers who review these documents have received training in fraud detection. Additionally, Fraud Detection Officers are assigned to most of the overseas offices.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Privacy Risk: Misuse of data.

Mitigation: FBI fingerprints and biometrics request and response records are attributed to the correct applicant file by matching fields such as A-Number, name, and DOB. Fingerprints themselves are biometrically verifiable. When a benefit is denied, the adjudicator must site the reason and section of law under which the denial was based. The applicant has the opportunity to appeal this decision. USCIS has standard operating procedures in place to instruct adjudicators on the review of RAP Sheets and how to conduct TECS Enforcement reviews. If a report is placed in the wrong file, the adjudicator may correct the misplacement and the applicant has the opportunity to correct during the interview.

Integrity checks are conducted at all points of data transfer and matching. All FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest information resides on and is connected to a secured network and servers with access limited to authorized personnel only. Audit logs are retained to track and identify unauthorized uses of system information. Information including the user's identity accessing the systems, time/date of access, and the events that occurred, sources of these events, and the outcomes of these events. If misuse of data is suspected, these logs can be used to review and analyze all activity in system. The misuse of data could be detected by reporting from employee and/or system monitoring. All FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest users are notified that these logs are stored and that USCIS management can use these to review any and all activity related to system usage.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

FMNS

Data in FMNS is only retained for 60 days.

CICS

No information is stored in CICS. The information is collected and transferred to BBSS or an encrypted portable storage device if network access is not available.

FD-258 MF

The biographic data and FBI response data contained in FD-258 MF is retained for 75 years pending National Archives and Records Administration (NARA) approval.[12]

BBSS

The biographic data and FBI response data, including RAP Sheets are retained indefinitely in BBSS per the requirements of the USCIS Office of Financial Operations (OFO) as approved by NARA.

IBIS Manifest

The biographic data and name check results are retained for 180 days. The results of the TECS Name Check are also placed in the A-File.

Paper Records Associated With Background Check Processes

The paper version of the RAP Sheet and TECS Name Check is maintained in the applicant's A-File for 100 years from DOB. The files are then turned over to NARA for permanent retention.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Retention schedules for FMNS [N1-566-08-2], FD-258 MF [N1-85-00-1], and BBSS [N1-566-08-3] have been approved by NARA. A retention schedule for IBIS Manifest is being drafted and will be submitted to NARA for approval.

[12] The current record published in the Federal Register states that the data in FD-258 is deleted 10 years after the last action. This retention timeframe is incorrect and an updated retention schedule is being submitted to the National Archives & Records Administration (NARA) and will be published in the Federal Register.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Privacy Risk: Keeping data longer than necessary would violate the Fair Information Practice that requires the retention of the minimum amount of information necessary to perform relevant governmental functions.

Mitigation: The information is needed for the indicated time period because the relationship between an applicant and USCIS may span the time period that the data is retained. USCIS will use the historical data in the systems for the adjudication of applications/petitions in the future. All data and electronic images are being retained for the indicated periods to fulfill the business requirements of DHS and in accordance to the limits of the retention schedules, which includes adjudication of decisions, law enforcement uses, protection of national security, responding to requests within DHS, as well as those requests from other government agencies requiring historical and/or biographical information on the individuals of interest. USCIS recognizes the indefinite retention of BBSS files is not consistent with retaining records for only as long as needed for agency business and as a result, once the new system which will consolidate the information goes live, the retention periods will change to 100 years from the DOB.

The ability to forge identities is a growing concern and keeping this biographic data on record for lengthy periods of time can help protect against fraudulent benefit applications. USCIS has implemented several measures to combat identity fraud and storing all background check data for future use supports this initiative.

Section 4.0 Internal sharing and disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

FD-258 MF shares information internally with CLAIMS 4, RAPS, and CLAIMS 3.

BBSS shares information internally with the US-VISIT program's IDENT system through the interface for fingerprint/biometrics image purposes. BBSS also sends information to the FD-258 MF via FD-258 EE.

IBIS Manifest conducts queries against the CBP TECS system. A history action code is placed in CLAIMS 3 if there is no derogatory information.

In addition, USCIS may share background check information within DHS where background responses yield information that may indicate a violation of immigration, criminal, or terrorism-related laws. Specifically, USCIS may share with CBP, ICE, and Office of Intelligence & Analysis.

4.2 For each organization, what information is shared and for what purpose?

FMNS does not share data directly. The biographic information entered into FMNS is printed on the FD-258 card. The applicant's 10-prints are captured on that same card. The FD-258 cards are sent to one of the service centers where they are scanned into BBSS. An EFTS record is created and electronically sent to the FBI for the 10-print criminal background check.

FD-258 MF shares information internally with CLAIMS 4, RAPS, and CLAIMS 3 to facilitate the adjudication of immigration benefits.

After BBSS captures the 10-Prints, they are transmitted to IDENT with associated biographic information to match against the IDENT database. This search is required in order to complete the IDENT fingerprint background check. US-VISIT uses the information to enroll the applicant into IDENT so biometric identification and verification can be performed in future encounters.

IDENT stores all biometric and biographic data transmitted from BBSS. US-VISIT also shares this information with CBP and other DHS components if US-VISIT determines that the receiving component has a need to know to carry out national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

TECS Name Check requests and responses are shared electronically between IBIS Manifest and the TECS Name Check system. IBIS Manifest electronically sends the applicant's first and last name, DOB, gender, and unique subject ID (either receipt number or A-Number) to initiate a name check request. CBP uses this information to conduct a name check against the TECS Name Check system, and sends the results back to IBIS Manifest. A history action code is placed in CLAIMS 3 if there is no derogatory information. If a TECS Name Check result contains items of law enforcement interest and national security concerns, USCIS may provide the information to other law enforcement entities such as ICE to determine if further law enforcement activities should be pursued.

4.3 How is the information transmitted or disclosed?

FBI fingerprint/biometrics images are sent electronically to US-VISIT in an unencrypted format within the DHS firewall. Transactions between BBSS and the FBI are conducted using the required EFTS format through a secure and reliable electronic interface. All transmissions to and from the FBI are encrypted.

Paper-based transmissions of RAP Sheets from the FBI are sent to USCIS via secure DOJ mail carrier.

TECS Name Check requests and responses are sent electronically between IBIS Manifest and TECS Name Check system.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Privacy Risk: Unauthorized access.

Mitigation: Internal sharing of data is conducted over secured networks controlled by DHS utilizing DHS approved computers, services, and software. The privacy risks associated with each step of internal sharing, including system and network security, data usage, data transmission, and disclosure have been identified and mitigated through adherence to DHS policies and procedures such as Information Technology Lifecycle Management (ITLM) that includes System Design Life Cycle (SDLC) documentation and Certification and Accreditation (C&A) documentation. In addition, only authorized users who need the information collected and contained in FMNS, CICS, FD-258 MF, BBSS, or IBIS Manifest have access to the system.

Privacy Risk: Misuse of data.

Mitigation: Given the technical security aspects above, there will always be the possibility of misuse and inappropriate dissemination of information. To help mitigate these risks, security logs, audit logs of user activity, and strict access controls are enforced. FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest users are granted access to these systems only after requesting access through their manager and the appropriate System Administrator.

Section 5.0 External sharing and disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

BBSS shares information with the FBI.

The information related to the UK Visa project outlined in the Introduction passes through BBSS and is sent to the UK government. It is deleted as soon as the data transfer is confirmed.

FMNS, CICS, FD-258, and IBIS Manifest do not share information with any organization outside of DHS.

Information resulting from the background check processes may be printed out and placed in the customer A-File. The A-File may be shared with external organizations such as immigration judges and other federal agencies. For a full discussion of the external sharing of the A-File, please see the A-File System of Records Notice (SORN), http://edocket.access.gpo.gov/2007/E7-375.htm.

5.2 What information is shared and for what purpose?

BBSS sends the EFTS 10-print record to the FBI to conduct a criminal background check against its IAFIS system.

As discussed in a separate PIA, BBSS also facilitates the transfer of biometric and biographic data pursuant to the UK Visa Program.

5.3 How is the information transmitted or disclosed?

FBI Fingerprint Check requests and responses are electronically transmitted through BBSS to and from the FBI's IAFIS system. FBI fingerprint and other biometric information and the responses are encrypted when electronically transmitted between BBSS and the FBI. The data exchange between USCIS and the FBI for the purpose of FBI Name Check occurs via zipped and encrypted email. For military applicants, if previous fingerprints are found, the liaison returns the fingerprint records on an encrypted compact disc to the Nebraska Service Center (NSC). Personnel at the NSC format these fingerprints from the compact disc and submit them through BBSS to the FBI for the required background check.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

USCIS has an existing MOU with the FBI (cited above) and US-VISIT that sets forth the terms and conditions for the transfer and use of information pertaining to background checks. USCIS also has an existing ISA with the United Kingdom. *Interconnection Security Agreement between USCIS and UK BBSS and UK VISAS, November 16, 2007.*[13]

5.5 How is the shared information secured by the recipient?

The recipient of the shared information is the FBI. The information provided to the FBI by USCIS is restricted to FBI employees with Top Secret clearances who work in secure facilities. The information transmitted is stored in FBI information systems that have been certified and accredited by the FBI in accordance with DOJ and National Institute of Standards and Technology (NIST) requirements.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

The external agency receiving access to the information sent by BBSS to the FBI IAFIS is the FBI. This information is used by FBI to perform criminal background check. The transfer of the data is

[13] USCIS is currently drafting an updated ISA for the UK VISAS Program.

conducted pursuant to the MOU between USCIS and the FBI. FBI employees who perform criminal background checks have received the required training to perform the checks.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Privacy Risk: Unauthorized access.

Mitigation: When BBSS sends information to and receives information from the FBI, the data is shared over DHS and FBI secured networks. FBI employees are trained and authorized to deal with biographic and biometric data. In addition, the FBI has policies and procedures in place to ensure that information is not inappropriately disseminated.

Privacy Risk: Misuse of data.

Mitigation: There is a possibility of misuse and inappropriate dissemination, but these risks are mitigated by taking advantage of the DHS Security specifications that require audit logs of user activity, security logs, and strict access controls. The risk associated with the fingerprint and biometric data that is transmitted to the FBI is also mitigated by the encryption of this data in accordance with DHS and NIST guidelines.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

The information in FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest are covered by DHS/USCIS SORN - 002(72 FR 31082), *Background Check Service*[14] and DHS/USCIS SORN - 003(72 FR 17172), *Biometric Storage System.*[15] This notice provides individuals with notice prior to the collection of information. Notice of also provided on all USCIS forms at the point of collection. (See Section 6.2).

[14] Available at http://edocket.access.gpo.gov/2007/07-2782.htm.
[15] Available at http://edocket.access.gpo.gov/2007/07-1643.htm.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Applicants who seek USCIS benefits are presented with a Privacy Act notice and a signature release authorization on the relevant benefit application/petition. The Privacy Act Notice details the authority and uses of information. The form is signed by the applicant indicating that s/he certifies and authorizes the release of any information from the applicant's record that USCIS needs to determine eligibility. Applicants are told at the point of data collection (generally in the form itself) that it is within their rights to decline to provide the required information; however, it will result in the denial of the applicant's benefit request.

USCIS benefit applications require that certain biographic information be provided and may also require submission of fingerprints and photographs. This information is critical in making an informed adjudication decision in granting or denying a USCIS benefit. The failure to submit such information would prohibit USCIS from processing and properly adjudicating the application/petition and thus preclude the applicant from receiving the benefit. Therefore, through the application process, individuals have consented to the use of the information for adjudication purposes, including background investigations.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3) of the Privacy Act and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested. The forms also contain a provision by which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Privacy Risk: The privacy risk associated with this particular collection of information is that the individual may not be fully aware that their information will be used to conduct an inquiry into benefits eligibility.

Mitigation: The collection of PII is a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk associated with this particular collection of information is that the individual may not fully understand how the data will be used to conduct background checks. In order to mitigate this risk, USCIS has provided a Privacy Act Statement on all benefit application/petition forms. The form also contains a signature certification and authorization to release any information provided by an applicant. The information in FMNS, CICS, FD-258 MF, BBSS,

and IBIS Manifest is covered by DHS/USCIS SORN - 002 (72 FR 31082), *Background Check Service* and DHS/USCIS SORN - 003(72 FR 17172), *Biometric Storage System.* The publication of the SORNs and this PIA serve as additional notice to individuals regarding the use of the information in all five systems.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

USCIS treats all requests for amendment of information in a system of records as Privacy Act amendment requests. Any individual seeking to access information maintained in these systems should direct his or her request to the USCIS FOIA/Privacy Act (PA) Officer at USCIS FOIA/PA, 70 Kimball Avenue, South Burlington, Vermont 05403-6813 (Human resources and procurement records) or USCIS National Records Center (NRC), P. O. Box 648010, Lee's Summit, MO 64064-8010 (all other USCIS records). The process for requesting records can be found at 6 Code of Federal Regulations (C.F.R.) § 5.21.

Requests for access to records in this system must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity (full name, current address, and date and place of birth) in accordance with DHS regulations governing Privacy Act requests (found at 6 C.F.R. § 5.21), and any other identifying information that may be of assistance in locating the record.

The information requested may, however, be exempt from disclosure under the Privacy Act because FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest files with respect to an individual may sometimes contain law enforcement sensitive information the release of which could possibly compromise ongoing criminal investigations.

If an individual would like to file a Privacy Act request to view their USCIS record the request can be mailed to the following address:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010,
Lee's Summit, MO 64064-8010

Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov.

7.2 What are the procedures for correcting erroneous information?

In addition to the Privacy Act procedure discussed above, if an individual determines that information in FMNS, CICS, FD-258, BBSS, or IBIS Manifest is inaccurate during the application and adjudication process, the individual can file a USCIS form for a name change located on the USCIS website, directed at changing the specific erroneous information.[16] For information such as an incorrect A-Number, the individual may contact USCIS' customer service number at 1-800-375-5283 (TTY 1-800-767-1833) to make the correction. USCIS personnel submit a ticket to the USCIS Help Desk requesting that the erroneous information be corrected. The correct information is then provided by the applicant and verified (if necessary). The Help Desk forwards the request to an authorized system administrator and the erroneous information is corrected. If an applicant believes their file is incorrect, but does not know which information is erroneous, the applicant may file a Privacy Act request as detailed in Section 7.1.

If the particular USCIS process requires a personal interview by a USCIS examiner in order to adjudicate a benefit application, the applicant also has the opportunity to request changes to correct erroneous information during the interview.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified of the procedures for correcting their information on USCIS forms, in the SORNs and PIA covering the information in these systems, and by USCIS personnel who interact with benefit applicants.

7.4 If no redress is provided, are alternatives are available?

USCIS provides redress to applicants as outlined in Sections 7.1 and 7.2.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Privacy Risk: The main risk with respect to redress is that the right may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: The redress and access measures offered by USCIS are appropriate given the purpose of the systems. Individuals are given numerous opportunities during and after the completion of

[16] The USCIS website contains links to all available USCIS forms. These forms include the AR-11 address change form as well as other immigration forms which may be used to amend information located in the individual's record.

the applications process to correct information they have provided and to respond to information received from other sources including receiving information about why a benefit was denied and their appeal rights.

Privacy Risk: There is a risk that a FOIA or Privacy Act request may not be expansive enough to include a search of specific systems or the records search may only include the A-File.

Mitigation: To mitigate this risk, USCIS places a hard copy of the RAP Sheet (if applicable) and results from the FBI Name Check (if positive) in the applicant's A-File which ensures that the requestor gains access to the information when appropriate under the FOIA and Privacy Act.

Section 8.0Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

USCIS deploys role-based access controls to limit access to only those persons who have a need to know this information in order to perform their duties. In compliance with federal law and regulations, users have access to FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest on a need to know basis. This need to know is determined by the individual's current job functions. Users may have read-only access to the information if they have a legitimate need to know as validated by their supervisor and the system owner and have successfully completed all personnel security training requirements. System administrators may have access if they are cleared and have legitimate job functions that would require them to view the information. Developers do not have access to production data except for specially cleared individuals who perform systems data maintenance and reporting tasks. Access privileges are limited by establishing role-based user accounts to minimize access to information that is not needed to perform essential job functions.

A user desiring access must complete a Form G-872A & B, USCIS and End User Application. This application requires justification for the level of access being requested. The requestor's supervisor, the system owner, and the USCIS Office of the Chief Information Officer (OCIO) review this request; if approved, the requestor's clearance level is independently confirmed and the user account is established.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors are used to maintain systems and to provide technical support.. Access is provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant USCIS and DHS policies. In addition, USCIS employees and contractors who have completed a G-872A & B form (See Section 8.1) and granted appropriate access

levels by a supervisor are assigned a login and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation in order to obtain the appropriate access levels. All access to the FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest systems follow the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

8.3 Does the system use "roles" to assign privileges to users of the system?

There are two classes of users for FMNS:

- Class 1 – Read/Write/Query – Users that enter masthead data, generate manifests and generate fingerprints appointment notices and have query capabilities; and
- Class 2 – System Administrator – Users requiring system administrative privileges.

There are two classes of users for CICS:

- Class 1 – RAIO Officer – captures and processes applicant biographic and biometric data; and
- Class 2 – Application Administrator – has the ability to modify configuration settings for the CICS application

There are two classes of users for FD-258:

- Class 1 – Query – Read access only. Users can query by A-Number or Name and DOB; and
- Class 2 – System Administrator – Users requiring system administrative privileges.

There are four classes of users for BBSS:

- Class 1 – User – Users requiring Fingerprint and Biometrics submission and query capabilities;
- Class 2 – Power User – Users requiring Fingerprint and Biometrics submission;
- Class 3 – Administrator – Users requiring all standard functions and the ability to run reports; and
- Class 4 – System Administrator – Users requiring system administrative and database administrative privileges. This class is reserved for authorized contractors that support BBSS who are located at the USCIS HQ location. Moreover, this class is not assigned to any user located at a USCIS field site.

There two classes of users for IBIS Manifest:

- Class 1 – Query – Read access only; and
- Class 2 – System Administrator – Users requiring system administrative privileges.

8.4 What procedures are in place to determine which users may access the system and are they documented?

A standard request form (G-872B) must be completed by each user and authorized by a supervisor in that department and by the system owner's representative.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

To ensure that users do not use the data outside of scope of their official job duties, audit trails are kept to track and record the activity of each user. Reports can also be run against each system to verify that a user's activity is consistent with his or her permissions.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest maintain audit logs on all transactions and user activities. Because Fingerprint/Biometrics data requests can be resubmitted based on poor or problematic images, audit trails are required to ensure that the Fingerprint/Biometrics data requests are not duplicated. Therefore, BBSS also provides audit trail records that record efforts to resubmit, review, and examine the originally submitted FBI Fingerprint/Biometrics request transactions. All transactions are subject to monitoring and review to ensure that the original requests or results are not lost, manipulated, or compromised in any manner. Lastly, NIST approved data encryption is used for data transportation between USCIS and the FBI to ensure that data has not been tampered with en-route and to prevent unauthorized personnel from accessing the data.

Locally employed staff at USCIS overseas field offices who are not US Citizens must have a DHS systems waiver to operate the CICS fingerprint units.

USCIS has followed DHS guidelines for encrypting all CICS mobile devices to ensure the data cannot be compromised. In addition, USCIS employs two-factor authentication for the fingerprint devices. CICS will comply with physical and logical security policies applicable to systems within the USCIS enterprise. This requires the protection of applicant data during capture through transmission to backend USCIS systems, secure transmission of sensitive data through the use of digital certificates and Secure Socket Layer (SSL) transactions, and username and password required for system access.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

USCIS provides training to all FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest users. This training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORN, Privacy

Act Statements, etc.). Each USCIS site has the responsibility to ensure that all federal employees, locally employed staff, and contractors receive the required annual security and Privacy Act training.

In addition, USCIS employees, locally employed staff, and contractors who have completed a G-872B form (See Section 8.4) and have been granted appropriate access levels (See Section 8.3) by a superior are assigned a login and password from the appropriate System Administrator used to access the system. These users have previously undergone federally approved clearance investigations and signed appropriate documentation in order to obtain the appropriate access levels.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The fingerprint/biometrics data that is captured, processed, and stored by FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest is secured in accordance with Federal Information Security Management Act (FISMA) requirements. The authority to operate (ATO) for BBSS was issued on June 29, 2009 and expires on June 29, 2012. FMNS is a subsystem under BBSS and follows the BBSS ATO. CICS also falls under the BBSS ATO. FD-258 MF was certified and accredited on July 31, 2008 for a three year period expiring July 31 2011. IBIS Manifest is covered under the CISCOR C&A. The ATO for CISCOR, which includes IBIS Manifest, was issued on March 21, 2008 and expires on March 28, 2011.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Privacy Risk: Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and transmission/sharing) that require mitigation.

Mitigation: Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users are broken into specific classes with specific access rights. Audit trails are kept in order to track and identify unauthorized uses of system information. Data encryption is employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Since FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest have been implemented in the production environment, authorized users are organized into specific classes with specific access rights, audit trails are retained to track and identify unauthorized uses, and data encryption is employed at every appropriate point to verify that only authorized users can view the data and the data is not compromised during transmission. Further, FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest comply with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack, and unauthorized information dissemination.

CICS will be developed with security provisions intended to prohibit unauthorized access and modification to system resources. Such provisions include installation on approved USCIS computing

resources, to include use of encrypted hard drives for laptop deployments.

CICS will enable RAIO Officers to upload applicant information to a centralized USCIS system, which is currently BBSS. The information can only be uploaded when secure communications with the USCIS network is established. In the event that communications with the USCIS network is not possible, CICS will enable RAIO Officers to save applicant information to secured portable media for manual processing.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

The FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest systems were designed and implemented with both commercial off-the-shelf products and custom designed software, databases, and user interfaces.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest developers followed the ITLM and SDLC security guidelines in the design and development of FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest respectively. All documentation has been reviewed and approved by USCIS OIT IT Security. Background check requests and result records are attributed to the correct applicant file by matching multiple data points including A-Number, receipt number, last name, and DOB.

9.3 What design choices were made to enhance privacy?

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest are only available to USCIS employees and contractors who have appropriate security and access controls. The general public does not have access to these systems. Protection and integrity of data, security, and privacy are of paramount concern. These systems follow all DHS Security guidelines for enhanced security including the C&A security documents, Federal Information Processing Standards 199, FISMA, Trusted Agent - FISMA, OMB memoranda, and NIST security guidelines.

Responsible Officials

Donald Hawkins
USCIS Privacy Officer
Department of Homeland Security

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

オーストラリア
(PIA Report)

事例）

オーストラリア移民帰化関係省

（DIAC）ＰＩＡ報告書

Australian Government
Department of Immigration and Citizenship

protiviti®
Risk & Business Consulting. Internal Audit.

Department of Immigration and Citizenship

Privacy Impact Assessment for the Movement Alert List

July 2010

Table of Contents

1. Executive Summary

1.1 Background

During 2009 the Australian National Audit Office (ANAO) conducted an audit of the effectiveness of the Department of Immigration and Citizenship's (DIAC's) management and use of the Movement Alert List (MAL). In this report the ANAO recommended that a Privacy Impact Assessment (PIA) be conducted on DIAC's Centralised Movement Alert List (CMAL). In particular, the ANAO report stipulated that:

"DIAC is aware of the importance of privacy of personal information and the relevant requirements of its own legislation and the Privacy Act. It is also aware that MAL very largely comprises personal information, some of which is sensitive. DIAC has not considered the privacy implications of its use of MAL in any substantial way. At one point, the department contemplated but did not proceed with a Privacy Impact Assessment (PIA) for MAL during its CMAL project. It is apparent from the analysis in Chapter 5 that DIAC would be better able to assure itself that it satisfies the Information Privacy Principles if it were to conduct a PIA of its administration of MAL. The department has agreed to do so". (ANAO Audit Report No. 35, 2008-09 "Management of the Movement Alert List, page 16)

The MAL is a computer database that stores details of identities and travel documents of immigration concern to Australia. The use of MAL to monitor and govern the entry to and presence in Australia of non-citizens who are characters of concern is a mature activity that enables DIAC officers to make appropriate decisions during the assessment phase of visa applications, inbound travel and post arrival requirements, such as medical checkups for foreign nationals. In addition, it provides controls around Australian identification documents, most notably passports, ensuring awareness of the misuse of identification documents that have previously been reported as lost, damaged or stolen.

Management within the Border Operation Centre (BOC) of DIAC requested this Review to discharge the obligation above, and ensure that the operation of the MAL is in compliance with the *Privacy Act, 1988*, and any relevant privacy implications of the *Migration Act, 1958*, *Australian Citizenship Act, 2007* and the *Freedom of Information Act, 1982* in relation to personal information held on the MAL.

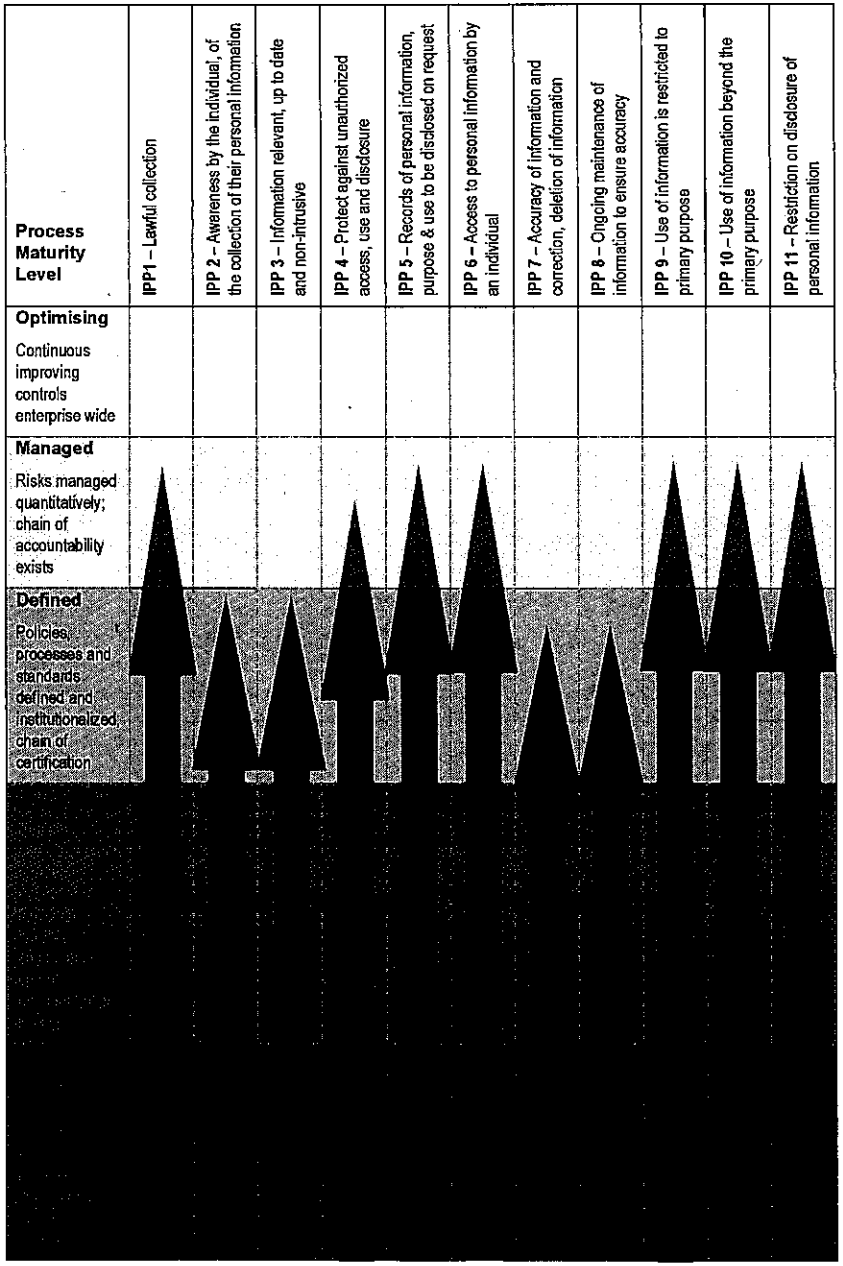
1.2 Overall Assessment

The assessment of privacy risks to the MAL did not indicate any major issues in relation to the eleven Information Privacy Principles (IPPs) contained in the *Privacy Act, 1988* and seven privacy elements in the *Privacy Impact Assessment Guide* produced by the Office of the Privacy Commissioner. Findings were identified in the areas of:

- Notification of collection of personal information stored in MAL (IPPs 1 & 2); and
- Maintenance of personal information in MAL and the accuracy of information (IPPs 7 & 8).

Consultation with the DIAC Privacy Officer and staff of the BOC indicated that the residual privacy risk facing the MAL databases and supporting systems are low. In this regard it should be noted that a review of the DIAC "Monthly Client Feedback Report" prepared by the Client Experience, Standards and Feedback Section of the Operational Performance Branch indicates only a small number of queries regarding personal information and/or privacy. The majority of these are not directed at the MAL.

The Privacy Capability Maturity Model depicts the maturity of the underlying business processes supporting the privacy program. The diagram below is an assessment of elements of the maturity of business processes for the MAL with regard to the IPPs:



It is worth noting that there is no requirement to reach an "Optimised" level and it is the responsibility of management, with the Secretary and SES, to determine how far along the process evolution scale the department wants to be in this area.

1.3 Recommendations

IPP2: Solicitation of personal information from individuals

DIAC can improve the information provided to persons entering Australia through the addition of an advisory note on visa applications, ETA and passenger movement cards stating:

"For further information about the collection and use of your personal information please see DIAC Fact Sheet 77 and form 993i. Please ask immigration officials, or see www.immigration.gov.au for details if required."

or similar, legally approved wording.

IPP4: Storage and Security of Personal Information

The BOC should document a security plan and undertake relevant testing of the plan for the CMAL version of MAL (being the latest version of the MAL). We note that security plans have been prepared for previous versions of the MAL (Heritage MAL).

IPP8: Record Keeper to Check Accuracy of Personal Information Before Use

Prior to making a final decision on an individual's request to enter Australia using personal information held in the MAL the DIAC officer involved should ensure that the information held is the most up to date and relevant information. This should include reference to the relevant ARC owner to request confirmation that the information provided is still accurate and relevant, prior to making a final decision.

The BOC, as managers of the MAL process on behalf of Whole of Government, should provide the strategic guidance to the owners of the data on MAL, to ensure a regular process of review is conducted to update information held in MAL which is deemed of lower accuracy or from a lower quality source, to ensure the accuracy of information held.

1.4 Other Matters

This report is intended solely for use by DIAC and should not be distributed, nor communicated to any third party without the consent of the Department Audit Committee, and without informing the Internal Audit Section, Governance and Audit Branch and Protiviti.

The report should be read in the context of the scope and scope limitations outlined in Section 2.

2. Introduction and Overview

2.1 Background

During 2009 the ANAO conducted an audit of the effectiveness of DIAC's management and use of the MAL. In this report the ANAO recommended that a PIA be conducted on DIAC's CMAL. In particular, the ANAO report stipulated that:

"DIAC is aware of the importance of privacy of personal information and the relevant requirements of its own legislation and the Privacy Act. It is also aware that MAL very largely comprises personal information, some of which is sensitive. DIAC has not considered the privacy implications of its use of MAL in any substantial way. At one point, the department contemplated but did not proceed with a Privacy Impact Assessment (PIA) for MAL during its CMAL project. It is apparent from the analysis in Chapter 5 that DIAC would be better able to assure itself that it satisfies the Information Privacy Principles if it were to conduct a PIA of its administration of MAL. The department has agreed to do so". (ANAO Audit Report No. 35, 2008-09 "Management of the Movement Alert List, page 16)

Management within the BOC of DIAC requested this Review to discharge the obligation above, and ensure that the operation of the MAL is in compliance with the *Privacy Act, 1988*, and any relevant privacy implications of the *Migration Act, 1958*, *Australian Citizenship Act, 2007* and the *Freedom of Information Act, 1982* in relation to personal information held on the MAL.

2.2 General Privacy Information

The Privacy Act 1988 defines "personal information" as:

"...information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

Personal information does not always need to include an individual's name to be regulated by the *Privacy Act*. It may include information that can be linked to or can identify a specific individual through association or inference. Unless consent is provided by the individual, the *Privacy Act* prohibits disclosure of personal information by a collector to any third party unless it is otherwise permitted by one of the information Privacy Principle 11 disclosure provisions.

Examples of personal information may include an individual's name, home and e-mail address, telephone number(s), passport number, bank account details, residency status and ethnic background.

The *Privacy Act* also defines "sensitive information" as:

"...information or an opinion about an individual's: racial or ethnic origin, political opinion, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practice, or criminal record that is also personal information, or the health about an individual."

Sensitive information is collected in the MAL databases on a number of the criteria specified.

Section 14 of the *Privacy Act 1988* contains 11 IPPs which explain how agencies should handle individuals' personal information. Please refer to Appendix 1 for the detail of the IPPs.

2.3 Background to the Movement Alert List

The MAL is a computer database administered by the BOC. The MAL stores details of identities and travel documents of immigration concern to Australia. The MAL facilitates the process of governing the entry to and the presence in Australia of non-citizens who are of character concern. The MAL was established to enable DIAC to apply relevant sections of the *Migration Act, 1958* and the *Australian Citizenship Act, 2007*.

DIAC officers use the MAL at several points during the visa application, Electronic Travel Authority (ETA) and inbound travel processes, contributing to a 'layered' approach to border management. In this way, the MAL forms an important element in Australia's national security and border protection

strategy.

The MAL contains two subsidiary databases; the first, the Person Alert List (PAL), contains adverse information about persons' identities, which are placed on this list for various reasons („Alert Reasons'). The second is the Document Alert List (DAL), primarily a list of lost and stolen travel documents. BOC processes include a cross-match of MAL data when any non-citizen seeks a visa, seeks to travel to or enter Australia or applies for citizenship. Essentially, the MAL is a collection of information, substantially personal or sensitive information as defined by the *Privacy Act,* about identities and travel documents of interest, primarily, to visa decision-makers.

Details of identities of concern are recorded on the MAL as a result of the department's liaison with national security, law enforcement agencies and departmental offices in Australia and overseas. If there is a MAL match a decision on entry is taken by the department in consultation with any other relevant agency. As a result, DIAC is both receiving and sharing personal (and at times sensitive) information from and with other Australian Government agencies.

The MAL is not a mandated system under the *Migration Act, 1958*; however the MAL facilitates the processes for governing border security, most noticeably "*to regulate, in the national interest, the coming into, and presence in, Australia of non citizens*" (Section 4(1) of the *Migration Act*).

2.4 Review Objective

The objective of the Review was to assess the effectiveness of the controls in place to mitigate the risk of DIAC not adhering to the *Privacy Act* and satisfying the IPPs, along with the privacy or personal information management requirements of other legislative requirements including; *the Migration Act*, the *Australian Citizenship Act*, the *Archives Act, the Freedom of Information Act, 1983* and DIAC Policies and procedures with regards to the MAL system.

The PIA included:

- An analysis of the privacy requirements of the *Migration Act, 1958*, *Australian Citizenship Act, 2007* and the *Privacy Act, 1988*;
- Assessment of process design effectiveness of compliance and non-compliance for the above stated legislative requirements for privacy;
- Assessment of the process design effectiveness of the transfer of information between MAL, Australian Customs and Border Protection Service and other agencies (as necessary);
- The identification of improvement opportunities of the BOC's business and IT processes regarding the collection, use, access and correction, data quality, identity management, disclosure and security of personal information against better practices; and
- The identification of residual improvement opportunities and development of action plans.

Scope Limitations

The PIA did not:

- Undertake an assessment of any other risks other than privacy;
- Assess the business processes of either the sources of, or destination for personal information that was beyond the MAL and the direct authority of the BOC;
- Assess the privacy requirements of information provided by, or to, the Australian Security Intelligence Organisation (ASIO),;
- Assess the computer coding of the MAL, or the data transfer protocols and secure communication lines used for transmission of information between DIAC offices and third party agencies;
- Conduct transaction testing of staff interaction with the MAL, or reviews of the audit trails to detect any inappropriate access; or
- Validate management representations which would require a significant amount of further audit work, where there is no reason not to rely on the representations made. For example, the Review did not consider the process for collection by, or rights of third parties to share information with the BOC for the purpose of updating an Alert Reason Code (ARC) in the system. Stakeholder consultation was conducted only to identify the interfaces, and the personal information shared between the BOC and those parties.

This report provides management with information about the nature of risks surrounding privacy at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this Review will not and cannot anticipate.

The management of the department is responsible for maintaining an effective internal control structure and to ensure adherence to the ANAO report Chapter 5. The purpose of this PIA is to assist management in discharging this obligation. This PIA was conducted in order to assess the system of internal controls of privacy for the MAL and to express an opinion on those control procedures.

Due to the inherent limitations in any internal control structure, it is possible that errors or irregularities may not be detected. Furthermore, the overall internal control environment within which the control procedures operate were not audited, and therefore an overall opinion of the effectiveness of the control framework is unable to be provided.

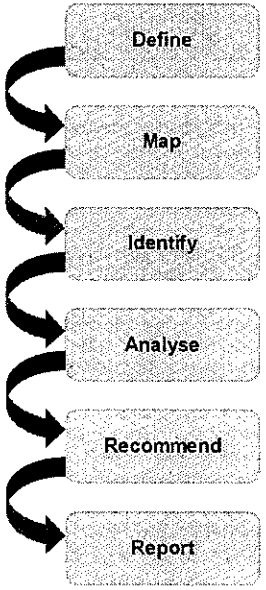
Please note that a PIA is not designed to detect all weaknesses in control procedures as it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis. Any projection of the evaluation of the control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

2.5 Method and Approach

The Review was conducted taking a holistic view of the MAL and the privacy requirements for the DIAC, using a business process approach.

During the Review we considered the existing operating processes and procedures, together with the proposed changes to the pending Central MAL (CMAL) Procedures Advice Manual (PAM – version 3).

The key stages of our privacy impact assessment method are shown below:



Define the project, clearly describing those components that are included and excluded from the PIA

Describe and map the process flows for personal information received by, used in and distributed from the MAL activity

Identify and document the access rights and content of all personal information held in the MAL

Analyse the privacy impacts of the process flows, user access rules and nature of personal information content, including the conduct of a risk assessment

Identify and discuss options to improve privacy outcomes with DIAC personnel

Compile a report including the privacy impact assessment, capability maturity model for the management of personal information and recommendations for improvement to MAL processes

This PIA followed the guidance for undertaking a PIA as issued by the Office of the Privacy Commissioner in its *Privacy Impact Assessment Guide, August 2006*, and specifically included the following:

- Consultation with the department's Privacy Contact Officer to ensure the department's policies, procedures and overall privacy risk management approach is built into the PIA, and the MAL project team, to understand the aims and objectives of the program;
- Mapping the information flows in the MAL and supporting business process;
- Identification of personal information as defined by the Office of the Privacy Commissioner and the department's policies and procedures on privacy management. This included answering the following questions:
  - what personal information is to be used;
  - how is the personal information to be collected;
  - how will the personal information be used;
  - who within the department will access or use the personal information;
  - disclosures of personal information;
  - security arrangements; and
  - any privacy, secrecy or other relevant legislation applying to those flows;
- Analysis of each of the elements of personal and sensitive information and how it is used, to determine how it affects upon privacy (both positively and negatively). In doing this, we followed the decision and assessment tools included in the Privacy Impact Assessment Guide; and
- Developed recommendations for system design or business process design to effectively manage identified privacy impacts (without unnecessarily over-investing in privacy management).

2.6 Risks Addressed

The following two risks from the 2009-10 Corporate Risk Register have relevance to the MAL and Privacy activities:

Risk No	Risk Summary	Consequences	Current Controls	Inherent Rating	Planned/Future Controls	Residual Risk Rating
5	Entry into Australia of persons of national security concern or persons with serious health issues	Reduces community confidence in the Department Outcome 4	Timely information sharing and cooperation with security agencies Relevant reviews of MSIs MAL and other IT security protocols in place Compliance / ALO network MAL, C-MAL, SRS Whole of Government partnerships Partnerships with like-minded countries	Significant	Investment in sound biometric data Improve analytic capabilities through the Next Generation Border Security Initiative	Moderate

Risk No	Risk Summary	Consequences	Current Controls	Inherent Rating	Planned/Future Controls	Residual Risk Rating
10	The Department's ability to collaborate with central agencies and relevant government stakeholders	Fails to raise the complex profile of immigration and citizenship issues Enabler	Engagement with other stakeholders Relationships with current IDC Cross government taskforces	Significant	Greater participation in IDCs Further engagement with stakeholders such as: - DEEWR - Health - PM&C Investment in policy / research capabilities of the Department: - FAS meetings - Secretary's messages	Moderate

These risks have been considered during the PIA and Risk Analysis together with more broad privacy related, operational and systems risk criteria.

3. Description of Project and Information Flows

3.1 Description of Personal Information Captured

Overall Aims of the Activity

The MAL is a computer database administered by the BOC, with the purpose of storing the details of identities and travel documents of immigration concern to Australia. The MAL contains two subsidiary databases, being the:

- Person Alert List (PAL), contains adverse information about persons' identities who are placed on this list for various reasons ('Alert Reasons'); and
- Document Alert List (DAL), primarily a list of lost and stolen travel documents.

BOC processes include a cross-match of MAL data when any non-citizen seeks a visa, seeks to travel to or enter Australian or applies for Citizenship. Essentially, the MAL is a collection of information (substantially personal or sensitive information) about identities and travel documents of interest, primarily, to visa decision-makers.

Reason for the Activity

The MAL was established to enable DIAC to apply relevant sections of the *Migration Act, 1958* and the *Australian Citizenship Act, 2007*. The MAL facilitates the process of governing the entry to and the presence in Australia of non-citizens who are of concern.

While not a mandated system under the *Migration Act, 1958*, the MAL facilitates the processes for governing border security, most noticeably "*to regulate, in the national interest, the coming into, and presence in, Australia of non citizens*" (Section 4(1) of the *Migration Act*).

Scope and Extent of the Activity

Details of identities of concern are recorded on the MAL as a result of the department's liaison with national security, law enforcement agencies and departmental offices in Australia and overseas.

If there is a MAL match a decision on entry is taken by the department in consultation with any other relevant agency. As a result, DIAC is both receiving and sharing personal (and at times sensitive) information from and with other Australian Government agencies.

Links to Existing Programs and Activities

DIAC officers use the MAL at several points during the visa application, Electronic Travel Authority (ETA) and inbound travel processes, contributing to a 'layered' approach to border management. In this way, the MAL forms an important element in Australia's national security and border protection strategy.

The MAL databases sit within the umbrella of the Systems for People system strategy of DIAC, a single portal providing DIAC staff with improved access to information across the DIAC business network. The MAL information does not however, automatically update or interface with other systems and databases either in or outside Systems for People. Rather, the MAL requires individual input and access by authorised persons.

What Personal Information is Collected

The MAL captures personal information, including sensitive and health information, primarily regarding non-citizens who have requested permission to travel to Australia (i.e. by way of a visa application or ETA). Personal information stored on MAL includes:

- Full Name
- Date of Birth
- Place of Birth
- Sex

- Country of Citizenship
- Passport Number, and
- Alert Reason Code (ARC) (one or more).

The ARC does not necessarily provide additional information in the MAL to explain the ARC. For example, ARC 06 is the relevant code for health related information. The MAL will include the ARC 06 and an indication of whether the code is deferred, that is, pending further information such as additional health test results, or time limited, indicating the individual is only permitted to stay on shore in Australia for a limited time period.

In this instance, details of the reason the ARC 06 is used are not contained in the MAL, but reside in a separate DIAC system, the Health Assessment Tribunal System (HATS). HATS generates a daily (Tuesday – Sunday) batch upload to CMAL, embedding the ARC into the MAL database. Only the ARC is included though, and a DIAC official requesting further information would need to contact a DIAC health case officer for assistance. A similar process is followed for other ARCs, for example, details of national security concerns would be referred to the relevant security agency (ASIO) and details of matters relating to children would be referred to the Department of Foreign Affairs and Trade (DFAT), with MAL only containing the ARC.

4. Privacy Impact Assessment

4.1 IPP 1 – Manner and purpose of collection of personal information

1. *Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:*

   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

   (b) the collection of the information is necessary for or directly related to that purpose.

2. *Personal information shall not be collected by a collector by unlawful or unfair means.*

Checklist	YES	NO
Does the MAL involve the collection of sensitive or intimate information?	☒	☐
Could the collection of the personal information be considered unfair or unlawful?	☐	☒
Will DIAC need to make amendments to current legislation to allow for the lawful collection of this personal information?	☐	☒
Is the following statement true? • The purpose for the collection of personal identifiers has not been defined.	☐	☒
Does the MAL involve surveillance?	☐	☒

Sources of Information

Collection of personal information recorded in the MAL is for a lawful purpose, as specified in Section 5A(3) of the *Migration Act*, and includes:

a) to assist in the identification of, and to authenticate the identity of, any person who can be required under this Act to provide a personal identifier; and

b) to assist in identifying, in the future, any such person; and

c) to improve the integrity of entry programs, including passenger processing at Australia's border; and

d) to facilitate a visa holder's access to his or her rights under this Act or the regulations; and

e) to improve the procedures for determining visa applications; and

f) to improve the procedures for determining claims for protection under the Refugees Convention as amended by the Refugees Protocol; and

g) to enhance the Department's ability to identify non citizens who have a criminal history, who are of character concern or who are of national security concern; and

h) Section 5A(3); and

i) to detect forum shopping by applicants for visas; and

j) to ascertain whether:

a. an applicant for a protection visa; or

b. an offshore entry person who makes a claim for protection under the Refugees Convention as amended by the Refugees Protocol;

had sufficient opportunity to avail himself or herself of protection before arriving in Australia; and

k) to complement anti people smuggling measures; and

l) to inform the governments of foreign countries of the identity of non citizens who are, or are to be, removed or deported from Australia.

The MAL is specifically designed to collect personal, including sensitive information from a variety of sources for the identification, assessment and control processes for DIAC. Sources include the individual concerned, other Australian Government agencies, foreign governments, health professionals, and in some cases, third parties such as family members or visa application support services, on behalf of the individual.

Collection Directly from an Individual

Collection directly from an individual is the preferred mechanism for collection of personal information under the *Privacy Act*. The majority of information collected for the purposes of the MAL database would be provided by the individual, for example, application by a foreign national for an Australian visa requires the individual to complete a Visa Application Form, containing the majority of personal information that is likely to be held in the MAL.

In a number of circumstances collection is from a third party, such as another Australian Government agency. The Document Alert List for example contains the details of lost, damaged or stolen passports that have been reported to the DFAT, and which that Department has forwarded on to DIAC for the purposes of inclusion in the DAL. Personal information in this instance includes the details stored in the passport, being the person's name, sex, date and place of birth and passport number.

4.2 IPP 2 – Solicitation of personal information from individuals concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law - the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

Checklist	YES	NO
Will clients be provided with information regarding the purposes for which their personal information will be used?	☒	☐
Will clients be provided with information regarding third parties to whom their personal information may be disclosed?	☒	☐
When seeking consent will we accurately inform the client of what s/he is consenting to?	☒	☐
Is the following statement true? • Consent from a client will not be assumed simply because the client does not object?	☐	☒
If the collection of the personal information is authorised or required by law, will the client be informed of this?	☒	☐

Checklist	YES	NO
If the collection of personal information is required under law will the consequences of not providing the personal information be explained?	☒	☐

During the collection of information from individuals for their visa application they are informed of the primary purpose of providing information to DIAC, being the assessment of their application for entry to Australia (and it's Excised Offshore Places).

Due to the lawful collection requirements under the *Migration Act* an individual is not able to withhold consent and still proceed with a visa application. Accordingly, there is an implied or assumed consent to the storage of information on the MAL for visa processing purposes. This would include both storage of personal information and cross referencing to the PAL for processing an individual's visa or ETA request.

There is no formal consent process for the storage of personal information associated with lost, stolen or damaged identification documents in the DAL however, the collection and use of information is required under the *Migration Act* and is therefore deemed a lawful collection.

There is no formal notification to the individual whose personal information is stored on, or cross matched with MAL, that their information has been collected and used in this way. As a result while DIAC complies with the collection principles for notification of information for purposes of immigration and border security, a greater level of awareness and information could be provided. To address this, DIAC have developed *Fact Sheet 77 – The Movement Alert List* which is available on the DIAC internet page, to inform the public of the MAL, however this document is neither referred to, nor provided at the time of collection of personal information.

Where an individual requests further information on the collection of their personal information, DIAC have issued the 993i form – *Safeguarding your personal information* which explains how DIAC handles personal information. This form is available online and at all DIAC offices, and the information in the form is relevant to the information stored on the MAL databases. This form includes details of disclosure to other Australian Government agencies, for example DFAT specifies that where disclosure is required by law, information will be provided to other Australian Government and state and territory agencies.

Risk

An individual could challenge DIACs right to collect and store personal information about them in the MAL. This challenge would most likely be a letter of complaint to DIAC in the first instance, potentially escalated to the Office of the Privacy Commissioner if the individual feels their complaint has not been adequately addressed.

Suggested solution	Priority
DIAC can improve the information provided to persons entering Australia through the addition of an advisory note on visa applications, ETA and passenger movement cards stating: *"For further information about the collection and use of your personal information please see DIAC Fact Sheet 77 and form 993i. Please ask immigration officials, or see www.immigration.gov.au for details if required."*. or similar, legally approved wording. DIAC should review DIAC Fact Sheet 77 to ensure it meets the ongoing needs, and is factually accurate with the transition to the CMAL platform.	Low

Management Response	
Agreed:	
Implementation Date:	
Section and Branch responsible for implementation:	
Comments:	

4.3 IPP 3 – Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector:

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Checklist	YES	NO
Will the personal information collected intrude to an unreasonable extent on the personal affairs of the client?	☐	☒
Could the collection of the personal information be considered excessive to perform required business functions/activities?	☐	☒
Is the following statement true? • Personal information will not be date stamped and modifications to the original will not be monitored?	☐	☒
Is it foreseeable that personal information may be used for a purpose other than the primary purpose for which it is collected?	☐	☒

All personal information collected and stored in the MAL is considered relevant to the primary purposes of collection, being amongst other things, the assessment of visa applications, authentication of identities and the identification of non-citizens who are characters of concern.

Where DIAC is provided with personal information from third party organisations, for example, via other Australian Government departments or foreign government departments, DIAC considers the nature of the information provided, and the original source of information prior to making a decision on whether to rely on the information provided.

All personal information collected is recorded with a date stamp and source code, to ensure relevance of the information is able to be monitored. Where personal information is subsequently considered to be out of date or inaccurate it is deleted or modified to reflect the current situation.

For example, where an ARC06 (Health) deferred status exists, this is followed up within six months of the requirement to provide a Health Undertaking, or sooner if the Health Undertaking is provided.

In contrast, where an identity is placed on the PAL based on information provided by a foreign government, and new information is subsequently presented by a more reliable source (e.g. an Australian Government department) then the data is modified to reflect the most accurate data.

4.4 IPP 4 – Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Checklist	YES	NO
Will access to personal information and access for the purposes of adding, deleting and changing personal information be limited to those individuals who need this access to carry out their job?	☒	☐
Will security safeguards be in place to prevent unauthorised attempts to access, manipulate or delete personal information?	☒	☐
Will staff be provided with ongoing training relating to the security of personal information?	☒	☐
Will sensitive personal information be transmitted by secure means to prevent unauthorised access or interception?	☒	☐
Will personal information be stored in a secure database?	☒	☐
Will third parties or contractors who are participating in the collection, disclosure or handling of personal information be required by contract to comply with the Information Privacy Principles?	☒	☐
Will the level of security of digital transactions match the potential harm caused by breaches of privacy?	☒	☐

DIAC have procedures in place to control access to the MAL database and associated personal information. This includes the "provisioning" process for access to information systems, where access to the MAL is based on the user position type, for example:

- CMAL Onshore Visa Processing Officer (VPO – Case officers that process citizenship or visa applications).
- CMAL Compliance (Compliance or Character officer access).
- CMAL Border (Airport and Seaport staff access).
- CMAL ARC owner.

National security records and *specifically nominated* other records are classified as PROTECTED and require referral to the BOC for further information and override keys.

The Review discussed on a sample basis only, the sharing of information with ARC owners, to assess whether access to information for decision making was provided unnecessarily. In all cases information provided between the BOC and ARC owner is only the necessary information for that purpose, for example, health information is not provided to persons other than the Health ARC owner.

In developing the MAL, a security plan was developed for the system, based on the National Institute of Standards and Technology (NIST) Standard Service Program (SSP) standards, incorporating the international standards ISO 17799 "Information Security" and Information and Communications Technology Security Manual (ISM) requirements. We note however that the latest version of the MAL (CMAL) has not yet undergone the complete security review under these standards.

All transfers of information between DIAC locations, including DIAC head office (Belconnen, ACT,

Australia), other Australian offices, international locations, airports and other Australian Government agencies (e.g. ASIO) are conducted over encrypted and secure data lines via the Australian Government protected enclave, as specified in the ISM. We were advised that testing of the application security, including data transfers was occurring at the time of the PIA.

Risk

Access to personal information retained in the MAL could be unlawfully or improperly obtained.

Suggested solution	Priority
A security plan and relevant testing of the plan for the CMAL version of MAL (being the latest version of the MAL) should be undertaken.	Medium

Management Response	
Agreed:	
Implementation Date:	
Section and Branch responsible for implementation:	
Comments:	

4.5 IPP 5 – Information relating to records kept by record-keeper

1. *A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:*

   (a whether the record-keeper has possession or control of any records that contain personal information; and

   (b) if the record-keeper has possession or control of a record that contains such information:

   (i) the nature of that information;

   (ii) the main purposes for which that information is used; and

   (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. *A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.*

3. *A record-keeper shall maintain a record setting out:*

   (a) the nature of the records of personal information kept by or on behalf of the record-keeper;

   (b) the purpose for which each type of record is kept;

   (c) the classes of individuals about whom records are kept;

   (d) the period for which each type of record is kept;

   (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

   (f) the steps that should be taken by persons wishing to obtain access to that information.

4. *A record-keeper shall:*

   (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

   (b) give the Commissioner, in the month of June in each year, a copy of the record so

maintained.

Checklist	YES	NO
Will personal information be retained in accordance with the relevant record management policies?	☒	☐
Will legislative requirements for the disposal of information be identified and managed?	☒	☐
Will information about the types of personal information collected and the purposes for the collection be maintained by DIAC and published in DIAC Personal Information Digest?	☒	☐

All information contained in the MAL is recorded in accordance with DIAC policy, including the requirements of relevant legislation, being the *Migration Act, Citizenship Act,* and the *Archives Act* (see Appendix 5 for further information on the privacy requirements within each of these Acts).

The disposal of personal information no longer required to be stored on MAL is deleted from the user interface of MAL, and archived according to Australian Government procedures and the requirements of the *Archive Act*.

Details about the types of personal information collected and the purposes of collection are provided by DIAC on Form 993i "Safeguarding your personal information".

4.6 IPP 6 – Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Checklist	YES	NO
Will records containing personal information be accessible to the individuals to whom the personal information relates?	☒	☐
Will appropriate information be available to clients under the Freedom of Information Act 1988?	☒	☐
Will the right to access personal information be explained to clients?	☒	☐
Will staff be made aware of the relevant provisions of the *Migration Act, Privacy Act* and *Freedom of Information Act* that govern access to records containing personal information?	☒	☐

Personal information of an individual is available to that individual on request. Details of how to access personal information is provided by DIAC Form 993i "Safeguarding your personal information" which outlines how personal information is available to an individual under the *Privacy Act* and the *Freedom of Information Act*.

DIAC staff are trained and made aware of their privacy responsibilities. During the conduct of the PIA, "Privacy Week" was held at DIAC, which included amongst other things:

- An email from the Secretary to all staff advising about Privacy Week, and the need to be privacy aware due to the large volume of personal information retained;
- A table in the foyer of the head office building, staffed during key periods of the day, and providing information to staff regarding privacy and how to protect personal information; and
- signage and information on the DIAC intranet site.

At that time, we were able to obtain the following DIAC documents, which are provided for the information of staff:

- Privacy Suggestions or Phrases;

- Privacy basics – what you need to know
- Disclosing personal information to foreign governments;
- Disclosing personal information to third parties (non-government agencies);
- Disclosing personal information for the enforcement of criminal law;
- Disclosing personal information with a client's consent; and
- Privacy, complaints handling and third party enquiries.

In addition to the above, all staff within the BOC are provided additional training regarding the handling, communication and recording of personal information to ensure appropriate records are kept and not inappropriately disclosed.

4.7 IPP 7 – Alteration of records containing personal information

1. *A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:*

   (a) is accurate; and

   (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. *The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.*

3. *Where:*

   (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

   (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

   the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Checklist	YES	NO
Will steps be taken to ensure that personal information is accurate at the time of collection and disclosure?	☒	☐
If technology will be used to gather or process personal information, will the technology be reliable?	☒	☐
Will the ways in which personal information can be accessed and corrected be explained to clients?	☒	☐
Will mechanisms be in place to allow for clients to access and correct personal information?	☒	☐
Is the following statement true? • Documents containing personal information are not withheld unless there are exemptions under the Freedom of Information Act 1988?	☒	☐
Will a mechanism be in place to monitor requests for access to or changes to records containing personal information?	☒	☐

BOC endeavour to ensure that all personal information held in the MAL is accurate, complete and up to date. The primary source of personal information collected and stored in MAL is from the individual, at the time that they submit their visa request, ETA or notify DFAT of a missing travel document (e.g. passport).

Form 993i *"Safeguarding your Personal Information"* provides individuals with sufficient information regarding the collection, use, disclosure and access to their personal information. Form 993i is available on the internet, and from any DIAC officer on request. Form 993i also discloses the individuals' rights under the *Freedom of Information Act*.

All requests for information are submitted on DIAC form 424A *Request for access to documents or information*. These requests are forwarded to a central point for processing, ensuring processes are in place for monitoring requests for access and changes to records containing personal information.

The MAL system and subsequent upgrades including the latest to CMAL are developed in-house, and follow a the development and testing processes documented in the National Institute of Standards and Technology (NIST) Standard Service program (SSP) standards, ISO 17799 "Information Security and Information and Communications Technology Security Manual (ISM). The development and testing processes have been conducted to ensure that the CMAL technology is reliable and secure at all times.

4.8 IPP 8 – Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Checklist	YES	NO
Is the following statement true? • Personal information will not be used unless it is known to be accurate, up to date and complete.	☒	☐

BOC endeavour to ensure that all personal information held in the MAL is accurate, complete and up to date. There are however times when this is not easily able to be confirmed, as the MAL maintains a static record of information at the time it was provided, and does not interface with other Australian Government systems.

DIAC have identified a hierarchy for the validity and accuracy of personal information provided to it. This is documented in the PAM. The hierarchy identifies the reliability of data records, and therefore accuracy, using rules summarised below:

- Where information is obtained from DIAC internal sources, this information is of the highest quality
- Where information is obtained from Australian Government agencies, this information is of high reliance, and
- Where information is provided by foreign government agencies, the source of the information to that government is desired, and the based on the source (original, third hand) information is considered of medium or low level of accuracy.

Where an individual is placed on the PAL based on information provided by a foreign government, and new information is subsequently presented by a more reliable source (including any Australian Government department) then the data is modified to reflect the personal information provided by the most reliable source data.

There are times where personal information will continue to be held, and appear to be inconsistent with known information about the individual, despite changes in the information for that individual. For example, a DAL record of a lost or stolen passport will continue to exist even in the event of the death or change of details (e.g. surname) of the individual concerned. The retention of the record is relevant as a valid passport is still an official document which could be the subject of identify fraud in

immigration matters. Expired passports are archived from the DAL following a mandated period of time consistent with the valid life cycle of the relevant passport authority.

Risk

An individual could complain to the Office of the Privacy Commissioner, requesting an investigation into the accuracy of personal information and the use of personal information for a relevant purpose under IPP8 of the *Privacy Act*.

Suggested solutions	Priority
Prior to making a final decision on an individual's request to enter Australia using personal information held in the MAL the DIAC officer involved should ensure that the information held is the most up to date and relevant information. This should include reference to the relevant ARC owner to request confirmation that the information provided is still accurate and relevant, prior to making a final decision.	Medium
The BOC, as owners of data held in MAL, should ensure a regular process of review is conducted to update information held in MAL which is deemed of lower accuracy or from a lower quality source, to ensure the accuracy of information held.	Medium

Management Response	
Agreed:	
Implementation Date:	
Section and Branch responsible for implementation:	
Comments:	

4.9 IPP9 – Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Checklist	YES	NO
Is the following statement true? • Personal information will not be used for a purpose other than the purpose for which it was collected unless it is lawful to do so?	☒	☐
Will DIAC audit logs be maintained to record all instances of data use?	☒	☐

The personal information held in the MAL database is only used for the purposes specified under section 4.1 – IPP1 Manner and collection of personal information, being those purposes outlined in Section 5A(3) of the *Migration Act*.

All DIAC staff are required to comply with the DIAC and Australian Public Sector code of conduct and ethical standards, including their handling of personal information. Members of the BOC are regularly reminded of the importance of client confidentiality and privacy matters due to the sensitive nature of the work, and high level of data available to them in their roles.

Audit trails exist to monitor all sources of access, and the Values and Conduct Section (VCS) have conducted spot audits to assess the appropriateness of access and browsing in the past. There is no formal mechanism of monitoring access requests, as the computer programming logic required to identify authorised access versus unauthorised access of an individual's personal information would require a very sophisticated level of programming to determine when access is non-authorised. The

cost to develop this level of sophistication far outweighs the risks associated with unauthorised access.

The ability to classify an individual PAL record at the PROTECTED level does exist but at the time of the review, only one DIAC based alert and all National Security alerts were classified as PROTECTED. All other DIAC sourced alerts are deemed DIAC-IN-CONFIDENCE. If used however, only persons within a select protective enclave would be able to access the record, and all other users would be directed to contact those persons. This approach is available if required for a higher level of protection.

4.10 IPP10 – Limits on use of personal information

1. *A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:*

   (a) the individual concerned has consented to use of the information for that other purpose;

   (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

   (c) use of the information for that other purpose is required or authorised by or under law;

   (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

   (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. *Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.*

Checklist	YES	NO
If DIAC finds a secondary use that can be made of data already collected, is the use consistent with uses consented to by the client?	☒	☐
Is the following statement true? • Personal information will not be used for a purpose other than the original purpose, unless the individual to whom the information relates consents or such use is required or authorised by law?	☒	☐
If personal data is used for law enforcement purposes will a note be kept on the record to indicate the disclosure?	☒	☐

The uses of personal information held in the MAL database are restricted to the uses specified in Section 5A(3) of the *Migration Act* and re-stated in Section 4.1. Policies and procedures require that BOC does not use the data for secondary uses.

4.11 IPP11 – Limits on disclosure of personal information

1. *A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:*

   (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

   (b) the individual concerned has consented to the disclosure;

   (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

   (d) the disclosure is required or authorised by or under law; or

   (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. *Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.*

3. *A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.*

Checklist	YES	NO
Will the client be reasonably likely to be aware that the information may be disclosed?	☒	☐
Will clients be informed of secondary disclosures of their personal information?	☒	☐
Would any disclosure of personal information to a third party or organisation be permitted by law?	☒	☐
Will personal information disclosed to third parties be protected from privacy risks?	☒	☐
If personal information is obtained from a third party will it only be used by DIAC for the purpose that it was provided for?	☒	☐
If personal data is disclosed for law enforcement purposes will a note be kept on the record to indicate the disclosure?	☒	☐

Personal information contained in the MAL database is not shared with other persons or government authorities without formal approval processes being followed. Where a request is received from a government agency, procedures are in place to ensure the request is forwarded in writing, through the appropriate channels. A number of staff were questioned during the Review to confirm this process. In all cases the staff were able to confirm:

a) the procedure for actioning a request from a government official, e.g. the Australian Federal Police (i.e. request in writing, through the formal BOC channels); and

b) the requirements and processes in place to enable access to information by a non-authorised DIAC officer or contractor (i.e. no access granted).

In addition to the procedures above, there are a number of exemptions within the *Privacy Act* for disclosing of information with intelligence agencies and various sections of the Department of Defence under Section 7(1)(ee) and 7(1A). These provisions make it possible for personal information contained in MAL to be provided to specific agencies, for specific purposes (e.g. persons who are of national security concern).

As a final control, the BOC operations room in use at DIAC's national office in Belconnen is a secure room, providing access only to authorised persons. Where a non-authorised person is on the floor and may be able to hear personal information being discussed over telephones (or observe personal information on computer screens) a blue light is displayed in the work area, notifying all staff of the presence of a non-authorised visitor, and the need to be more discreet when the visitor is nearby (e.g. lower voices when speaking on the telephone to clients). This added protection assists in the prevention of unauthorised or accidental disclosure of personal information.

Personal information is used for law enforcement purposes, where information may be disclosed upon request or need, to law enforcement agencies of both the Australian Government and state and territory governments. This may include sharing of information regarding a non-citizen's criminal history or their character where they are deemed a character of concern or national security concern.

Personal information regarding non-citizen minors in the case of child custody disputes are not generally provided to agencies other than the Department of Foreign Affairs and Trade, where an ARC may be applied to an individual's record at the request of the Department. This information is not shared with other agencies.

5. Appendix 1 – Information Privacy Principles

5.1 Principle 1 - Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

   (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

5.2 Principle 2 - Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law - the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

5.3 Principle 3 - Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector:

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

5.4 Principle 4 - Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or

disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

5.5 Principle 5 - Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

   (a) whether the record-keeper has possession or control of any records that contain personal information; and

   (b) if the record-keeper has possession or control of a record that contains such information:

      (i) the nature of that information;

      (ii) the main purposes for which that information is used; and

      (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

   (a) the nature of the records of personal information kept by or on behalf of the record-keeper;

   (b) the purpose for which each type of record is kept;

   (c) the classes of individuals about whom records are kept;

   (d) the period for which each type of record is kept;

   (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

   (f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

   (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

   (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

5.6 Principle 6 - Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

5.7 Principle 7 - Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

   (a) is accurate; and

   (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

   (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

   (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

   the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

5.8 Principle 8 - Record-keeper to check accuracy etc of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

5.9 Principle 9 - Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

5.10 Principle 10 - Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

   (a) the individual concerned has consented to use of the information for that other purpose;

   (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

   (c) use of the information for that other purpose is required or authorised by or under law;

   (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

   (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

5.11 Principle 11 - Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

   (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

   (b) the individual concerned has consented to the disclosure;

   (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

   (d) the disclosure is required or authorised by or under law; or

   (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

6. Appendix 2 – Personnel Contacted

The following personnel provided assistance and information during the review:

- Gary Sheppard, Director, Border Operations Centre
- Trevor Tier, Assistant Director, Policy & Liaison, Border Operations Centre
- Chris Maclure, Acting Assistant Director, Policy & Liaison, Border Operations Centre
- Linda Rossiter, Director, FOI and Privacy Policy Section
- Barbara Bernardi, Health Alert Reason Code Owner
- Navroze Belihomji, Business Analyst, Competency Centre
- Simon Christopher, Assistant Director, Intelligence Analysis Section
- Matthew Fraser – Privacy Officer, FOI and Privacy Policy Section
- Michael Searle – Manager, Competency Centre, IT Security Section
- Andrew Muller –IT Security Analyst, IT Security Section

7. Appendix 3 – Documents Reviewed

The following documents were assessed / read during the review:

- Procedures Advice Manual – Version 3 (PAM)
- Step by Step Guide – CMAL RIF 2010 – DAL Maintenance
- Step by Step Guide – CMAL RIF 2010 – PAL Maintenance
- CMAL RIF – User Guide for ICSE Users
- CMAL Bulk Upload – External Agency User Guide
- PAL and DAL Maintenance – BOC User Guide
- DIAC (DIMIA) Privacy Impact Checklist (DRAFT)
- Monthly Client Feedback Report – February 2010. Prepared by the Client Experience, Standards and Feedback Section, Operational Performance Branch
- Form 993i – Safeguarding your personal information
- Form 815 – Health Undertaking
- Fact Sheet 77 – Movement Alert List
- Audit Report No. 35, 2009-10 "Management of the Movement Alert List", Australian National Audit Office

8. Appendix 4: Prioritisation of Findings and Recommendations

DIAC's risk management methodology was used to rate the risks identified throughout this report. The following criteria were then used to prioritise recommendations made to address these risks.

DIAC Risk Rating	Recommendation Priority	Comments
High	High	Significant system weaknesses or cases of non-compliance with prescribed procedures, which could severely compromise management control, or result in inefficient use of resources.
Significant or Moderate	Medium	System weaknesses or cases of non-compliance with prescribed procedures, which could undermine the system of management control, or result in the inefficient or ineffective use of resources.
Low	Low	System weaknesses or cases of non-compliance with prescribed procedures, which could have a minor impact on the efficiency or effectiveness of the process or use of resources. Low priority recommendations are not included in the audit report; rather they are reported separately to line management for implementation action.

9. Appendix 5: Legislation Review

The following assessment of legislation was conducted during the Privacy Impact Assessment for the Movement Alert List database at the Department of Immigration and Citizenship. This assessment was conducted to identify the relevant components of legislation that relate to privacy and the collection of personal information. Legislation assessed includes the:

- *Migration Act, 1858*
- *Australian Citizenship Act, 2007*
- *Archives Act, 1983*

For the purposes of all Acts listed below, a *personal identifier* and/or *indentifying information* is any of the following (including any of the following in digital form):

a) fingerprints or handprints of a person (including those taken using paper and ink or digital live-scanning technologies);

b) a measurement of a person's height and weight;

c) a photograph or other image of a person's face and shoulders;

d) an audio or a video recording of a person (other than a video recording under section 261AJ of the *Migration Act 1958*);

e) an iris scan;

f) a person's signature;

g) any other identifier prescribed by the regulations (except an identifier the obtaining of which would involve the carrying out of an intimate forensic procedure within the meaning of section 23WA of the *Crimes Act 1914*).

For the purposes of all Acts listed below, a document or record that is *exempt* is so if it contains any of the following:

- information or matter the disclosure of which would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person); or
- information or matter that relates to the personal affairs, or the business or professional affairs, of any person (including a deceased person).

Where a record that would otherwise be required to be made available for public access is an exempt record, agencies may, where it is reasonably practicable to do so, make arrangements for part of, or a copy of part of, that record to which access could be given without disclosing information or matter by reason of which the record is an exempt record, to be made available for public access.

Accordingly, under the *Freedom of Information Act 1982*, all documents relating to any individual are considered exempt as per the definition above. Access to such information is governed by the *Privacy Act 1988*.

Please note this document is a summary of key legislative points only, and is in no way intended to act as a complete guide to the listed legislation.

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
Legislation pertaining to collection of information	**5A Meaning of personal identifier** (2) Before the Governor-General makes regulations for the purposes of paragraph (1)(g) prescribing an identifier, the Minister must be satisfied that: a) obtaining the identifier would not involve the carrying out of an intimate forensic procedure within the meaning of section 23WA of the *Crimes Act 1914*; and b) the identifier is an image of, or a measurement or recording of, an external part of the body; and c) obtaining the identifier will promote one or more of the purposes referred to in subsection (3). (3) The purposes are: a) to assist in the identification of, and to authenticate the identity of, any person who can be required under this Act to provide a personal identifier; and b) to assist in identifying, in the future, any such person; and c) to improve the integrity of entry programs including passenger processing at Australia's border; and d) to facilitate a visa-holder's access to his or her rights under this Act or the regulations; and e) to improve the procedures for determining visa application; and f) to improve the procedures for determining claims for protection under the Refugees Convention as amended by the Refugees	**40 Request for personal identifiers** (1) For the purposes of the Minister being satisfied of the identity of: a) a person in relation to an application under this Part; or b) a person who has sought to sit a test approved in a determination under section 23A; the following persons may request the person, in writing, to provide one or more specified personal identifiers: c) the Minister; d) a person who is authorised under subsection (3); e) a person who is included in a class of persons authorised under subsection (4).	

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	Protocol; and g) to enhance the Department's ability to identify non-citizens who have a criminal history, who are of character concern or who are of national security concern; and h) to combat document and identity fraud in immigration matters; and i) to detect forum shopping by applicants for visas; and j) to ascertain whether: i. an applicant for a protection visa; or ii. an offshore entry person who makes a claim for protection under the Refugees Convention as amended by the Refugees Protocol; had sufficient opportunity to avail himself or herself of protection before arriving in Australia; and k) to complement anti-people smuggling measures; and l) to inform the governments of the identity of non-citizens who are, or are to be, removed or deported from Australia.		
Legislation pertaining to access of information	**336C Accessing identifying information** (1) A person commits an offence if: a) the person accesses identifying information; and b) the person is not authorised under section 336D to access the identifying information for the purpose for which the person accessed it.	**42 Accessing identifying information** (1) A person commits an offence if: a) the person accesses identifying information; and b) the person is not authorised under this section to access the identifying information for the purpose for which the person accessed it.	**11 Right of access** (1) Subject to this Act, every person has a legally enforceable right to obtain access in accordance with this Act to: a) a document of an agency, other than an exempt document; or b) an official document of a Minister, other than an

Please note this document is a summary of key legislative points only, and is in no way intended to act as a complete guide to the listed legislation.

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	(1A) This section does not apply if the person believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of any other person. **336D Authorising access to identifying information** (1) The Secretary may, in writing, authorise a specified person, or any person included in a specified class of persons, to access identifying information of the kind specified in the authorisation. (2) The Secretary must specify in an authorisation under this section, as the purpose or purposes for which access is authorised, one or more of the following purposes: a) one or more of the purposes set out in subsection 5A(3); b) disclosing identifying information in accordance with this Part; c) administering or managing the storage of identifying information; d) making identifying information available to the person to whom it relates; e) modifying identifying information to enable it to be matched with other identifying information; f) modifying identifying information in order to correct errors or ensure compliance with appropriate standards; g) the purposes of this Act or the regulations or of	(1A) This section does not apply if the person believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of any other person. (3) The Minister may, in writing, authorise a specified person, or any person included in a specified class of persons, to access identifying information of the kind specified in the authorisation.	exempt document. **15A Request for access to personnel records** (1) In this section *personnel records*, in relation to an employee or former employee of an agency, means those documents containing personal information about him or her that are, or have been, kept by the agency for personnel management purposes. (2) Where: a) there are established procedures in an agency (apart from those provided for by this Act) in accordance with which a request may be made by an employee of the agency for access to his or her personnel records; and b) a person who is or was an employee of the agency wishes to obtain access to his or her personnel records; the person must not apply under section 15 for access to such records unless the person: c) has made a request for access to the records in accordance with the procedures referred to in paragraph (a); and d) either: i. is not satisfied with the outcome of the request; or ii. has not been notified of the outcome within 30 days after the request was made. For the purposes of this Act, a record is in the open

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	the *Australian Citizenship Act 2007* or the regulations made under that Act; h) complying with laws of the Commonwealth or the States or Territories. (3) However, the Secretary must not specify as a purpose for which access is authorised a purpose that will include or involve the purpose of: a) investigating an offence against a law of the Commonwealth or a State or Territory; or b) prosecuting a person for such an offence; if the identifying information in question relates to a personal identifier of a prescribed type.		access period if a period of 30 years has elapsed since the end of the year ending on 31 December in which the record came into existence. For the purposes of this Act, a record containing Census information from a particular Census is in the open access period for that Census if a period of 99 years has elapsed since the Census day for that Census.
Legislation pertaining to disclosure of information	**336E Disclosing identifying information** (1) A person commits an offence if: the person's conduct causes disclosure of identifying information; and the disclosure is not a permitted disclosure. (1A) This section does not apply if the person believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of any other person. (2) A permitted disclosure is a disclosure that: a) is for the purpose of data-matching in order to: i. identify, or authenticate the identity of, a person; or ii. facilitate the processing of persons entering or	**43 Disclosing identifying information** (1) A person commits an offence if: a) the person's conduct causes disclosure of identifying information; and b) the disclosure is not a permitted disclosure. (1A) If: a) a disclosure of identifying information is made to a person who is not an entrusted person; and b) the disclosure is a permitted disclosure; this section does not apply in relation to any further disclosure of that identifying information by a person who is not an entrusted person. (1B) This section does not apply if the person believes on reasonable grounds that the disclosure is necessary to prevent or lessen a	**30A Non-disclosure of Census information** (1) An Archives officer must not, at any time before a record containing Census information from a Census is in the open access period for that Census, divulge or communicate any of that information to another person (except to another Archives officer for the purposes of, or in connection with, the performance of that other officer's duties under this Act).

Please note this document is a summary of key legislative points only, and is in no way intended to act as a complete guide to the listed legislation.

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	departing from Australia; or iii. identify non-citizens who have a criminal history, who are of character concern or who are of national security concern; or iv. combat document and identity fraud in immigration matters; or v. ascertain whether an applicant for a protection visa had sufficient opportunity to avail himself or herself of protection before arriving in Australia; or vi. inform the governments of foreign countries of the identity of non-citizens who are, or are to be, removed or deported from Australia. (Please refer to Act for full definition of permitted disclosure.) **336F Authorising disclosure of identifying information to foreign countries etc.** (1) The Secretary may, in writing, authorise a specified officer, or any officer included in a specified class of officers, to disclose identifying information of the kind specified in the authorisation to one or more of the following: a) one or more specified foreign countries; b) one or more specified bodies each of which is: i. a police force or police service of a foreign country; or ii. a law enforcement body of a foreign country (including a war crimes tribunal); or iii. a border control body of a foreign country;	serious and imminent threat to the life or health of the person or of any other person. (2) A permitted disclosure is a disclosure that: a) is for the purposes of this Act or the regulations or of the *Migration Act 1958* or the regulations made under that Act; or b) is for the purpose of administering or managing the storage of identifying information; or c) is for the purpose of making the identifying information in question available to the person to whom it relates; or d) is to an agency of the Commonwealth, a State or a Territory in order to verify that a person is an Australian citizen; or e) takes place under an arrangement entered into with the Commonwealth, a State or a Territory or an agency of the Commonwealth, a State or a Territory, for the exchange of identifying information; or f) is reasonably necessary for the enforcement of the criminal law of the Commonwealth, a State or a Territory; or g) is required by an Australian law; or h) is for the purpose of a proceeding, before a court or tribunal, relating to the person to whom the identifying information in question relates; or i) is for the purpose of an investigation by the Privacy Commissioner or the Ombudsman relating to action taken by the Department; or j) takes place with the written consent of the	

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	c) one or more specified international organisations, or specified organisations of foreign countries, that are responsible for the registration of people as part of refugee or humanitarian programs; d) one or more prescribed bodies of a foreign country, of the Commonwealth or of a State or Territory; e) one or more prescribed international organisations. (2) The Secretary must specify in the authorisation, as the purpose or purposes for which disclosure is authorised, one or more of the purposes set out in subsection 5A(3). (3) A disclosure is taken not to be authorised under this section if: a) the person to whom the identifying information relates is: i. an applicant for a protection visa; or ii. an offshore entry person who makes a claim for protection under the Refugees Convention as amended by the Refugees Protocol; and b) the disclosure is to a foreign country in respect of which the application or claim is made, or a body of such a country. (4) A disclosure is taken not to be authorised under this section if: a) the person to whom the identifying information relates is:	person to whom the identifying information in question relates.	

Please note this document is a summary of key legislative points only, and is in no way intended to act as a complete guide to the listed legislation.

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	i. an applicant for a protection visa; or ii. an offshore entry person who makes a claim for protection under the Refugees Convention as amended by the Refugees Protocol; and b) the officer making the disclosure is not reasonably satisfied that the country or body to which the disclosure is made will not disclose the identifying information to a foreign country in respect of which the application or claim is made, or a body of such a country. (5) However, if: a) the person to whom the identifying information relates has requested or agreed to return to the foreign country in respect of which the application or claim is made; or b) the person is an applicant for a protection visa, and the application has been refused and finally determined; or c) the person is an offshore entry person: i. who makes a claim for protection under the Refugees Convention as amended by the Refugees Protocol; and ii. who, following assessment of his or her claim, is found not to be a person to whom Australia owes obligations under the Refugees Convention as amended by the Refugees Protocol; then: d) subsection (3) does not apply to a disclosure to that country or to a body of that country; and		

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	e) subsection (4) does not apply to a disclosure to a body or country that may disclose the identifying information to that foreign country or to a body of that country.		
Legislation pertaining to modification of information	**336G Unauthorised modification of identifying information** (1) A person commits an offence if: a) the person causes any unauthorised modification of identifying information; and b) the person intends to cause the modification; and c) the person knows that the modification is unauthorised. **336H Unauthorised impairment of identifying information** A person commits an offence if: a) the person causes any unauthorised impairment of: b) the reliability of identifying information; or c) the security of the storage of identifying information; or d) the operation of a system by which identifying information is stored; and e) the person intends to cause the impairment; and f) the person knows that the impairment is unauthorised.	**44 Unauthorised modification or impairment of identifying information** (1) A person commits an offence if: a) the person causes any unauthorised modification of identifying information; and b) the person intends to cause the modification; and c) the person knows that the modification is unauthorised. (2) A person commits an offence if: a) the person causes any unauthorised impairment of: i. the reliability of identifying information; or ii. the security of the storage of identifying information; or iii. the operation of a system by which identifying information is stored; and b) the person intends to cause the impairment; and c) the person knows that the impairment is unauthorised.	
Legislation pertaining to	**336K Destroying identifying information**	**45 Destroying identifying information**	**24 Disposal, destruction etc. of Commonwealth**

Please note this document is a summary of key legislative points only, and is in no way intended to act as a complete guide to the listed legislation.

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
disposal of information	(1) A person commits an offence if: a) the person is the responsible person for identifying information; and b) the identifying information is not of a kind that may, under section 336L, be indefinitely retained; and c) the person fails to destroy the identifying information as soon as practicable after the person is no longer required under the *Archives Act 1983* to keep the identifying information. **336L Identifying information that may be indefinitely retained** (1) Identifying information may be indefinitely retained if the non-citizen to whom it relates: a) is, or has ever been, in immigration detention; or b) has ever had an application for a visa refused, or has ever had a visa cancelled; or c) has ever: i. entered Australia on a temporary visa; and ii. since its expiry, remained in Australia as an unlawful non-citizen; or d) has ever been convicted of an offence against this Act or the regulations; or e) has ever been subject to action taken under this Act or the regulations for the purpose of: i. deporting the non-citizen; or ii. removing the non-citizen from Australia; or	(1) A person commits an offence if: a) the person is the responsible person for identifying information; and b) the person fails to destroy the identifying information as soon as practicable after the person is no longer required under the *Archives Act 1983* to keep the identifying information. (2) This section does not apply if the identifying information is: a) a personal identifier that is any of the following: i. a measurement of a person's height and weight; ii. a photograph or other image of a person's face and shoulders; iii. a person's signature; or b) identifying information derived from or relating to such a personal identifier.	**records** (1) Subject to this Part, a person must not engage in conduct that results in: a) the destruction or other disposal of a Commonwealth record; or b) the transfer of the custody or ownership of a Commonwealth record; or c) damage to or alteration of a Commonwealth record. (2) Subsection (1) does not apply to anything done: a) as required by any law; b) with the permission of the Archives or in accordance with a practice or procedure approved by the Archives; c) in accordance with a normal administrative practice, other than a practice of a Department or authority of the Commonwealth of which the Archives has notified the Department or authority that it disapproves; or d) for the purpose of placing Commonwealth records that are not in the custody of the Commonwealth or of a Commonwealth institution in the custody of the Commonwealth or of a Commonwealth institution that is entitled to custody of the records.

Legislation	Migration Act 1958	Australian Citizenship Act 2007	Archives Act 1983
	f) is a person in respect of whom the Minister has issued a conclusive certificate under subsection (4).		

イギリス
(PIA report)

事例）

英国国境局ＰＩＡ報告書

Home Office
UK Border Agency

Report of a

PRIVACY IMPACT ASSESSMENT

conducted by the UK Border Agency

in relation to the

HIGH VALUE DATA SHARING PROTOCOL

amongst the immigration authorities of the

FIVE COUNTRY CONFERENCE

Table of Contents

1. The FCC Protocol - Introduction and overview

This Protocol will enable secure data sharing based on fingerprint checks between the UK Border Agency and its partners in the Five Country Conference (FCC) - the immigration authorities of Australia, Canada, New Zealand and the United States of America:

- the Department of Immigration and Citizenship (DIAC) in Australia;
- Citizenship and Immigration Canada (CIC) and the Canada Border Services Agency (CBSA);
- the Department of Homeland Security (DHS) in the United States of America;
- and Immigration New Zealand (INZ).

The FCC countries are bound together by many historical ties and a common language. Data sharing trials have shown they also share many common patterns of both regular and irregular migration, and that proportionate and targeted data sharing activity between the FCC countries to improve the effectiveness of our border and immigration management systems would provide real benefits to our citizens. This Protocol is a next step in this activity, which is in addition to and complements the existing procedures for data sharing which the UK conducts with its European partners.

Under this Protocol, each FCC country will securely and confidentially check an agreed volume (initially 3,000 per year) of fingerprint sets of immigration cases against relevant fingerprint databases of the other FCC countries. Each country will decide which of its immigration cases it will check under the Protocol, to derive best value. The UK Border Agency intends to use the Protocol primarily to check asylum cases where there is good reason to do so – for example, if the person cannot be identified or there is reason to believe the person may be known to another FCC country – and those foreign national criminals who are difficult to remove from the UK due to identity and documentation issues.

Fingerprints exchanged under the Protocol will be destroyed securely once the matching has taken place, and used for no other purpose. On cases where fingerprints are found to match, the countries will exchange such other information as is relevant, proportionate and lawful to exchange for their immigration and nationality purposes.

This will support the process of immigration control and provide benefits both to genuine applicants and to the UK public. Information from fingerprint matching assists the genuine applicant by helping to confirm his or her account, whilst protecting the public by identifying and assisting with removal from the UK of false applicants and people who pose a risk.

The information will be shared securely via a Secure File Share Server (SFSS) hosted by the government of Australia.

The UK Border Agency has decided to publish this Privacy Impact Assessment (PIA) report after considering the recommendations of the Cabinet Office Data Handling Review and having received advice from the Information Commissioner's Office, the Ministry of Justice, and other interested parties.

2. What is this document for?

2.1 What is a Privacy Impact Assessment (PIA)?

Projects that involve exchanging personal information inevitably give rise to privacy concerns. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and government agencies alike. Privacy Impact Assessment (PIA) is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that we can foresee problems, develop solutions, and ensure that concerns are addressed appropriately. For this reason we have followed a PIA process whilst developing the arrangements for the FCC Data Sharing Protocol.

2.2 What does this PIA report cover?

This report sets out how the arrangements for the Protocol will operate, and how its operation can be expected to relate to the privacy of the individuals whose information is exchanged. This includes assessment of the arrangements for the central server through which the information will be exchanged, of the arrangements which each of the participating countries has put in place internally for processing the information, and of the overall adequacy of the data protection arrangements.

A previous version of this report was published on initial implementation of the Protocol between Australia, Canada and the United Kingdom. A second version was published on implementation of the Protocol with the US and this final version has been updated to reflect forthcoming implementation by New Zealand.

2.3 How have we conducted the PIA?

We have sought to examine the arrangements both objectively and from the point of view of the individual, to ensure that we meet the legitimate expectations of people whose information is exchanged.

In assessing the impacts and developing the arrangements, we have been informed by previous trial activities, and by the responses of people whose information has been shared in those trials. We have consulted a number of interested parties, in particular the Information Commissioner's Office, whose guidance has been extremely helpful, as has the assistance of the Ministry of

Justice. Our colleagues in the other FCC countries have also been assessing the privacy impacts of the arrangements, and we have worked closely together in developing them.

The arrangements reflected in this report are the fruits of these processes. We have found these processes useful to follow, and believe that the arrangements that we have put in place for the FCC Protocol demonstrate good practice in data sharing and protection, striking a fair balance between protecting the privacy rights of the individual and the interests of the wider public.

2.4 What type of PIA have we conducted?

The PIA process is relatively new in the UK. To date, it has largely been used in connection with new projects to collect and store personal information. We are not aware of its previous use in the UK in relation to international information exchange projects of this kind, where many of the privacy issues and risks manifest themselves in different ways than they do in projects related to new databases. We have therefore followed the general guidance of the Information Commissioner's Office in undertaking this process, and sought specific advice on how it can best be applied to this type of project. We hope this report reflects that this process has been effective.

In deciding whether to conduct a PIA, and what type of PIA to conduct, we considered carefully the nature and scope of the FCC Protocol proposition, and its potential to impact on the privacy rights of the individual, in particular that:

- the project does not involve the introduction of new legislation, or present a new policy area. Concepts and practices of data sharing based on fingerprint checks for immigration functions are already well advanced in other contexts, for example across Europe through the Eurodac system. However, whilst this project largely builds on such initiatives, it does contain new features, whose privacy impacts need to be understood and any adverse impacts minimised;
- the project does not involve collecting or storing new data from individuals, but it does involve new arrangements for exchanging personal data (including some sensitive personal data) with authorities of different countries. The ability of Her Majesty's Government to control the use of that data may therefore be diminished, or at least perceived to be diminished;
- the data will be used for limited purposes that are already well established, namely immigration and nationality purposes, which are generally the same as or similar to the purposes for which the data was originally collected. Nevertheless, these purposes involve inherent sensitivities;
- the project involves data sharing on a case by case basis, based on anonymised fingerprint matching, rather than bulk data exchange;
- the other countries with which data will be shared are outside the EEA and therefore not bound by European data protection legislation. It is therefore

important to find other ways to ensure that the rights and freedoms of data subjects are respected; and

- each of the countries participating in the project has committed to developing clear arrangements for how it will operate and how privacy risks will be minimised, with the guidance of privacy experts in each country. Having such arrangements in place should in itself be a major factor in mitigating the privacy risks, and the PIA process should help make sure they do so.

On the basis of our assessment and advice received, we decided to follow a small scale PIA process for the FCC Protocol arrangements. This is because the project had privacy issues associated with it, but not the large inherent risks that would warrant a full scale PIA, for example those typically associated with new policy areas, major new databases, or using data collected in connection with one purpose for very different purposes. Nevertheless, we found that a substantial range of issues emerged, and we expanded our approach to ensure that those issues were all addressed appropriately.

2.5 Is this report the end of the PIA process?

No. We decided to publish this report on the UK Border Agency website in order to increase transparency and public understanding of this activity. We would also appreciate any comments readers may have, either on the FCC Protocol itself or on the extent to which this document achieves its purpose. In particular, any suggestions on how we could improve our approach in future would be most welcome.

We and our FCC partners will closely monitor and review the Protocol's operation, including ongoing review of the privacy impacts, and monitoring compliance with the specific privacy and security arrangements. This will help us ensure that the Protocol continues to support the process of immigration control and provides benefits both to genuine applicants and to the public which outweigh any adverse impact on the privacy of individuals. Feedback would assist the review process. We will update this document, and publish updated versions, to reflect future developments.

3. What is the Five Country Conference Protocol for?

3.1 The immigration context

Immigration is one of the top concerns of the public in the United Kingdom. In some polls, it has been the number one issue, higher than the economy, and law and order. Two thirds of UK adults say that laws on immigration should be much tougher and nearly half say their biggest concern is pressure on public services and jobs. However, the public also want a system that meets the country's needs

for migration, and is compassionate to those who need our protection. The UK Border Agency is responsible for pursuing and balancing these objectives.

An important aspect of this task relates to identity management of foreign nationals coming to the UK. The public are heavily reliant on the UK Border Agency to ensure that the people who come into the UK are who they claim to be, and can readily be identified as such. This is important not just in immigration terms, but to protect the public and their services against all kinds of risk. We have deployed a wide range of capabilities to help us do this, such as the biometric visas we now issue globally.

The UK has one of the strongest immigration controls in the world. Nevertheless, as with all other countries, the international nature of migration and absence of globally joined-up solutions mean that some of our functions within the UK are exercised without having the sorts of information that we would require from an overseas applicant. In particular, within the asylum and enforcement processes we regularly encounter people who are unable to substantiate their claimed identity or account, for which we may have no previous record to check.

This presents serious issues both for the individual and the public. Asylum seekers in genuine need of protection would benefit from an enhanced ability to verify their credentials. Equally, there are strong public protection reasons for wanting to enhance our ability to identify claims that are fraudulent, or applicants who are not who they say they are. And the unsuccessful claimants who are presently difficult to remove from the UK because we do not know who they are or, sometimes, even to which country we should be removing them, will be able to be processed far more effectively with the aid of international capabilities to verify their identities.

3.2 Five Country Conference activity

These issues can only be addressed internationally. As well as working with European partners, we have been working with our FCC partners to scope the issues and to develop proportionate solutions. FCC data sharing trials, based on exchanging biometrics in an effectively anonymous manner, and then sharing data on the cases where biometric matches are achieved, have shown that substantial opportunities exist to improve our abilities to address the patterns both of legal and illegal migration that affect our countries.

Checks on visa applicants have shown largely compliant patterns of behaviour within this population. However, trials with asylum and enforcement populations have consistently shown high levels of abuse as well as legitimate activity. For example, fingerprint checks of 30,000 UK asylum cases against US Department of Homeland Security data provided fingerprint matches on 429 cases (1.43%), and high value findings on the great majority of these. 63% of cases had given a

different identity to the UK than the identity known to the US. 29% of cases also presented a different nationality. The US was able to supply a verifiable identity for 63% of cases which could (if appropriate) be used to re-document and return the person to country of origin. 89% of matching cases that were claiming asylum as unaccompanied children had given details to the US indicating they were adults. There were also many other relevant findings, such as whether the whereabouts of a person when fingerprinted by the US authorities tallied with their claim.

The proportion of cases which achieve a fingerprint match varies between countries and increases over time. For example, whilst the above trial achieved a 1.43% match rate overall, the more recent cases within it achieved a match rate of around 3%, and another trial of searching Canadian asylum fingerprints against the UK system achieved a match rate of 3.5%. Checking fingerprints across the FCC countries via the Protocol will provide a higher combined match rate, which will also increase over time alongside the expansion of immigration fingerprint holdings.

It should be stressed that the figures from the example trial above relate to asylum and enforcement cases where fingerprint matches were achieved between the UK and US, that is to say, they were known to both countries. These are not representative of asylum and enforcement cases more generally, not least because the people concerned predominantly have travelled by air between continents - a very different pattern to those who migrate through Europe by land and sea. The capabilities we are developing across the FCC are complementary to and a logical extension of the checks we already conduct with our European partners.

These findings also reflect opportunities presented by recent capability advances: for example, collecting fingerprints of asylum seekers has been well established for some years, but the ability to use these to establish a true identity rests on cross-checking with more recent advances such as biometric visas, as people will have produced their passports in connection with their visa transactions.

3.3 The Protocol as next step

This Protocol is a next step in FCC activity. It will enable each country to check 3,000 sets of anonymised fingerprints per year against the other FCC countries, and share appropriate data on matching cases, for use for immigration and nationality purposes. The data will be shared via a fully accredited Secure File Share Server hosted by Australia. As fingerprints will be checked on a request basis, each country will (within parameters) decide which of its cases to check, thus obviating the need to check bulk samples and enabling each to derive best proportionate value.

In the UK we intend to derive best value by using the Protocol primarily for asylum cases where there is good reason to do so – for example, reason to believe the person may be known to another FCC country – and for foreign national criminals who are difficult to remove due to identity and documentation issues. We expect to derive the following direct benefits for data subjects and the UK public:

- better informed decision making, hence greater confidence that genuine applicants who need our protection will be successful whilst fraudulent applicants will be refused;
- increased ability to remove foreign criminals and failed asylum seekers from the UK, by linking them to their true identities and travel documents;
- harm reduction by identifying and enabling action on cases that present risks to the public, such as through identity fraud or where they are known to be dangerous criminals;
- savings to the UK taxpayer, by ending expenditure on people who consequently leave the UK and by withdrawing public services from people who are not entitled to them. This includes for example costs of foreign criminals in British prisons, asylum support costs, and NHS costs of those who falsely claim asylum to access free NHS treatment; and
- improved child protection, for example by validating the ages and identities of those seeking to access UK child care services.

The Protocol will deliver specific benefits both to the genuine applicant and to the public. Information from fingerprint matching that is consistent with a person's account is seen as supporting evidence for their claim, thereby assisting the genuine applicant, whilst information that contradicts their account needs explanation. The UK Border Agency believes that the Protocol represents a proportionate step, which is necessary in view of pressing social needs and strikes an appropriate balance between safeguarding the private lives of the individuals concerned, protecting the public and meeting public expectations.

Whilst operating the Protocol we will also continue to develop more systematic solutions for the longer term. Each of the FCC countries is implementing biometric immigration capabilities, but we are at different stages in rolling these out. The Protocol provides a flexible arrangement by which we can derive good value for each of our countries during that rollout. Once there is greater consistency in our biometric capabilities we intend to implement arrangements for systematic biometric checks of appropriate immigration cases across the FCC countries.

4. What does the FCC Protocol involve?

4.1 The data sharing conundrum

People are naturally concerned to ensure that there is an appropriate balance between the individual's right to privacy and the state's need to share data in order to carry out its functions effectively. People often have very different perspectives on where this balance should lie. Whilst the great majority of people agree that government agencies should share relevant data to an extent that is necessary and proportionate for their purposes – which is also the basic essence of UK data protection law – what this extent actually is in practical terms is often hotly debated. In many ways this is because of the effect of what we might call the 'data sharing conundrum':

"Government agencies should share data that is relevant to their purposes. However, it is impossible for them to tell what data will turn out to be relevant, until they have shared it. What then, should they do?"

Data sharing initiatives can therefore involve sharing a relatively substantial amount of data in order to find relevant nuggets within. Whether the data sharing is seen as justifiable is likely to depend on how many, and how valuable, those nuggets are, in comparison with the totality of the data sharing. The broader the data sharing, the more intrusive people will find it to be and the more value they will expect it to provide before they consider it to be justified. It is therefore important for Government agencies to ensure they target their activities to derive the maximum benefit for the public from the minimum data sharing, as a matter of public trust as well as legality.

4.2 What approach have we taken in the FCC Protocol?

In developing the FCC Protocol, we and our partners were anxious to ensure that our approach to the 'data sharing conundrum' provided greatest benefit for our immigration controls with minimum intrusion. We examined on all levels how this could be done, and arrived at the following proposition:

- the Protocol will be used only to check immigration cases of types which present the highest value in doing so, in particular asylum and enforcement cases, and will not be used to check nationals of the UK or other FCC countries (see section 4.3);
- checks will be based on nigh anonymised fingerprint matching, so that otherwise identifiable data is only shared on cases where fingerprint matches occur, between the two countries that have a legitimate interest in the individual (see section 4.4);
- on the cases where matches do occur, a Search Code Guide will be used to identify data for sharing only to the extent that is necessary for the specific type of case (see section 4.5); and

- checks will only be made against relevant databases of the other countries (see section 4.6).

We believe this multi-layered approach ensures as far as possible that data will only be shared where it is directly relevant to the case in question.

4.3 Whose information will be exchanged?

The Protocol will enable the immigration authorities of each FCC country to check the fingerprints of up to 3,000 immigration cases per year against the fingerprint systems of the other FCC countries. The countries may over time agree to increase the volume of fingerprint checks. Each country will decide which of its immigration cases to check using the Protocol, in order to derive best value from the arrangement. The arrangements provide that these cases are likely to include, but not limited to:

- immigration cases with an indication of derogatory activity or other associations of concern such that the person would be inadmissible to one or more of the FCC countries;
- immigration cases where the identity of the individual is unknown or uncertain;
- immigration cases where there is reason to believe that the person has been encountered by another of the FCC countries; and
- other sensitive immigration cases.

Each country has considered which types of case it intends to check using the Protocol. The UK Border Agency considers that we will derive best value for the public by using 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 presently practicable because we cannot sufficiently confirm their identity and/or nationality. Where another FCC country is able to confirm this, it will help enable us to arrange the person's re-documentation and return to country of nationality; and
- asylum seekers, where there is a particular reason to do so, for example because the person's identity is in question, or because the person is believed to have been known to other FCC countries. This will help to confirm or deny the person's claim and, where their claim is unsuccessful, to re-document and return the person to the country of nationality.

The other FCC countries intend to use the Protocol to check similar types of case in the first instance. There will also be other scenarios where there is good reason to use the Protocol. Each FCC country seeks to derive maximum value from the Protocol, and will therefore use it to check the cases which present greatest proportionate value. This has been informed by the trials we have undertaken, and we will develop our approach according to our experience of using the Protocol. However, we have also built in safeguards to ensure that

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 (see above);
- the purposes for which shared data may be used, and the extent to which it may further be disclosed, are defined (see section 5); and
- the data that may be shared is defined (see section 4.5) to ensure that it does not go beyond what is relevant and proportionate for those purposes.

4.3.1 Will we use the Protocol to check our own citizens?

We have also agreed that the fingerprints exchanged for searching under the Protocol will **not** contain fingerprint data of known FCC nationals. Thus a national of the UK or another FCC country, who does not purport to be otherwise, may be assured that his or her fingerprints will not be searched under this arrangement. The only scenario in which the fingerprints of a FCC national may be searched under the Protocol is where that person is purporting not to be a FCC national. For example, one person whose fingerprints we exchanged during trials because he was claiming asylum in the UK as a Somali, was found to be an Australian citizen, who was wanted in Australia for rape. Identifying this enabled the UK Border Agency to resolve his asylum claim and return him to Australia. This is appropriate activity for immigration purposes.

In the case of the UK, this also means that we will not search fingerprints of known EEA nationals or their family members, who have free movement in the EEA and we would not therefore have an immigration reason to check their fingerprints outside the EEA.

4.4 How will the information be exchanged?

All of the data exchange will be conducted securely through a Secure File Share Server (SFSS). The arrangements for this are set out further in section 7.1 of this paper.

The data exchange will happen in two stages. In the **First Stage** nigh anonymised fingerprints will be transferred for the purpose of searching against the other countries' fingerprint databases. Only in the instance of a fingerprint 'match' being identified will the **Second Stage** data sharing take place, transferring biographical and other relevant data between the country that supplied the fingerprints and the country that identified a fingerprint match. Thus the first stage represents the effectively anonymous checking of fingerprints between the two countries, and the second stage applies to those cases where this yields fingerprint matches, that is to say, those cases which are already known to and whose fingerprints are held by both countries.

The **First Stage** of the intended transfer data will involve transferring nigh anonymised fingerprints. By 'nigh anonymised', we mean that whilst the

fingerprints do in themselves constitute personal data, and it is right to protect them as such, they are shared with no biographical data attached, and therefore it could not readily be ascertained to whom they relate. The fingerprints will be transmitted accompanied only by:

- a unique reference number, which in the case of UK fingerprints will be allocated as part of the exercise and only be identifiable to the UK Border Agency officials administering the Protocol. This is in order to be able to identify the cases on which fingerprint matches are achieved; and
- a search code to indicate the type of case to which the fingerprints relate, for example, an asylum seeker or foreign national prisoner. As different types of data are relevant to be transferred in different types of case, the search code is to enable a country that obtains a fingerprint match to ascertain what data will be relevant to transfer (in the second stage) in respect of that person.

A person whose fingerprints are checked through the Protocol may be assured that this does not present any significant risk to his or her rights and freedoms. The arrangements provide that:

- the fingerprints will be transferred securely in a nigh anonymous manner;
- the fingerprints will only be used for the purposes of matching against the relevant databases, and for notifying the supplying country of the result;
- the matching will be done and results notified within three days wherever possible; and
- the fingerprints will securely be destroyed as soon as the matching has been carried out (whether or not a match is achieved).

Thus the country which has received the fingerprints will not retain or use them for any purpose of its own. Where a country achieving a fingerprint match has itself a legitimate purpose connected with the fingerprint match, this will be considered in the second stage of data sharing, rather than by retaining or otherwise using the fingerprints.

Even in the unlikely event that the fingerprints were obtained by an unauthorised person, it is highly unlikely that the data subject would suffer any adverse consequences, as an unauthorised person would only be able to identify the data subject in the event that they themselves had access to a fingerprint database which already contained the person's details.

4.5 What information will be exchanged?

Where a fingerprint 'match' is identified, the **Second Stage** of the process involves the two countries concerned sharing relevant biographical and other data on a bilateral basis. Certain information will be shared as a matter of course, as it will always be relevant, whilst further information sharing will depend on the nature of the case.

The data elements that will be shared as a matter of course on matching cases (to the extent that they are available within the relevant country's biometric system), are:

- Date, location and reason fingerprinted
- Last name, first name, any other names
- Date of birth, place of birth, nationality and gender
- Travel document number
- Photograph, facial image, and/or scan of the travel document biodata page

These data elements provide information about the **identity** presented by the person and the **transaction** in which it was presented. Both countries concerned need the identity data to establish whether the person has presented the same identity to both countries. If the identity held by both countries is the same, this serves to add assurance that the person is who he or she claims to be. If different, the countries will need to consider what action or conclusions should flow from the discrepancy (for example, how to establish whether either or both of the identities is genuine). The transaction information is important in determining the level of assurance that may be attached to an identity, as, for example, identities presented by people bearing their passports whilst applying for visas will carry more assurance than identities presented in transactions which only reflect who the subject claimed to be at the time.

The countries concerned will share additional data, where appropriate, in accordance with an agreed Search Code Guide (SCG), which will specify what additional data (if any) will be shared as a matter of course. As different types of data are relevant in different types of case, the SCG assists in ascertaining what data will be relevant to transfer in any given case, according to the search code that was originally sent with the fingerprint searching request, and the nature of the information held by the country that identified the fingerprint match. This enables more effective and efficient data sharing.

The SCG also helps ensure that the data shared will be relevant and proportionate to the legitimate use, as the data sharing will focus only on those data elements that are pertinent to the specific type of case. For example, on types of case where the purpose of the check is purely to obtain the person's identity and passport details, the SCG sets out that no further data needs to be exchanged beyond these items. There are other types of case where the

person's history or current location needs to be confirmed, and the SCG sets these out.

Either country may also request additional information from the other on a case by case basis, and will provide sufficient reasons for such requests to enable the other country to determine the legality of disclosing such further information. In the case of the UK, we will only share such further information where we are satisfied from the reason given for the request that the further data transfer is proportionate and lawful. Information may only be exchanged to the extent that is relevant and proportionate to the countries' immigration and nationality purposes. These purposes are set out further in section 5 of this paper.

4.6 What databases will people be checked against?

The fingerprints that are exchanged will be searched securely against the other countries' biometric databases that are relevant to immigration purposes. These are:

- the Immigration and Asylum Fingerprint System (IAFS) in the UK, which is administered by the UK Border Agency;
- the Biometric Acquisition and Matching System (BAMS), in Australia, which is administered by the Department of Immigration and Citizenship;
- the Automated Fingerprint Identification System (AFIS) in Canada, which is administered by the Royal Canadian Mounted Police for their own purposes and on behalf of Citizenship and Immigration Canada and the Canada Border Services Agency
- the IDENT System in the USA, which is administered by the Department of Homeland Security; and
- the Immigration Biometric System (IBS), which is administered by the Department of Labour New Zealand

Some of these systems include both immigration and policing entries. The data that will be shared, however, will only be data that is relevant and lawful to exchange for immigration and nationality purposes, as set out in section 4.5. Each country is responsible for ensuring that the records it searches, and the information it discloses, supports this construction.

4.7 How will we know the information is accurate?

Each of the countries' fingerprint matching systems operates to a high degree of assurance. Potential matches are identified by the fingerprint systems and verified by appropriately qualified fingerprint examiners. In some systems, all potential matches are manually examined, whilst others differentiate between 100% certain automated matches that do not need further verification and less certain ones that are then manually examined. The outputs are acceptable as evidence in each of the countries' domestic courts up to and including the level of

proof required in criminal cases, a higher benchmark than generally operates in immigration matters. The accuracy of fingerprint matching has been the subject of much study which is freely available, and which we have not sought to replicate in this document.

There remain some issues about varying standards in different countries, and about the ability of an authority in one country to evidence a fingerprint match for the purposes of an authority in another country. For this reason, in the event that a fingerprint match is disputed, the fingerprints held on the database of the country which confirmed the match will be supplied to the other country, whose own fingerprint experts will re-examine both sets of fingerprints. Thus a person whose immigration case is being dealt with in the UK need not fear that he or she may be affected by a false fingerprint match provided by another country, which could not then be subject to scrutiny. Both sets of fingerprints would be available in the UK, the fingerprint match examined by a UK qualified examiner, and the fingerprint match and any conclusions following from it would be subject to the requirements of UK law.

There are some risks around the accuracy of the biographic information exchange on the cases where biometric matches are identified:

- data may be inaccurate because of errors in the source database;
- data may be inaccurate because it has been incorrectly transcribed; or
- data may be incorrectly interpreted by the country receiving it.

In trials, we have sought the best ways to mitigate these risks, and reflected these in the Protocol arrangements:

- each country will provide the other countries with an Interpretation Guide which explains how to interpret the information it will be sharing, including, for example, any quirks of its biometric system which need to understood by the other countries;
- all of the data exchange will in each country be handled by a central team, trained both on how to provide information to the other countries in a readily understandable form, and on how to interpret the information provided by other countries;
- the information which is exchanged on all matching cases will wherever possible be produced automatically from the relevant country's biometric database. This is information that has been captured during a fingerprinting encounter, whose accuracy and interpretation will be readily understandable from the information and the guidance from the country concerned. This further mitigates the risks to the accuracy of the information pertaining to the biometric encounter;
- other information to be exchanged in accordance with the Search Code Guide will be provided in an agreed and understood format. It will be restricted to clear, factual information and will not include any subjective

information that is liable to misinterpretation, such as the opinions of an immigration officer that had dealt with the case;

- 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. This will be the same procedure that will ensure that such sharing is proportionate and lawful; and
- the arrangements provide for co-operation between the different countries' central teams to liaise and correct any data that is found to be inaccurate.

4.7.1 Can I see and if necessary correct any information held about me?

It is important for the fair processing of people's information and for public trust that there is transparency in the arrangements. Whilst we have taken a range of steps to ensure that the data shared is accurate and is correctly understood, there always remains some level of accuracy risk. However, we have confirmed in our assessment of the other countries' data protection arrangements (see section 6.3) that each provides individuals with adequate rights to access information which is held on them, to correct any erroneous information, and for the opportunity to seek redress against breaches of the law. We have also specifically set out that no data may be exchanged under the Protocol which may not be disclosed to the individual to whom it relates.

Any issues concerning personal data provided by the UK to the other countries would also be actionable through the UK Border Agency under the Data Protection Act 1998.

The Protocol further supports our duty under the fourth data protection principle in the Data Protection Act 1998 to ensure that data is kept accurate and up to date. Checks made under the Protocol will help us to correct and update our systems. For example, where they show that an immigration offender believed to be in the UK is now elsewhere, we will be able to update our records accordingly.

5. How will we use the information that has been exchanged?

How information will be used is of as much legitimate concern to the public as how it will be collected, stored and exchanged. People naturally do not like to find that information about themselves which they have provided for one purpose then gets used for a very different purpose. In developing the FCC Protocol we were anxious to ensure that the information shared under it could only be used for our and our partners' proper purposes, as the immigration authorities of the FCC countries.

However, we also considered it necessary to ensure that we did not prevent ourselves from acting on the information in any of the ways that the public would rightfully expect. Wherever data that is shared indicates a need to take action in

line with our proper purposes and in the public interest, we need to be able to take that action. Precluding ourselves from taking proper and necessary action would be as great a disservice to the public as not having the information in the first place.

The remainder of this section explores how we have reconciled these objectives in the Protocol arrangements.

5.1 For what purposes will the information be used?

The fingerprints exchanged in the first stage of the process will only be used for the purposes of matching against the relevant databases, and for notifying the supplying country of the result, and for no other purpose. The information that is shared in the second stage of the process on the cases where fingerprint matches are achieved may then be used for any of the immigration and nationality purposes of the relevant FCC country.

'Immigration and nationality purposes' are defined in this context as '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.

These provisions are designed to allow only appropriate use of the information by each FCC country's immigration authorities, including assisting them to make accurate and informed casework decisions, and to remove unsuccessful applicants to their countries of origin.

The information that is shared in the second stage may also be used for determining the person's eligibility for public benefits or services which are connected with his or her immigration status. Thus if the information received indicated that a person who was being accommodated and supported by the UK Border Agency was not entitled to that support, we could act on that information to end such support. For example, trial exercises showed that several people who were claiming asylum and asylum support, had previously been granted asylum and citizenship by other European countries, but were fraudulently claiming in the UK as being their original nationality. The information was used successfully to end that support.

However, access to benefits and services would not in itself be a reason to check fingerprints through the Protocol. Fingerprints will only be checked through the Protocol for direct immigration and nationality purposes. Use of information received in relation to immigration-related benefits and services will occur where this is a necessary consequence in view of the information received.

5.1.1 Use in judicial proceedings

All of the relevant functions are potentially subject to judicial scrutiny in some form. For example, asylum decisions made by the UK Border Agency are appealable to the Asylum & Immigration Tribunal and further to the higher Courts. The Protocol arrangements explicitly provide for disclosure of the information shared in relevant judicial proceedings. Judicial scrutiny provides a fundamental safeguard for people's rights and freedoms in immigration matters. If any of the authorities using the Protocol made a wrong decision about a person based on information that had been shared – whether because the information itself was wrong, or a wrong conclusion had been drawn from it – the person affected would have the ability to challenge this in the Courts.

5.1.2 Use to verify identity and return to country of origin

Where identity and/or identity document information exchanged under the Protocol indicates that a person may be a national of, or have status in, a particular country, that information may also be disclosed to the relevant authorities of that country, for the purposes of verifying the person's true identity, establishing the provenance of the identity documents, and/or in connection with re-documenting and returning the person to that country.

For example, if a fingerprint match shows that a person claiming to be a national of country X was using a passport issued by country Y when he or she was encountered by another FCC country, it may be necessary to contact the authorities of country Y:

- to verify whether they genuinely issued the passport to that person, who is one of their citizens (as opposed to it being either a false document, or one that was issued to someone else), and
- if the person is confirmed as a citizen of country Y, to arrange new travel documentation for his or her return there.

Such disclosure is part of normal immigration processing. Using identity and travel document details which have been obtained from another FCC country for this purpose presents no more risk to the rights and freedoms of data subjects than disclosing similar details provided by the data subject, or obtained from another source. Therefore in this process the FCC countries will apply the same safeguards to the shared information as they do with other information used for these purposes. However, for additional clarity we have agreed two explicit restrictions on such use of the shared data:

- like other data shared under the Protocol, any such disclosure is subject to the appropriate human rights and other protection considerations (see section 5.4.1); and
- only identity and/or identity document information may be disclosed under this provision, and not other forms of information – such as about a person's

behaviour. Thus whilst a person who has concealed his true identity in order to avoid being returned to his home country can expect that identity, once uncovered, to be used for that purpose, this will not result in his home country finding out other information, which might potentially be more sensitive.

5.2 What organisations may use the information?

The full range of immigration and nationality functions are not carried out by a single agency in each of the FCC countries. For example, in Canada the main functions are divided between the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC). There are also circumstances where an immigration function may fall to a different authority – for example in the UK, the police may investigate and the Crown Prosecution Service may prosecute an immigration crime, and they would clearly need the relevant information to do so. The Protocol therefore provides that the authority receiving the information may disclose it to other appropriate domestic authorities that are responsible for pursuing immigration and nationality purposes. However, we have agreed some further safeguards to ensure that the need to share the data domestically will not provide a gateway for inappropriate disclosure or use:

- the data will only be shared for immigration and nationality purposes, and where necessary for the consequential immigration–related benefits and services adjudication (see section 5.1);
- the data will thus be shared only to the extent that the other authority has a need to know in order to carry out its official duties. For example, whilst information relating to a particular immigration crime being investigated by UK police may be communicated to them, data received under the Protocol more generally would not; and
- wherever one of the participants in the Protocol does share data with another authority, they will ensure that authority applies an equivalent level of protection to the information, and limitations on its use and disclosure.

5.3 Data exchange across the FCC countries

The Protocol provides that the information may only be shared between the country that requested the search and the country that confirmed the fingerprint match. It may not be shared across the other FCC countries. There may be occasions where multiple countries confirm fingerprint matches in relation to the same person. In such cases, the fact that there is a multiple match will be notified across the countries concerned, which will then arrange any necessary exchange of personal data on a bilateral basis. The exchange of personal data will thus be limited to the countries that have a legitimate interest in the individual.

5.3.1 Limitations on the above use and disclosure – protection of the data subject

All of the FCC countries are committed to protecting the human rights of data subjects, and to various international instruments which seek to protect those rights, specifically, the 1951 Convention relating to the Status of Refugees, its 1967 Protocol, the Convention Against Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment and, in the case of the UK, the European Convention on Human Rights. Each FCC country has existing arrangements in place to prevent information being processed in ways which could lead to a person being persecuted.

For the avoidance of doubt, the arrangements for the Protocol also expressly prohibit the countries from exchanging, using or disclosing any of the information in any way such that the information could become known to any government, authority or person from which the subject of the information is seeking or has been granted protection under one of those instruments, or under their domestic laws implementing those instruments, or in any circumstances where, by virtue of the government, authority or person becoming aware of such information, the subject of the information may become eligible for such protection.

A person whose data is checked through the Protocol may therefore be assured that this will not enable his or her information to be communicated to any party from which he or she has a legitimate reason to fear persecution. This also means that, in the rare event where an issue of persecution by one of the FCC countries may arise, the person may be assured that the Protocol would not be used to check that person with the FCC country in question.

5.3.2 Limitations on the above use and disclosure – stipulation by providing country

Cases may arise where the country providing the information may not be able to allow its full use as set out above. This may arise, for example, where some of the information has been collected by another government agency and its further use is subject to the permission of that agency, or it has been collected in circumstances or for purposes with which the above uses would not be fully consistent.

For this reason, under the Protocol a country may in any case attach additional restrictions on the use or disclosure of information that it exchanges, which will be complied with by the country receiving the information.

The explicit exception to this is the area of subject access rights. A country may not attach a restriction preventing the information being disclosed to the person to whom it relates. A person may therefore be assured that his or her information will not be exchanged in a way that prevents him or her being able to see that

information in accordance with the subject access provisions of the relevant countries' laws. Further information on the rights of people whose data is exchanged is set out in section 9 of this paper.

5.4 Further use and disclosure

We have set out above the ways in which the information exchanged may, as a matter of course, be used or disclosed. No further disclosure or use of the information for any other purpose or to any other person may take place without the prior written approval of the country that supplied the information. In the case of the UK, we would not agree to such further use or disclosure unless we were satisfied that the proposed disclosure or use was lawful, and was consistent with the rights and freedoms of the data subject.

6. What is the legal basis for the information exchange?

This section summarises the legal basis for the FCC Protocol, including how the arrangements have been set out and agreed across the FCC countries, how the data sharing complies with UK law, and our assessment of why the data protection arrangements in the other participating countries are adequate.

6.1 How are the Protocol arrangements set out between the FCC countries?

The arrangements for the Protocol are set out in Memoranda of Understanding (MoUs) agreed between each pair of participating countries, supported by a suite of agreed business documents which relate to the practical arrangements for how it will operate. Wherever we refer to 'the arrangements for the Protocol' this means the terms and provisions set out in those documents, which are reflected in this report. The suite of documents currently includes:

- bilateral MoUs between each pair of participants, presently being Australia, Canada, the US, New Zealand and the UK's immigration authorities, setting out the general Protocol provisions;
- a Service Arrangement between Australia and the other countries which sets out how the central SFSS will be managed (section 7 explains);
- a Search Code Guide which sets out what information is appropriate to be shared according to the type of case (section 4.5 explains); and
- an Interpretation Guide from each country which explains how to interpret the information shared by that country (section 4.7 explains).

Although each participating country has its own systems and processes, we have agreed a consistent approach to the Protocol by which we can be confident that each participating country will operate it as is reflected in this report and the separate privacy documents which the other countries have produced in accordance with their particular requirements.

Although these documents are not legally binding, we can reasonably expect the Australian, Canadian, New Zealand and US governments to honour these arrangements in view of all the circumstances, and in particular, their stability and integrity, their close relationship with the United Kingdom individually and collectively, and our mutual interest in successful operation of the Protocol, which will be of benefit to each of our countries.

6.2 How is the FCC Protocol compliant with UK law?

There is no single source of law that determines when and how the UK Border Agency can share and use personal data. The principal considerations are:

- the UK Border Agency needs to have the power to share the data, either under statute or common law, and not be precluded from doing so by any other legislation or international obligation;
- the data sharing also needs to fulfil each of the following requirements:
  - comply with, or be exempt from, each of the eight data protection principles set out in the Data Protection Act 1998 (DPA);
  - comply with the Human Rights Act 1998 (HRA) and other human rights obligations; and
  - be consistent with our duty of confidence under common law.

6.2.1 What power does the UK Border Agency have to share the information?

As an agency of a government department headed by a Minister of the Crown, the UK Border Agency has broad common law powers to share data in connection with its immigration and nationality purposes, provided that such sharing complies with the other relevant legal requirements and is not expressly or impliedly prohibited by statute. All of the data sharing to be conducted under the Protocol falls within the ambit either of our common law powers or of specific legislation.

Some of the data disclosed under the Protocol is categorised as "personal customs information" as a consequence of the Borders, Citizenship and Immigration Act 2009 ("BCI Act"). This will include information (for example, a record of a person entering the UK) which may be relevant both for immigration and customs purposes, but which is known to have been acquired initially in the exercise of a customs function. It will also include information which is capable of being acquired in the exercise of a customs function in circumstances where it cannot be said that it was *not* acquired in that way. Such information will therefore only be shared under the Protocol where lawful to do so under the provisions of the BCI Act.

The UK Border Agency needs and is empowered to share data both inwardly and outwardly in connection with its immigration and nationality purposes. Our trials demonstrated the practical necessity of two-way data sharing, as both of the countries involved in a fingerprint match need to share data in order to receive the benefit, for example, by seeing whether the information known to each is consistent. It is also clearly necessary to share appropriate data outwardly with our partners as part of a reciprocal arrangement in order to serve the legitimate purpose for the United Kingdom. Further, a false identity used to penetrate another country's border can equally be used to penetrate the UK border, and it is directly in the interests of the UK to work together with other countries to identify false and compromised identities in order that they can be taken out of circulation.

There are no legislative barriers or international obligations preventing this activity. To the extent that international obligations relate to the Protocol, the arrangements provide for the activity to be carried out in accordance with those obligations – for example, section 5.4.1 sets out how the activity will comply with specific human rights obligations. More generally, the arrangements for the Protocol expressly provide for each participating country to comply with its domestic laws and international obligations.

6.2.2 How do the arrangements comply with the Data Protection Act 1998, and other legal requirements?

The Data Protection Act 1998 (DPA) sets out eight legally enforceable Data Protection Principles (DPP):

- 1st principle – fair and lawful processing. Section 9 summarises the issues in relation to how the Protocol arrangements are fair to the person whose data is being shared. 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. Some of the data to be processed under the Protocol will be sensitive personal data. However, the UK Border Agency's processing of data under the Protocol will go no further than is necessary for the exercise of its immigration and nationality functions. Accordingly, at least one condition in Schedule 2 and at least one condition in Schedule 3 will be met. Sections 4 and 5 of this document set out how the arrangements ensure that data may only be processed to the extent that is necessary for the exercise of these functions.
- 2nd principle – obtained for limited purposes and not further processed for incompatible purposes. Section 5 sets out how the Protocol provides for processing only for legitimate immigration and nationality purposes.
- 3rd principle – adequate, relevant and not excessive for the purpose. Section 4 sets out the multi-layered approach which will ensure, so far as practicable, that data will only be processed to the extent necessary for the legitimate purposes.

- 4th principle – accurate and up to date. Section 4.7 sets out how the arrangements will ensure the accuracy of the data exchanged, and its interpretation, and how this will support the wider accuracy of our data.
- 5th principle - not kept for longer than is necessary. Section 8 sets out the arrangements we have agreed for retention of the information.
- 6th principle – processed in line with rights under the DPA. The Protocol does not interfere with the right under section 7 of the DPA to make a subject access request to the UK Border Agency, nor does it otherwise contravene this principle.
- 7th principle – secure. Section 7 sets out the technical and practical arrangements to ensure the security of the data.
- 8th Principle – not transferred to countries without adequate protection. Section 6.3 sets out how we have assessed the adequacy of the data protection arrangements in our partner countries

As well as operating in accordance with the DPA, the UK Border Agency respects its duties of confidentiality and ensures that the human rights of people whose data is shared are respected. This includes both ensuring that the data sharing itself is consistent with people's rights – in particular the right to a private and family life under Article 8 of the Human Rights Act 1998 – and ensuring protection of the rights of people whose information is shared with our partner countries.

The maintenance of a fair and effective immigration control is a legitimate social aim which is necessary in a modern and democratic society. Sections 3-5 of this document set out why the UK Border Agency believes the FCC Protocol is in general a proportionate step to take, which strikes an appropriate balance between safeguarding the private lives of the individuals concerned and protecting the public. Information is shared only to the extent necessary for the specific purpose, and with appropriate protection in relation to onward disclosure or use.

An individual will only have his fingerprints disclosed under the Protocol if it is thought that value could be derived from that disclosure. Further information will be exchanged only where there is a match. Even if there is a match, only basic levels of information are shared automatically. Disclosure of more detailed information will only take place where it is relevant, proportionate and lawful in the individual case.

To any extent that this arrangement may interfere with an individual's right to a private life, we consider such interference to be proportionate to achieve our legitimate aim of upholding immigration control.

Equally, the duty of confidentiality is not absolute, and we consider it is outweighed by the public interest in checking fingerprints of relevant immigration

cases, and sharing relevant data between countries that have a legitimate immigration interest in the individual.

6.3 Are the other FCC countries' data protection arrangements adequate?

6.3.1 Why did we conduct an 'adequacy assessment'?

As all European countries' domestic legislation enshrines the rights and freedoms set out in European data protection law, we can have reliance on the adequacy of data protection arrangements within Europe. However, when considering sharing people's data outside the EEA, it is important for us to ensure as far as possible that adequate protection for rights and freedoms also exist in the countries to which we may be sending people's data. Specifically, the eighth data protection principle in the DPA prevents the transfer of personal data outside of the EEA unless either:

- the receiving country ensures an "adequate level of protection" for the rights and freedoms of data subjects in relation to the data processing; or
- the eighth data protection principle does not apply, by virtue of one of the conditions in Schedule 4 of the DPA being met.

One of the conditions in Schedule 4 is where the transfer of data is necessary for reasons of substantial public interest. We consider that data processing under the Protocol is necessary for reasons of substantial public interest, and that the 8th data protection principle therefore does not apply. However, as a matter of policy, the UK Border Agency seeks to ensure as far as possible the adequacy of the protection arrangements for data shared outside the EEA, rather than simply relying on exemptions. We have therefore assessed the data protection arrangements in Australia, Canada the US, and New Zealand and developed the specific arrangements for the Protocol with a view to ensuring their adequacy in all the countries.

6.3.2 How did we conduct the adequacy assessment?

We considered both the General Adequacy and Legal Adequacy Criteria in relation to these countries, in accordance with the UK Information Commissioner's guidance and in consultation with his office and the Ministry of Justice. We also checked our findings with our colleagues in those countries to ensure that our understanding of their arrangements is correct. In line with the DPA's requirements, in assessing adequacy we took particular account of:

1. the nature of the personal data;
2. the country or territory of origin of the information contained in the data;
3. the country or territory of final destination of that information;
4. the purposes for which and period during which the data are intended to be processed;
5. the law in force in the country or territory in question;

6. the international obligations of the country or territory in question;
7. any relevant codes of conduct or rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
8. any security measures taken in respect of the data in that country or territory.

6.3.3 What were our findings on the General Adequacy criteria?

We assessed the arrangements for fingerprint sharing in the first stage of the Protocol process separately from the arrangements for sharing biographical data in the second stage (see section 4.4), as the levels of inherent risk involved and the necessary steps to mitigate those risks were very different:

- in relation to the first stage, having taken into account all the circumstances, we concluded that Australia, Canada, the US and New Zealand would each provide an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data transferred to them. No significant risk to the rights and freedoms of the individuals involved would be presented by the transfer of nigh anonymous fingerprints under the agreed arrangements for the Protocol; and
- in relation to the second stage, we considered that the personal data to be transferred carried significant risk, being readily identifiable and in some cases sensitive personal data which may need to be retained for a considerable time for the recipient authority to complete its processing. However, we also considered that the risks to the rights and freedoms of data subjects would be sufficiently mitigated by the security of these countries' existing arrangements, and by the specific arrangements implemented for the Protocol, as to allow for adequacy under the eighth data protection principle, provided that the legal adequacy criteria can also be met.

6.3.4 What were our findings on the Legal Adequacy criteria?

We were able to recognise Australia, Canada the US and New Zealand as stable states, with no real danger of prejudice, and have confidence that they recognise the rule of law and have effective legal frameworks for the protection of rights and freedoms of individuals generally. Each has specific legislative arrangements for protecting the rights and freedoms of data subjects, including a Privacy Act incorporating similar data protection principles as are set out in EU law and relevant international instruments, such as the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These principles are more widely recognised as the core of personal data protection.

Compliance with data protection law in Australia, Canada and New Zealand is overseen by independent national Privacy Commissioners and is enforceable in their national courts. The US compliance framework is in contrast a networked and layered approach, directly involving a range of actors and processes across

the executive, legislature, judiciary and public community. There are a number of similarities and differences between these countries' arrangements and the European framework. None of these countries is currently subject to a general finding of adequacy by the European Union, although the EU has put in place arrangements with each, for which it has made findings of adequacy.

In making our assessments, and in developing our arrangements, we took account of the principles and arrangements already agreed by the EU, and the European Data Protection Supervisor's published Opinions thereon, intending to ensure that the Protocol arrangements met our test of adequacy and also met or exceeded the standards agreed and recommended at European level.

The key question we sought to answer in our adequacy assessments was whether the specific terms of the MoU, and the wider legal framework within which each country operates, would between them ensure adequate protection for the rights and freedoms of people whose data we would share. In doing so, the key differences we encountered were:

- none of the other countries' privacy legislation differentiates 'sensitive' personal data from other forms of personal data. However, the Protocol arrangements are such that all personal data disclosed by the UK Border Agency (whether sensitive personal data or not) will only be processed by the legitimate state authorities of those countries for their immigration and nationality purposes. Therefore, protection comparable to that provided in the UK by Schedule 3 of the DPA is in place (see section 6.2.2);
- the approach to retention in the Privacy Act in Australia is formulated differently. However, the Protocol arrangements provide an agreed approach to retention (see section 8);
- Canada's and the US' legislation does not explicitly require restrictions on data processing that are imposed by the originating party to be respected. However, the Protocol arrangements provide for this (see section 5.4.2);
- whilst Canada's legislation requires its institutions to ensure the accuracy of their information, rights of access and corresponding rights to request corrections and notations can only be exercised by people who are citizens or residents of, or are physically present in Canada. Foreign nationals would thus be able to exercise these rights only if they were present in Canada. However, our arrangements for the Protocol specifically provide that similar opportunity for access, correction and notation will extend administratively to all people whose data is shared. This is a similar approach to that taken in the EU-Canada API/PNR treaty, which is publicly available;
- equally New Zealand's legislation requires foreign nationals to be physically present in New Zealand to exercise their rights of access and corresponding rights to request corrections and notations. However, New Zealand's Department of Labour does already go beyond the requirements of its Privacy Act by providing in its internal policies the right of access and correction to all people about whom it has made a decision on an immigration matter

regardless of location. The Protocol will also extend these arrangements to all people whose data is shared under it.

- similarly, access, correction and notation rights under the US Privacy Act only apply statutorily to US citizens and residents. However, US DHS has administratively extended these to foreign nationals whose data is provided to DHS under the Protocol arrangements, and this is explicitly provided for in the arrangements, a similar approach as with the publicly available EU-US PNR agreement; and
- the networked and layered US compliance framework is very different from the European model, involving a range of checks and balances between the executive, legislature, judiciary and public community. We assessed that a person whose data is shared with DHS through the Protocol would have adequate opportunity to exercise and enforce his rights through the various US administrative and judicial mechanisms.

Having taken into account all the circumstances, we considered that Australia, Canada, the US and New Zealand would each provide an adequate level of protection for the rights and freedoms of data subjects under the Protocol, and that the Protocol can therefore take place in compliance with the Eighth Data Protection Principle.

7. What are the technical and practical arrangements?

7.1 How do we know the data exchange will be secure?

Other than in the contingencies set out in section 7.3 below, all of the data exchange will be conducted securely and using encryption between designated points of contact in each country, through a Secure File Share Server (SFSS) hosted by the Government of Australia. The security measures include appropriate technical measures in line with ISO17799/BS7799 standards for transferring the fingerprints via the SFSS, which will be fully accredited by the system security accreditors of each of the FCC countries before they implement the Protocol. This will minimise the risk of any outside interference in the data transfer.

The SFSS is constructed in such a way that data can only be accessed by the country for which it is intended. The country retrieving the data from the SFSS will delete that information from the SFSS upon retrieval. Thus all data exchange is bilateral between two of the countries, no data will be seen by any authority for which it is not intended, and the data will not remain on the SFSS for longer than the short time that is necessary for the rightful recipient to retrieve it.

The security and management arrangements for the SFSS are set out in an agreed Service Arrangement between the government of Australia and the other participating countries.

7.2 How do we know that each country will protect the data appropriately?

Each country has made arrangements for the data exchange to be carried out securely by named individuals in a central unit, interfacing directly with the other countries via the SFSS, with the operators of their fingerprint system, and with other parts of their organisation.

The fingerprints that are shared in the first stage of the process will be removed from the SFSS by the receiving country, transferred securely to the fingerprint system operators for matching, and after matching, will be destroyed. Thus the fingerprint processing will occur within a closely controlled process undertaken between the Protocol operators and the fingerprint system operators, each of which will operate within a closely controlled environment, presenting minimal risk of error of interference.

The personal data that is shared in the second stage of the process, on cases where fingerprint matches are identified, will also be processed securely by the central unit in each country. However, it will necessarily have to be transferred elsewhere within (or sometimes beyond - see section 5.2) the organisation in order to be acted on by the relevant operational unit. In order that the rights and freedoms of people whose data is shared are not weakened by this further transfer, the arrangements require additional safeguards in each country to ensure the continued security of the data received from the other countries.

In particular, each country will maintain the data in a manner at least as secure and with similar privacy and data protection rights being afforded to the data subject as is the case with its own citizens. Specific minimum standards include:

- personal data received will be handled in accordance with an appropriate level of classification. The countries' classification systems are different, but each will apply a broadly equivalent classification. In the UK this will be the "restricted" classification, in Australia and New Zealand "in confidence", in Canada "protected B", and in the USA "sensitive but unclassified".
- personal and official information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information. Each country will store the data in secure electronic and/or paper storage systems at all times.
- access to the data received will be restricted to those authorised personnel who have a need to know the information to carry out their official duties, for uses which are consistent with the purposes of the Protocol;
- all persons who have access to the data will have been appropriately educated and trained regarding the handling and restrictions on use of this information to ensure the overall safeguarding of the information and compliance with the Protocol arrangements; and
- each country will ensure that information received is protected from unauthorised dissemination, and will take appropriate action under its

administrative, civil, and/or criminal laws in the event of misuse, unauthorised alteration or deletion, or unauthorised access or dissemination of the information by its own employees, agents or any third party.

7.3 What will happen if there is a problem with any of the arrangements?

If the Secure File Share Server is unavailable for any reason, there are two agreed contingencies for data transfer:

- information may be transmitted via direct country-to-country e-mail transfer, which will be encrypted using an Advanced Encryption Standard (AES) 256 bit key; or
- in the unlikely event that the SFSS and encrypted e-mail are both unavailable, but there is an urgent need to share information, it may be hand delivered, with appropriate protection, by one of the designated contacts to the relevant Embassy or High Commission of the other country, for onward transmission to the latter's home government within its secure e-mail network.

As these two contingencies provide secure alternate methods of communication, the possibility of the SFSS being unavailable for any reason does not present any significant risk to the security of the arrangements.

We have also agreed further safeguards in the event of unforeseen difficulties occurring in any of the countries, in particular:

- for each country to notify the others immediately in the event of a disaster or other situation that disrupts the intended transfer of information between them; and
- as soon as reasonably practicable, but no later than twenty-four hours after becoming aware of any breach of the security of the information systems containing, or unauthorised use or disclosure of, any personal information that has been shared.

Whilst each country reasonably expects the other countries participating in the Protocol to implement the agreed arrangements in good faith, as a further safeguard we have specifically provided for reporting and audit facilities:

- the countries will produce comprehensive, joint performance and management information about the operation of the Protocol, which will explicitly identify the number and severity of any security or privacy breaches and of remedial actions taken;
- any country may request assurance from another country that sufficient safeguards are being maintained in respect of the information shared, which may include an audit of the safeguards, to be carried out by an appropriate internal or external auditor with terms of reference agreed between the countries; and
- in the unlikely event that a country considered it necessary to decline to provide further information to another because of perceived deficiencies in

safeguards, it could do so. This would be notified to all of the countries participating in the Protocol, which would consult each other immediately to decide upon the appropriate course of action.

8. What are the arrangements for retaining the information?

There has been much debate about the circumstances in which personal information should be retained by government agencies, and for how long. The general principle is that it should be retained for as long as it remains relevant for the necessary purpose, and for no longer. However, the continued relevance of a set of information is likely to vary in different circumstances. Thus a fixed 'retention period' is likely to be a very blunt instrument, both from the point of view of the person who does not want his information kept longer than is actually necessary, and from the perspective of the organisation that wishes to keep it for as long as it may be needed. For how long it may be needed is also a difficult question, as the organisation cannot necessarily predict whether it will come into contact with a particular person in the future, or whether the information would again be relevant if it did.

In developing the FCC Protocol and assessing its impacts, it was clear that a 'one size fits all' retention policy would not serve anyone's interests very well. Therefore we considered which information would need to be kept in which context, and how we could best regulate that. This section sets out the approach we formulated, and why we believe it is the most appropriate. Personal information that is exchanged under the Protocol may only be retained as set out below, unless the agency that supplied the information has given its prior written approval. The UK Border Agency would not give such approval unless we were satisfied that the information was still relevant and further retention was appropriate.

8.1 Retention on the Secure File Share Server (SFSS)

There is no need to retain information on the SFSS after it has been retrieved by the receiving country. All personal information will therefore be deleted from the SFSS upon being retrieved successfully. This will be done by the person retrieving the information, backed up by an automated deletion mechanism. The SFSS will not hold a back up copy of the information. This provides confidence that the data is no longer held in the central system, without presenting risk of data loss, as the relevant countries' tracking arrangements would identify any data that was missing, which could then simply be re-sent via the SFSS.

8.2 Retention of the fingerprints that are shared for searching

As the fingerprints may only be used for searching against the biometric database, and for no other purpose, there is no need to retain them after the

searching has been done. Each country will therefore destroy them securely once they have been searched.

8.3 Retention on the case file for the person whose information is shared

Where information that is shared is included in the case file (either electronic or paper) for the individual to whom the data relates, because it has ongoing relevance to the file, it may be retained as part of that case file in accordance with the domestic laws and data retention policies of the country that has received it. Thus if we receive information about one of our customers, which is pertinent to our decision, we will reflect that information in our decision, and keep the information as part of the file for the same period we would keep other relevant information. This is both appropriate and inevitable.
People would expect their personal file records to be kept complete and accurate, for as long as they are kept. This does not present the same privacy risks as retaining data in other systems. Removing part of the information which led to a decision would corrupt the file record, and it would not in any case be possible where the information in question had been reflected in other case papers, for example, in the decision letter issued to the person. There would be no logic in seeking to apply an arbitrary retention limit to information held on case files. Each FCC country has laws and policies applying to retention of case files and we have agreed that those will apply in this context.

8.4 Retention for watch list purposes

Each of the FCC countries maintains one or more 'watch lists' which enable it to identify persons of interest who come into contact with it. Each country has its own system for managing the information placed on those watch lists, as an integral part of its immigration processing. Whilst it is important for each country to be able to put appropriate information that is uncovered through the Protocol onto those watch lists, and trials have shown high value in doing so, this would if unregulated present a number of risks to people whose information is shared. The Protocol arrangements therefore regulate how this will operate, and identify that personal information in relation to three categories may be placed onto watch lists:

- false identities and travel documents. It is strongly in the public interest for false identities and documents that are uncovered to be placed onto watch list systems, in order that they cannot be used again and, if they are, that they can then be taken out of circulation;
- multiple identities used by the same person. Trials have shown that where people are using multiple identities, it may be necessary to place all of these onto a watch list system. In some circumstances there is more value in putting such a person's true identity onto the system than the false one: for example, where someone is using a false identity within the country, whilst travelling in and out of the country in their true identity, it is putting the true identity onto the system that will result in the person being caught; and

9.3 Fair processing

It is most important that the processing of people's information is transparent and fair, both from the point of view of the individual whose information is being processed and for wider public trust.

We have reflected in this report how the UK Border Agency and its FCC partners have developed the Protocol to enable sharing of appropriate information within an arrangement that we believe provides high standards of data protection, with a range of safeguards to ensure the information will only be used for appropriate purposes, that it will be accurate, and that people whose information is shared will be able to see and if necessary correct that information.

We have seen how information obtained through the Protocol is in the interests of the genuine applicant as it helps corroborate his application. It is also important to consider how the information will be processed fairly within our operational processes. Where we receive information that introduces ambiguity because it contradicts what one of our applicants tells us, we intend to put the information directly to the person, give him an opportunity to respond to it, and take his response equally into account. This is part of fair processing. There may be a rational, innocent explanation for something that at first appeared to contradict a person's account.

However, the information obtained from the fingerprint matching is factual, and is susceptible of proof. It is also predominantly well known to the applicant - for example, a person will be well aware of whether he had previously visited the USA using a different identity – and it is incumbent upon him to respond truthfully to it. Our trials showed that in practice an applicant can respond in three ways when such information is put to him:

- he can tell us that he is the person who was fingerprinted by the other country, in his true identity. In this scenario the information has revealed the person's true identity, and associated information, and he will need to explain himself in the light of this;
- he can tell us that he is the person who was fingerprinted by the other country, but that he was using a false identity at the time. We will interview the applicant further to determine whether this is credible in the light of the associated information; or
- he can tell us that the fingerprint match is false, and therefore none of the information relates to him. We can confirm the accuracy of the fingerprint match to the standard of proof applicable in criminal matters (see section 4.7). In the unlikely event that the match was found to be false – which never occurred in our trials – the information relating to it would be disregarded.

In each scenario, the information assists in resolving the case, whether or not the person responds truthfully. Most people know that fingerprint matching is susceptible of proof, and in trials most applicants admitted that the fingerprint

match was genuine. A number provided potentially innocent explanations, which were then examined further in the interview. We were able effectively to determine whether those explanations were true. This is because a true account would tally with additional information known about the alternate identity, whereas the falsity of contrived explanations was demonstrable as they did not accord with other known facts.

The key question that always has to be considered is whether the person meets the criteria to be recognised as a refugee. This is clearly not the same as the question of whether the person is telling the truth, although these questions are linked. A person fleeing persecution may well have needed to use deception at some stage in his flight, and if he tells us the truth about this then it does not detract from his claim. Equally, a person who has previously been dishonest with us may, once the truth is established, turn out to qualify for refugee status after all. In all cases, the first aim is to establish the truth as it relates to the application.

However, it remains incumbent on an applicant to provide a true account of himself, which he has ample opportunity to do, and one who continues seeking to deceive will have little credibility, and his application is likely to be expedited for refusal and removal on the basis that it is clearly unfounded. Where people continue deceptively seeking to frustrate our endeavours to achieve the correct outcome for their case, we will consider criminal proceedings as appropriate. As with all other immigration cases, where necessary and appropriate, immigration detention may be used in managing a case to its conclusion.

9.4 Judicial scrutiny

All of our relevant functions are also directly or potentially subject to judicial scrutiny in some form. For example, asylum decisions made by the UK Border Agency are appealable to the Asylum & Immigration Tribunal and onward to the higher Courts. Judicial scrutiny provides a fundamental safeguard for people's rights and freedoms in immigration matters. If we made a wrong decision about a person based on information that had been shared – whether because the information itself was wrong, or a wrong conclusion had been drawn from it – the person affected would have the ability to challenge this in the Courts.

This is a fair process that is in the interests of the genuine applicant as well as the UK public.

- persons engaged in derogatory activity that would render them inadmissible to the other Participant's territory. For example, a serious foreign criminal who would be debarred from entering our country because of that criminality may be entered on our watch list, in order that he cannot enter the country whilst concealing his criminality.

The Protocol provides that such information may be retained for as long as it is relevant to that Participant's border controls, up to an initial maximum of ten years. Ten years is a sensible period for retention, coinciding with the length of validity of many travel documents (that is, they could otherwise still be used for up to ten years). However, false identities may be renewed and there may be a case for retaining some information for longer than ten years. The Protocol therefore provides that, as part of our ongoing review of watch list entries, the FCC countries will discuss the continued relevance of the information within the ten years and seek agreement on any further retention. However it is likely that wider international agreements on watch list arrangements will be in place within that timescale, with which we may simply agree to fall in line.

8.5 Retention in central record or elsewhere

Each of the countries may, to a greater or lesser extent, also need to keep information that it receives under the Protocol elsewhere, in particular, in a record held by the central team that administers the Protocol. This is particularly the case in the UK, where the central team will pass information to the relevant operational colleagues for action, but will also have an ongoing monitoring and liaison role to ensure effective action is taken, and will need separate access to the data for that purpose. However, none of our countries wish to allow the development of a database of personal information shared under the Protocol, or the possibility of the data being held unnecessarily elsewhere. The Protocol arrangements therefore provide that any such retention is limited to two years. This will allow time for the necessary operational action, but avoids the risks of data accumulation.

9. Is the data sharing consistent with the legitimate expectations of the people whose data is being shared?

We have set out in the other sections of this paper why the FCC authorities are implementing the High Value Data Sharing Protocol, and how it will operate legally, technically and practically. We considered it would be useful to complete our report by reflecting on whether its operation will be consistent with the legitimate expectations of people whose data is shared under it, and in particular, whether it will be fair to them.

9.1 Expectations notice and consent

People whose information may be shared through the Protocol are already routinely notified (usually when their fingerprints are initially captured) that their data may be subject to international checks. For some years, asylum seekers and certain categories of enforcement case have had their fingerprints checked against other European countries' data through the Eurodac database as a matter of course. The Protocol presents a further avenue for making such checks.

A person who has fled persecution may arrive in the UK from halfway across the world, by whatever route, with little or no means of demonstrating his credentials. If he has previously been encountered by a country with which we can conduct checks, this can only help to verify those credentials. We believe the general public would agree that we should have the facility to conduct such checks, with rigorous security, as a positive means of validating our customer's account. Thus the implementation of the Protocol supports our ability to identify and protect genuine refugees.

Conversely, however, we consider it our duty to make checks to detect those who make fraudulent claims on the UK public and to identify foreign criminals and others who seek to obstruct our ability to remove them to their country of origin by destroying their documents and concealing their true identities. For this reason, although we notify our customers that we make such checks, we do not make the checks dependant on the consent of the individual. The public would not be well served by a system which allowed fraudsters to escape detection simply by withholding consent.

9.2 Expectations on security and confidentiality

A person whose fingerprints are checked through the Protocol can legitimately expect his information to be handled securely and confidentially. A reasonable person would not expect us to be sharing personal information about our customers with other countries in an uncontrolled way. However, we believe a reasonable person would expect us to co-operate operationally with partner countries on cases presenting mutual immigration interest.

We believe that the Protocol arrangements as described in this report provide high levels of data security, and appropriate confidentiality. The fingerprints are checked in an effectively anonymous way, and are not retained or used for any other purpose. Personal biographic information is only then exchanged on cases where a fingerprint match is found, with another country which has already encountered and has a legitimate immigration interest in the individual. We believe this accords with what a reasonable person would expect.

カナダ

(PIA summary)

事例）

公共事業・政府サービス省及び歳入庁におけるＰＩＡ報告書概要

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

Canada

※公共事業・政府サービス省

Privacy Impact Assessment (PIA)

To assure Canadians that privacy principles are being taken into account when there are proposals for, and during the design, implementation and evolution of programs and services that raise privacy issues by:

- prescribing the development and maintenance of Privacy Impact Assessments; and
- routinely communicating the results of Privacy Impact Assessments to the Privacy Commissioner of Canada and the public.

Privacy Impact Assessments provide a framework to ensure that privacy is considered throughout the design or re-design of programs or services. The assessments will identify the extent to which proposals comply with the provisions of the Privacy Act, regulations and Treasury Board Secretariat Privacy Impact Assessment Policy. Assessments assist managers and decision-makers to avoid or mitigate privacy risks and promote fully informed policy, program and system design choices.

Privacy Impact (PIA) Report Public Summaries

The subsection 5(2) of the *Privacy Act* requires government institutions to notify individuals of the intended uses, consistent uses and disclosure of personal information when it is being collected. To complement this requirement and to promote a broader understanding of how privacy issues related to the program or service have been addressed, institutions must make summaries of the results of their Privacy Assessments available to the public.

- Certification Program for the Federal Government Procurement and Materiel Management Community
- Compensation Web Applications
- Foreign Banking Services (FBS)
- Government of Canada Pension Modernization Project - Release 1.0
- Industrial Security Program – Release of Personal Security Screening Information
- Integrated Information System (IIS)
- Minister's and Deputy Minister's Correspondence Process
- On-line Registration and Credential Administration – Release 1.0
- Publications Website
- Receiver General Buy Button (RGBB)
- Receiver General Buy Button (RGBB) Upgrade

Date Modified: 2010-08-31

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada | Canada

Government of Canada Pension Modernization Project – Release 1.5 - Enhanced Case Management and Imaging

Introduction

This document summarizes the Privacy Impact Assessment (PIA) Report that the Government of Canada undertook to ensure that privacy was considered throughout the development and deployment of Release 1.5 of the Government of Canada Pension Modernization Project (GCPMP). The PIA Report concluded that personal information is involved in Release 1.5 with an overall risk rating of "medium". Implementation of the mitigation mechanisms described in the Privacy Risk Management Plan below will alleviate potential issues and concerns.

Background

Public Works and Government Services Canada (PWGSC) is the administrative authority for the disbursement of pay and pension services under the *Department of Public Works and Government Services Act*. PWGSC is responsible for the administration of pension plans for public servants governed under the *Public Service Superannuation Act* (PSSA), and for the administration of the respective pension plans for the Members of Parliament, Federal Judges, the Diplomatic Corps, and the Lieutenant Governors. The Department also provides pension services, on a cost recovery basis to the military members of the Department of National Defence (DND).

The GCPMP has been established to develop and implement Information Technology solutions for the renewal of PWGSC pension administration systems and services. The GCPMP will provide a modern pension administration system through the phased adoption of commercial-off-the-shelf (COTS) software based solutions.

Business Process

The business requirements for GCPMP Release 1.5 are focused on the automation and enhancement of service delivery to Clients. Release 1.5 consists of providing Public Service Pension Centre (PSPC) operations and other groups within Compensation Sector with enhanced case management capabilities and the addition of digitized images for all incoming documents received by mail and fax.

PSPC Agents include Pension Specialists, Client Inquiry, Pension Portability and Executive Services personnel. Unlike R1.0 where only half of the PSPC staff in Shediac were expected to access the system, Release 1.5 extends the Case Management capabilities to the rest of the PSPC operations, approximately 600 end users.

In Release 1.5, all incoming mail and faxes will now be received and digitized by the Cheques Redemption Control Directorate (CRCD) Imaging Facility located in Matane, Québec. Upon receipt of incoming hard copy mail or fax by the CRCD, an image of each document is captured. In addition to processing all incoming mail, Release 1.5 provides the capability to process requests received by electronic mail. An e-mail received from a Client will be automatically acknowledged by the system with an indication to the sender as to when an answer should be provided.

Personal Information Collected by GCPMP Release 1.5

The following data elements which constitute personal information are collected as follows:

- **Personal Identifiers:**
  - Personal Record Identifier (PRI);
  - Pension Number (PN); and
  - Social Insurance Number (SIN) - in scanned documents only.
  - Universal Unique Identifier (UUID) – for internal system use only.
- **Names**: Last and first name of an individual and other variations of names such as name changes, maiden name, given name, etc.;
- **Dates**: Date of birth, death, etc.;
- **Addresses**: Mailing address, temporary address, out of country address, e-mail address, fax number, etc.;
- **Bank Information**: Banking institution, transit number and account number; and
- **Payment Information**: cheque number, payment amount and encashment date.

The new imaging functionality in Release 1.5 does not have an impact on the following processes: Consent for Disclosure; Safeguarding Personal Information, Accuracy; Openness; Individual's Access to PI; and Challenging Compliance.

Data from the existing Production Control File Location System (PCFLS) will be converted and brought into the Case Management application. No other legacy applications or databases are being discontinued during the operational period for Release 1.5.

Data Analysis

The data flow analysis section of the PIA Report identifies and traces personal information from the point of collection to the point where all copies of the information are disposed or permanently destroyed. Table 1 – Data Flow Analysis - documents the personal information involved in three GCPMP Release 1.5 business processes: "Manage Contacts", "Manage Correspondence" and "Manage Contributions and Receivables".

Table 1 - Data Flow Analysis

Description	Collected by	Format	Purpose of Collection	Used by or Disclosed to	Storage or Retention Site
Name Salutation Home Address E-mail Address Phone Number Fax number Personal Reference Identifier Pension Number Date of Birth	Toll free numbers CRM - Call Monitoring Manage incoming correspondence Legacy Annuitant/ Contributor Systems via SMIRS Bridge	Phone IVR TTY Fax E-mail	To manage client inquiries/ requests via PSPC Client Contact Centre	Active/Retired member (Ex) spouses/ (Ex) partners of an Active/Retired member Children of a Retired member Family members of an Active/ Retired member Power of Attorney/Lawyer	Pension System Universal Client Management (UCM) Customer Relationship Management (CRM)
Document Image Document PRI/PN Surname Given Name Address Phone Number E-mail Address	Cheque Redemption Control Directorate (CRCD) System generated Agent or Pension Expert	Mail Fax E-mail Image	To manage incoming and outgoing correspondence.	Active Member Retired Member Power of Attorney/Lawyer Employer External Stakeholder	CRCD Imaging System Database CRCD Image Repository Customer Relationship Management (CRM)

Cheques payments: • Document Image • Name • Amount • Cheque Number • Bank Account Number • Transit Number • Financial Institution Number • Encashment Date Department Remittance Information File for BPS: • PRI/PN • Name • Amount • Possibly other personal data	Cheque Redemption Control Directorate (CRCD) Bill Payment Services (BPS) Contractor (National Bank of Canada)	Mail Image	To handle receipt of contributions and other receivables.	Common Department Financial System (CDFS) Receiver General	CRCD Imaging System Database CRCD Image Repository Bill Payment Services Database

Privacy Risk Management

Section 6 of the PIA Report identifies GCPMP Release 1.5 privacy risks and potential risk mitigation strategies. Table 2 – Risk Management Plan - below summarizes that information.

Table 2 - Risk Management Plan

Element	Nature of risks	Level of risks	Proposed Mitigating Mechanisms
Potential Unauthorized Disclosure of Private Information	Inappropriate access Disclosure of personal information to unauthorized persons	Low	Continue to provide training to Agents Implement periodic audits of calls to monitor Refresher training on privacy issues
Capturing Personal Identifier Data Over IVR (Integrated Voice Response)	Inappropriate access Compromise of personal information to unauthorized persons	Low	PRI or SA is not related to or stored with a name in the IVR
Compliance with *Privacy Act* (ss. 5 (2)) for Privacy Statements	Inconsistent access to the Privacy Statement across all channels	Low	Callers are instructed to obtain the Privacy Statement via the existing website or to wait for an Agent Develop a standard, generic Privacy Statement for all channels Add a link in outgoing E-fax and E-mail messages to a web site with further information on PWGSC Privacy Policy
Documented Security Procedures	Inappropriate access Compromise of personal information to unauthorized persons Accountability	Low	Establish and document detailed security procedures for the collection, transmission, storage, and disposal of personal information

Audit Logs and Audit Trails	Inappropriate access Compromise of personal information to unauthorized persons Unauthorized changes to personal information	Medium	Define audit requirements Design, develop and implement audit solution for all application software components
Safeguards to Protect Personal Information	Inappropriate access Compromise of personal information to unauthorized persons Unauthorized changes to personal information	Medium	Implement safeguards recommended through the Certification & Accreditation process Continue to abide by conditions set out in Letter of Accreditation

Conclusion

The highest privacy risk identified in the Privacy Risk Management Plan is evaluated as "medium". PWGSC has examined the impacts and has proposed appropriate mitigation strategies for the identified privacy risks associated with Release 1.5 of GCPMP.

Most notably, there is a need for audit requirements and additional safeguards to be implemented to protect personal information. Security activities are being conducted in parallel with the PIA in accordance with the Certification & Accreditation (C&A) process.

The proposed mitigating mechanisms for the identified privacy risks indicate a continued commitment by the Crown in ensuring the confidentiality and privacy of the personal information collected from individuals.

Date Modified: 2010-09-28

Publications Website Privacy Impact Assessment Summary

Introduction

Part of the mandate of the Public Works and Government Services Canada (PWGSC) – Consulting, Information and Shared Services Branch (CISSB) is to inform Canadians about the federal programs and services available to them. To assist in this mandate, CISSB – Publishing and Depository Services Program (PDS) has created a Web application to provide an integrated computerized solution for the management, publishing, promotion and sales of Government of Canada (GoC) publications.

The Government of Canada Publications Web site is designed to leverage the publishing, marketing and cataloguing expertise of the PWGSC's Publishing and Depository Services Program to create "one-stop-shopping" for GoC publications.

This web site supports other Government of Canada Primary Portals – the Canada Site, 1 800 O-Canada, and the Service Canada in-person centres - through providing e-access to bibliographical information, publication availability, distribution sources and ordering information.

Benefits

Visitors benefit from end-to-end services for searching, ordering, and purchasing Government of Canada publications.

Credit card purchasing activities are accomplished through the use of the Receiver General Buy Button (RGBB), a secure shared government service.

PDS employs external service providers to deliver its services such as shipping, warehousing and distribution services.

Information about the Crown Copyright and Licensing section and its activities is also made available on the Government of Canada Publications Web site. Visitors may request permission to reproduce, adapt, revise and/or translate any Government of Canada works by downloading the application form accessible from the web site in PDF format or by applying on-line using the web form. The web form provides a fast and easy way to fill out and submit requests for copyright clearance on Government of Canada works.

Report Objective

A privacy impact assessment (PIA) for this on-going initiative was conducted to determine if there were any privacy, confidentiality and security issues associated with the Government of Canada Publications Web site and its various components/interfaces, and if so, to make recommendations for their resolution or mitigation.

Description

For information on Government of Canada Publications, customers can send their questions or their comments through the GoC Publications Web site using the Contact Us form or call directly the PDS Customer Service. Personal information collected includes name, telephone number and e-mail address if the visitor wants to receive an answer.

Customers can purchase Government of Canada Publications through the GoC Publications Web site in addition to traditional channels (i.e. mail, fax, and phone).

Only personal information needed for order fulfillment is requested from individuals.

Personal information collected by the web order form is the same information that PDS has been collecting via paper form, and is typical of personal information collected for order fulfillment. The personal information includes individual's name, and either the individual's home or office contact details such as mailing address, e-mail address, fax number and telephone number.

Ordering from the Government of Canada Publications Web site is a matter of choice by the customer and, therefore, consent is inherent with that choice.

Customers who select to pay by credit card through the GoC Publications Web site are directed to the Receiver General Buy Button (RGBB) Web interface. This secure Web interface collects and validates the customer's credit card information. If the credit card payment is accepted, the RGBB Web interface returns the authorization number for the payment.

The authorized credit card order is then submitted via an automated interface to the Inventory / Order / Sales management application for order fulfillment. The authorization number is stored in the Inventory / Order / Sales management application and used to process the payment.

The GoC Publications Web application does not process, capture or store any credit card information.

Existing customers who have pre-established credit with PDS can charge their order on account through the GoC Publications Web site. Such orders are automatically submitted to the Inventory / Order / Sales management application for order fulfilment. The customer's shipping data is then sent to the external warehouse.

At any time prior to confirm their online order/payment, customers have the option of canceling the transaction and can choose another channel such as mail, fax or telephone to submit their order.

Customers who select to pay by cheque or money order through the GoC Publications Web site are informed to print the completed order form and mail it along with their payment to Publishing and Depository Services Program.

Customers who prefer to use the paper-based order form can mail or fax their order to PDS Customer Service. Customers may also contact the Customer Service Desk directly to request publications of their choice. Faxes are received in a restricted access room.

RGBB also provides a Web console service where telephone, mail or FAX orders with credit card payments are authorized and captured. The authorization number returned from RGBB is recorded with the order. All correspondence received is secured in a locked cabinet with restricted access.

PDS discloses personal information in accordance with section 8(2)(a) of the *Privacy Act*, for the completion of inquiries and orders pertaining to GoC Publications.

Financial transactions such as sales and account receivables are submitted to the departmental finance system. Customer information such as name, address, telephone number and E-Mail is also provided and stored in the departmental financial system for the purpose of adjustments and reconciliation, should the customer need to be contacted.

Visitors are being informed of the purpose for which their personal information is being collected at every point of collection throughout the Publications website.

Occasionally, PDS promotes Government of Canada publications to subscribers to its mailing list. New customers as well as current ones are being informed of the Government of Canada Publication's mailing list for promotional material and have the opportunity to sign up to receive promotional material while they place an order.

Data Analysis

The different types of personal information collected or used during the various stages of the business process are as follows:

Personal Information elements by cluster	Collected by	Type of format (e.g. paper, electronic)	Purpose of collection	Used by or Disclosed to	Storage or retention site	Retention Schedule (Subject to LAC Document Mgmt review)
Call-back information (Name, title, phone number, comments)	Government Enquiry Services call centre PDS Customer Services	Electronic (via e-mail or telephone) Paper (faxes, mailings)	Call back	PDS Customer Services PWGSC Finance	E-Mail server account PDS Customer Services restricted access room and locked cabinets	1 year 1 year
Contact Information (Name, mailing address, shipping address, invoicing address, telephone)	Government Enquiry Services call centre PDS Customer Services Publications Website application	Electronic (via e-mail or telephone) Paper (faxes, mailings) Web (via Publications Website application)	GoC publications orders fulfillment GoC publications promotions Application for Crown Copyright Licencing Updates to contact information from Client Centre function	PDS Customer Services PWGSC Finance GoC Publications Warehouse GoC publications distributors (mailing lists) CCL Officer Other GoC author department for CCL. request.	E-Mail server account Axapta backend application database PDS Customer Services restricted access room and locked cabinets CCL backend application.	1 year 2 years after inactive 1 year Indefinite
Credit Card (Number, Expiry Date) Entered manually via RGBB online console.	Government Enquiry Services call centre PDS Customer Services	Telephone Paper (faxes, mailings)	Payment for GoC Publications orders	PDS Customer Services RGBB for verification	PDS Customer Services restricted access room and locked cabinets	1 year
Email addresses	Government Enquiry Services call centre PDS Customer Services Publications Website Web application	Electronic (via e-mail or telephone) Paper (faxes, mailings) Web (via Publications Website application)	To respond to queries To confirm GoC publications order details to customer To send notices	PDS Customer Services CCL	E-mail box (server) Axapta backend application database CCL application	1 year 2 years after inactive Indefinite
Payments (Name, address, payment details)	Government Enquiry Services call centre PDS Customer Services Publications Website Web application	Telephone Paper (faxes, mailings) Web (via Publications Website application)	For payment of GoC Publications orders.	PDS Customer Services PWGSC Finance	PDS Customer Services restricted access room and locked cabinets Axapta backend application database	1 year 5 years

Privacy Risk Management

Privacy risks raised in the Publications Website Privacy Impact Assessment are the following (since many of the risks are currently under mitigation a status is also reported):

Privacy Risk	Level	Status
Purpose for which Personal Information (PI) is collected has not been documented.	Low	Implementation completed in the 1st quarter 2008-09.
Consent for secondary purpose not obtained.	Low	Secondary purpose identified at all collection points and a process to obtain consent has been developed. Implementation completed in the 1st quarter 2008-09.
Lack of GoC Publications specific data retention and disposal policies	Low	Records Disposition Authority (RDA) number is to be requested by PWGSC - CISSB for the branch. PWGSC - CISSB to develop policy relating to the retention and disposal of PI.
The adequacy of existing safeguards on personal information has not been systematically addressed	Low	System security procedures are scheduled to be developed in fiscal 2009-10.
Update privacy notices on the GoC Publications web sites to conform to Treasury Board of Canada Secretariat (TBS) standards on Privacy Notices Statements.	Low	Implementation completed in the 1st quarter 2008-09.

Conclusion

This privacy impact assessment of the GoC Publications Web application did not identify any privacy risks that cannot be managed using either current safeguards or others that have been specifically developed for the implementation of the system.

The GoC Publications Web application poses few privacy risks to Canadians, all of which are considered to be low in severity as they relate mostly to process documentation.

These risks have been mitigated with the implementation of the recommendations in the Privacy Risk Management Plan.

Date Modified: 2010-05-04

Canada Revenue Agency | Agence du revenu du Canada

Canada

※カナダ歳入庁

About the CRA > Protecting your privacy

Privacy impact assessment

A privacy impact assessment (PIA) is a process used to determine how a program or service could affect the privacy of an individual. It can also help to avoid or lessen possible negative effects on privacy that might result from a program or service. Also, a PIA is a way for the federal government to state its commitment to protect the privacy of individuals. PIAs promote transparency and accountability, and contribute to continued public confidence in the way the government manages personal information.

PIA summaries

At the links listed below, you can find summaries of the results of PIAs that the Canada Revenue Agency has conducted.

- (2011) Charities – Public Safety and Anti-Terrorism
- (2011) Registered Disability Savings Plans
- (2011) Tax-Free Savings Account
- (2010) Xenon Web Crawling Initiative
- (2009) T3010B (09) Registered Charities information Return
- (2007) The Agency Data Warehouse (ADW)
- (2006) Interactive warning system products

Directive on Privacy Impact Assessment

On the Treasury Board of Canada Secretariat Web site, you can get information for the Directive on Privacy Impact Assessment. This directive requires federal departments and agencies to conduct PIAs when:

- new programs or services raise privacy issues; or
- changes to programs or services affect the way personal information is collected, used, or disclosed.

More information

If you have questions about our PIA summaries, please contact:

Program Support and Training Group
Access to Information and Privacy Directorate
45 Rideau Street, 6th Floor
Ottawa ON K1A 0L5

Telephone:
613-960-5393 (Ottawa area)
1-866-333-5402 (toll free)

Email: ATIP-AIPRP@cra-arc.gc.ca

Date Modified: 2011-05-25

Privacy Impact Assessment Summary - Charities – Public Safety and Anti-Terrorism

Introduction

This document summarizes the Charities – Public Safety and Anti-Terrorism privacy impact assessment (PIA) prepared by the Review and Analysis Division (RAD) of the Canada Revenue Agency (CRA). RAD is responsible for delivering the Agency's mandate under the *Anti-Terrorism Act* to prevent the abuse of registered charities for the financing of terrorism. This PIA highlights the key points that demonstrate how privacy considerations have been factored into the development and implementation of RAD. For a detailed description of the personal information relevant to this program please refer to the personal information bank number CRA PPU 200 in Info Source at www.infosource.gc.ca.

Description

To contribute to the fight against terrorism financing, and fulfill its international obligations and commitments, Canada put in place a comprehensive domestic regime in 2001, integrated with its existing anti-money laundering regime, to counter terrorism financing. The regime is specifically designed to detect and deter terrorism funding and is administered and enforced through a horizontal structure that unites nine federal departments and agencies including the Canada Revenue Agency – Charities Directorate in a coordinated effort. These departments and agencies in turn work in close cooperation with other governmental entities and the private sector.

As part of the suite of legislation enacted in 2001 under the rubric of the *Anti-terrorism Act*, that facilitates the anti-terrorism regime, the Parliament of Canada enacted the *Charities Registration (Security Information) Act, An Act respecting the registration of charities having regard to security and criminal intelligence information*, (CRSIA). The law deals with the rare situation where classified intelligence information about terrorist activities is needed to exclude an organization from registration as a charity. In most situations, open-source information and normal procedures should be sufficient to establish if an organization does not meet the requirements for registration. The purpose of this legislation is three-fold:

1. to demonstrate Canada's commitment to participating in concerted international efforts to deny support to those who engage in terrorist activities;
2. to protect the integrity of the registration system for charities under the *Income Tax Act* (ITA), and
3. to maintain the confidence of Canadian taxpayers that the benefits of charitable registration are made available only to organizations that operate exclusively for charitable purposes.

Importantly, the legislation requires the balancing of two important principles, specifically that:

1. maintenance of the confidence of taxpayers may require reliance on information that, if disclosed, would injure national security or endanger the safety of persons; and
2. the process for relying on the information referred to in paragraph (1) in determining eligibility to become or remain a registered charity must be as fair and transparent as possible having regard to national security and the safety of persons.

It is within this framework that the Charities Directorate of the CRA established RAD as a standalone unit with specialized personnel who could work with other intelligence agencies to administer CRSIA and related provisions of the ITA.

The ITA was amended to allow for greater information sharing and use of information by the Canadian Security Intelligence Agency and the Royal Canadian Mounted Police and now also allows for information sharing with Financial Transactions and Reports Analysis Centre of Canada. It is because of this new information-sharing framework which helped operationalize the national security strategy that RAD established new mechanisms to collect, use and protect the personal information collected about directors, foreign agents, non-resident donors, employees of charities and organizations seeking to be registered as charities.

In regards to much of the personal information used by RAD, the Division also relies on the same information gathering tools developed and used by the Charities Directorate. The two main tools are the T2050, *Application to Register a Charity under the Income Tax Act* and the T3010-1, *Registered Charity Information Return*.

Furthermore, and consistent with other divisions of the CRA, RAD also relies on its own, specially trained team of auditors to conduct investigations relating to charitable organizations who may be abusing the charitable registration system in Canada. RAD auditors rely on Part XV of the ITA to conduct investigations related to the administration and enforcement of the ITA.

PIA Objective

This PIA demonstrates the parameters of RAD's collection, use, retention, disposal and destruction of personal information rooted within the framework of its administrative responsibilities in the Charities Directorate. The privacy analysis examined its adherence to the following 10 fair information principles:

Principle 1: Accountability for Personal Information

The CRA has designated the Director of RAD as the individual accountable for the personal information related to this PIA. To ensure performance requirements are met, the program has a number of security measures in place; audit trails, security and privacy training, in-house dedicated computer systems, system tracking and an on-site security advisor.

Principle 2: Collection of Personal Information

The purposes for the collection and use of the information is to protect the integrity of the registration system for charities under Canada's ITA by screening applications and monitoring charities for the risk of terrorist involvement. RAD analysts may consult open source and public databases for the enforcement and administration of the ITA and CRSIA.

Principle 3: Consent

A notice is included on both the application and on the annual returns of the organization that describes how the information may be shared with certain government departments and agencies. In addition, statutory authority derived from the ITA and CRSIA allows for the collection, use and disclosure of information as necessary for the Acts' administration and enforcement.

Principle 4: Use of Personal Information

All information collected is used for the administration and enforcement of the ITA and/or the CRSIA.

Principle 5: Disclosure and Disposition

Personal information that is disclosed to the public is related to the Charities Directorate's mandate to provide public information about charities and is authorized by the ITA. The personal information to be disclosed will be limited to what is required by or provided by legislation. Personal information shall be retained only as long as is necessary to fulfill those purposes.

Principle 6: Accuracy of Personal Information

Charitable organizations are required to file annual information returns, as part of the filing requirement; organizations are asked to certify that the information provided is accurate and complete. Where information obtained from a publicly available source demonstrates that the information on file is incorrect, the information will be verified to determine accuracy and corrected on the file. Where the information is found to be incorrect it will be discarded.

Principle 7: Safeguarding Personal Information

Security policies on the collection, transmission, storage and disposal of information are documented in chapters 5, 6, 7, and 8 of the CRA Finance and Administration Manual. System security was considered satisfactory based on the threat and risk assessment that was previously conducted. Use and access is authorized according to security clearance of user and is strictly on a "need to know" basis.

Principle 8: Openness of Information

The Charities Directorate maintains an accessible and regularly updated website at http://www.cra-arc.gc.ca/chrts-gvng/menu-eng.html. Embedded in that site are guides, forms and pamphlets that describe the work of the Directorate in great detail. This includes information that describes the various issues addressed by RAD in considering applications for registration by organizations and also when reviewing the information returns of registered charities.

Principle 9: Individual Access to Personal Information

Certain statutorily identified information is available on the CRA Internet in accordance with the ITA. Individuals can also request their personal information either through the *Privacy Act* or the *Access to Information Act*.

Principle 10: Challenging Compliance

CRA complies with complaint procedures established under the *Privacy Act* and Treasury Board Policies.

PIA Findings

The privacy analysis identified that RAD places privacy and security of information as an overarching and fundamental consideration in every aspect of its operations.

Date Modified: 2011-05-25

Privacy Impact Assessment Summary - Registered Disability Savings Plans

What is a Registered Disability Savings Plan?

Budget 2007 announced the introduction of a new Registered Disability Savings Plan (RDSP) whose purpose is to help parents and others save for the long-term financial security of persons with severe and prolonged disabilities.

The financial institutions that offer RDSPs to the public are known as issuers. The issuer must be a trust company licensed or authorized to carry on business in Canada. An individual who is a Canadian resident, eligible for the disability tax credit (DTC), and for whom an RDSP is established is the beneficiary. The beneficiary may be under the care of one or more primary caregivers. Lastly, the entity that opens an RDSP for a beneficiary is the holder. The beneficiary, their parent or other legal representative may become a holder.

The RDSP consists of three main elements:

1. **Contributions from individuals with the consent of the plan holder.** Contributions are limited to a lifetime maximum of $200,000. Contributions will be permitted until the end of the year in which the beneficiary attains 59 years of age.
2. **Amounts paid into the plan from the Canada Disability Savings Grant program (Grants).** Grants are paid at matching rates of 100%, 200% or 300% up to a maximum lifetime Grant limit of $70,000.
3. **Amounts paid into the plan from the Canada Disability Savings Bond program (Bonds).** Bonds of up to $1,000 per year will be provided to RDSPs established by low and modest-income families, up to a maximum lifetime Bond limit of $20,000, and will not be contingent on contributions.

The administration of the RDSP program is a shared responsibility between the CRA and Human Resources and Skills Development Canada (HRSDC). The Registered Plans Directorate is responsible for ensuring the requirements of the *Income Tax Act* are met with respect to the registration of RDSPs. HRSDC administers the program's Grants and Bonds in accordance with the provisions of the *Canada Disability Savings Act* and *Canada Disability Savings Regulations*.

Protecting Personal Privacy

A Privacy Impact Assessment (PIA) Report on the RDSP program was prepared by the Directorate to ensure that the CRA is compliant with privacy requirements as outlined in the *Privacy Act*, the *Income Tax Act* and Treasury Board Secretariat Policies. The purpose of this PIA Report is to determine if any privacy issues exist with respect to the Directorate's administration of the RDSP program and, if so, to provide recommendations on ways to mitigate or resolve them.

Summary of the RDSP PIA Report

The RDSP program involves the collection, use, disclosure and retention of personal information. The *Income Tax Act* provides the CRA with the authority to collect personal information for the purpose of administering the RDSP program. The privacy analysis examined the adherence to the ten privacy principles provided in the PIA Guidelines. The PIA Report has shown that:

- Personal information from the beneficiary, holder(s), primary caregiver(s), and legal representative (if applicable) is necessary to administer the RDSP program.

- Appropriate measures are in place for the custody and control of personal information. The institutions accountable have been documented.
- Only personal information necessary for program administration is collected. The Directorate collects personal information indirectly from HRSDC's Canada Disability Savings Program System.
- The CRA only discloses to HRSDC the required information needed to administer the *Canada Disability Savings Act* and *Canada Disability Savings Regulations*. Similarly, HRSDC only discloses the personal information necessary for the CRA to ensure compliance with the *Income Tax Act*.
- Personal information is safeguarded when transmitted between issuers and HRSDC because the data is encrypted. Information that is transmitted between HRSDC and the CRA is also encrypted and, thus, safeguarded.
- A description of the personal information maintained by the CRA with respect to the RDSP program is included in the CRA's Info Source chapter in the personal information bank entitled Registered Retirement and Deferred Income Plans (CRA PPU 226). Individuals can access their personal information either informally or through a formal *Access to Information Act* or *Privacy Act* request submitted to the CRA's Access to Information and Privacy Directorate.

Access to personal information is in accordance with the CRA information management, privacy, and security policies. An employee's *view access profile* limits the type of data they can access, ensuring that only authorized individuals have access to this data. To increase awareness of the importance of safeguarding personal information, the CRA provides security and privacy awareness training to its employees outlining relevant policies regarding breaches of security and privacy.

Date Modified: 2011-05-13