CBSA ASFC
PROTECTION • SERVICE • INTEGRITY
PROTECTION • SERVICE • INTÉGRITÉ

Faces on the Move: Multi-camera Screening

Privacy Impact Assessment (PIA)

Traveller Programs Directorate
Programs Branch
January 14, 2016

PROTECTED B

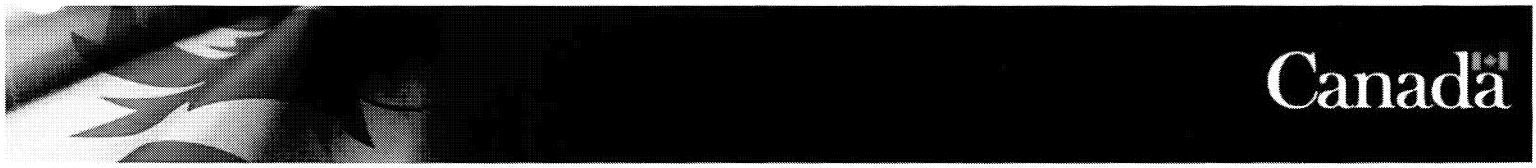

Table of Contents

EXECUTIVE SUMMARY

This privacy impact assessment (PIA) is intended to assess privacy risks within the Canada Border Services Agency's (CBSA's) planned demonstration of facial recognition (FR) technology at Pearson International Airport, currently expected to begin in early 2016. This project is divided into two phases. The demonstration phase will last for six months and will use facial recognition technology to match travellers against a database of previously deported persons (hereinafter referred as the "Previous Deportation Database" or PDD). This will be followed by a three- to six-month lab evaluation phase where the technology's performance will be assessed. Currently, the CBSA has no definitive plans to deploy this technology for full-time operational use. The solution described in the PIA is a demonstration to test the efficacy of FR software in an operational border context. The success or failure of the project will assist CBSA senior management in making further testing decisions regarding FR technology use within the border context. The CBSA recognizes that any future testing or use of FR technology will require an additional PIA.

This PIA has been drafted using the CBSA *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology* (*AV Policy*) and the *Policy on the Use of Wireless Technology*, as well as the associated Directives, the *Privacy Act* and the *Privacy Regulations*, and the *Immigration and Refugee Protection Act* (IRPA) as references. This PIA addresses only the *Faces on the Move* project, which is completely separate from the CBSA's existing use of Overt Audio/Video surveillance. The *AV Policy* was implemented on August 15, 2011, revised in November 2012, and updated again in July 2013. The current version the policy dates to November 2013. No audio will be collected or used in this project.

The CBSA has identified thousands of international travellers who have been denied entry to Canada or who have been deported after being admitted into Canada. These travellers have been deemed inadmissible for any of a number of reasons, such as security, criminality, health grounds, misrepresentation, or non-compliance with the IRPA. Many of these inadmissible travellers try repeatedly to re-enter Canada. The CBSA uses a list containing the names of previously deported persons and other, similar lists to identify inadmissible travellers at ports of entry (POEs). Many such travellers, however, use false identity documents, or even legally change their names in their home countries and obtain new, legal travel documents under their new names. Name-based lists such as those currently in use have inherent limitations which can be overcome using biometric technologies.

Although FR technology is widely available for a variety of applications, the use of face recognition with live video has not yet been tested in an operational environment by a Canadian law enforcement body. The CBSA is planning to conduct this demonstration of FR technology to assess whether this technology solution is effective, feasible, and accurate for identifying inadmissible travellers in a busy Port of Entry environment.

The CBSA plans to deploy multiple project-specific cameras in the CBSA-controlled area of the international arrivals section of Terminal 3 at Pearson International Airport. The cameras for this project will not be connected to the existing camera network that supports video surveillance at Terminal 3. Also, the project cameras are connected to the project's FR server and associated applications, but not existing CBSA information systems.

Areas and activities that may be monitored or recorded include, but are not limited to: approaches to the arrivals hall, approaches to Primary Inspection Line (PIL) booths, during PIL interviews, approaches

travellers seeking admission into Canada as they move through the CBSA-controlled area. This technology will not be used in Customs Controlled Areas outside the CBSA's traditional processes.

These cameras will record and store images of travellers' faces. No audio will be collected or used in the FOTM project. A dedicated FR system will compare these "live-capture" images with a database of stored images of persons who have previously been deported or removed from Canada that is specific to this technology demonstration . The system will notify CBSA officers when a match is detected. After human review of the match, an officer will be dispatched to find the traveller to refer them to secondary inspection. Some cameras, known as "scene cameras", will also record video of the areas under surveillance. These video recordings will show what a traveller is wearing and carrying and who they are with; this will make it easier for the CBSA to identify and find the traveller in the airport if the traveller is matched by the system with a person of interest.

As the CBSA has no guarantees that a PDD individual will enter through Terminal 3 during the project, volunteer CBSA employees (defined as "actors" throughout this document) will have their photographs and fictitious bio-data elements stored in the FR system as well.

After six months of operation, the equipment will be re-located from Terminal 3 to the CBSA's Science and Engineering Directorate (SED) lab in Ottawa, where further tests will be conducted to measure and possibly improve the system's performance.

Protecting your Personal Information

In order to carry out its mandate, the CBSA must collect a wide variety of personal information. The collection of this information is required in order for CBSA officers to make admissibility decisions regarding persons who wish to enter Canada. Although the CBSA is already using overt video surveillance, this technology demonstration will involve putting that information to a new use that supports the CBSA's admissibility determination processes. The differences between the current AV program and the *Faces on the Move* demonstration are in the ways the information will be used and the length of time it will be retained.

Through the use of closed-circuit television (CCTV) technologies, as described in the *PIA on the Overt Use of Video Monitoring and Recording Technology* that was submitted to the Office of the Privacy Commissioner (OPC) in November 2013, the CBSA is capturing the physical images of travellers or members of the public (although these images are not current being used to support admissibility decisions), in addition to the other elements of personal information already collected. Within the CBSA, only those employees who require access to video recordings or photographs as part of their duties are permitted to do so as per CBSA policies and procedures.

Some personal information collected through the *Faces on the Move* demonstration may be used in support of the CBSA's admissibility determination process. As a result, photographic and video records (excluding FR templates and related data) may be disclosed internally to CBSA personnel. Within the context of this time-limited technology demonstration, photographic and video records will *not* be shared with any external stakeholders.

Any access to or disclosure of facial photos, scene camera recordings, or PDD records will be governed by the provisions of the *AV Policy*.

Retention

The retention practices for the *Faces on the Move* demonstration will be governed by the provisions of the *AV Policy*, with some variances. In particular, facial photographs, some scene camera recordings, and PDD records must be retained until the end of the project. All records will be destroyed at the end of the project, except for records that were used for an "administrative purpose" (e.g., where a match was verified and a traveller was identified and diverted to secondary screening). Any records used for an administrative purpose will be retained for two years following the date of last use in accordance with s. 4 of the *Privacy Regulations*.

Right of Access

All records, regardless of storage medium, will be stored either in a locked cabinet (container or a safe) or in a secure room designed in accordance with specifications approved by the Infrastructure and Information Security Division of CBSA.

Records will be securely retained in accordance with established policies and guidelines, and may be disclosed within the CBSA. For the duration of this time-limited technology demonstration, records will not be shared with external organizations.

Individuals may formally request access to their personal information, or access to corporate records related to or created as a result of the *Faces on the Move* project by contacting the Access to Information and Privacy (ATIP) Division. More information about this can be found at: http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/menu-eng.html. In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the subject and date of correspondence, incident and location and legal authority for those acting on behalf of an account holder or estate.

Accountability

If individuals have concerns about the collection, use, disclosure or retention of their personal information, they may issue a complaint to the CBSA ATIP Division. Complaints should be made in writing, and include their name, contact information, and a brief description of their concerns. Contact information for the ATIP Division at the CBSA can be found here:

http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/contact-eng.html

To make a compliment, comment or complaint, the CBSA has made available a feedback form to help us to understand our clients and improve the delivery of our programs and services. Information on providing feedback can be found here:

http://www.cbsa-asfc.gc.ca/contact/com-eng.html

The CBSA posted a Video Recording and Monitoring Privacy Notice on its external website on November 19, 2012. This Privacy Notice states:

Privacy Notice

Video Monitoring and Recording

The Canada Border Services Agency (CBSA) uses video monitoring and recording technology to fulfill its mandate and to increase its ability to protect the public, and to protect employees and assets of the Agency. The use of video monitoring and recording technology is an integral part of the CBSA's security framework and operations management.

Cameras monitor and record CBSA operations at ports of entry and inland offices. Areas and activities that may be monitored or recorded include, but are not limited to: primary interviews, secondary examinations, interactions at CBSA information counters, cashier counters, commercial counters, detention cells, and interview rooms. Cameras may also monitor the movement of travellers and goods from one point in a CBSA operation to another, for example, from primary to secondary.

Use of Recordings

The CBSA collects personal information using overt video monitoring and recording technologies at ports of entry and inland CBSA service locations, to carry out the mandate of the CBSA under the authority of the Canada Border Services Agency Act. Recordings may be used to investigate suspected offences related to border legislation, and may be used as evidence in court proceedings. Recordings may also be disclosed as permitted by legislation to the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, and/or to municipal, provincial or local law enforcement agencies to investigate or enforce federal laws.

Retention and Disposal

Any new or replacement video monitoring and recording equipment must be able to retain recordings for no less than 30 days. Recordings that are used by the CBSA shall be kept for two (2) years following the date of their last use.

Upon expiry of the above retention periods, recordings are permanently deleted/overwritten, or in the case of removable media, recordings are physically destroyed.

Access to Information

Individuals have the right to access their personal information and the right to ensure their personal information is appropriately protected under the Privacy Act. The information collected is described in Info Source under the Overt Audio-Video Surveillance Personal Information Bank CBSA PPU 1104.

ABBREVIATIONS AND ACRONYMS

The following is a list of abbreviations and acronyms used in this report:

ATIP	Access to Information and Privacy (Division of CBSA)
AV	audio-video
AV Policy	*Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*
CA	certificate authority
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CCTV	closed-circuit television
CD	compact disc
CoP	Community of Practice
CPIC	Canadian Police Information Center
CSIS	Canadian Security intelligence Service
CSS	Centre for Security Science
CSSP	Canadian Safety and Security Program
DFD	data flow diagram
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DVD	digital video disc / digital versatile disc
FOSS	Field Operations Support System
FOTM	Faces on the Move
FR	Facial Recognition
GCMS	Global Case Management System
HR	Human Resources
I	identification
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IRB	Immigration and Refugee Board
IRPA	*Immigration and Refugee Protection Act*
ISTB	Information, Science and Technology Branch
MIDA	Multi-Institutional Disposition Authorities
MITS	*Operational Security Standard: Management of Information Technology Security*
MOU	Memorandum of Understanding

N/A	not applicable
NCMS	National Case Management System
OPC	Office of the Privacy Commissioner
PAA	program activity architecture
PDP	Previous Deportation Database
PIA	privacy impact assessment
PIB	personal information bank
PIL	Primary Inspection Line
PKI	public key infrastructure
POC	Privacy Oversight Committee
POE	port of entry
PSC	Public Safety Canada
RCMP	Royal Canadian Mounted Police
RDA	Records Disposition Authority
RFID	radio frequency identification
SED	Science and Engineering Directorate
SIN	social insurance number
SoS	statement of sensitivity
TBS	Treasury Board of Canada Secretariat
TC	Transport Canada
TRA	threat and risk assessment
USB	universal serial bus
VPN	virtual private network
Wi-Fi	A trademarked term that identifies wireless networking products that comply with the IEEE 802.11 standards

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Administrative purpose	The *Privacy Act* defines an "administrative purpose" to be the use of an individual's personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Facial recognition	As used in this report, is the technologies and processes used to identify a person by comparing a digital image or video frame of the person's face with a database of known facial images.
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the *Privacy Act*. Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in *Info Source* PIBs, as applicable. The *Info Source* publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Primary Inspection Line	The term "Primary Inspection Line" is used to refer to the point at which the person entering Canada makes a report of his or her person and goods as required under the *Customs Act* and the IRPA. The CBSA has PIL booths from which officers conduct primary examinations.
Scene camera	A video camera deployed as part of the *Faces on the Move* project that records wide-angle video scenes at various locations in the CBSA-controlled areas of Terminal 3 at Pearson International Airport. When a potential match from the Previous Deportation Database is identified, a short video clip from a scene camera will be added to the match record. The video clip will be centred in time and space on the matched facial image. It will show the larger context of the potentially matched traveller by showing what the traveller is wearing and carrying and the people around the traveller.
Transitory Record	As defined by Library and Archives Canada and for the purposes of this policy are those records that have no enduring value to the CBSA. They are records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record but **do not** include records that are required to control, support or document the delivery of programs, to carry out operations, to

	make decisions, or to account for activities of government. (Source: *MIDA 2.1*, 4. Definition)
Previous Deportation Database	A database of selected previously deported persons created specifically for the *Faces on the Move* project. The database will contain facial images and related biographical information (e.g., name, date of birth, warnings) extracted from the CBSA's existing Previously Deported Persons list. The database will contain entries for persons who have been deemed highly likely to attempt to return to Canada during the *Faces on the Move* demonstration.

SECTION 1 – INTRODUCTION

This section below provides an overview of the project. It is supported by the remaining sections of this PIA and is intended to ensure a description of the project is clear at the onset of reviewing this document.

A. Background/Overview

In 2014, the Canadian Border Services Agency (CBSA) received funding from the Defence Research and Development Canada (DRDC) for a project that will test the readiness of facial recognition (FR) technology as a means of screening against a database in an operational environment. This Privacy Impact Assessment (PIA) provides the background on the project, its partners, the test period (herein referred to as the "demonstration period"), the evaluation period, and the associated privacy risks. The project is called *Faces on the Move* (*FOTM*).

B. DRDC and CSSP[1]

As an agency of Canada's Department of National Defence (DND), the DRDC provides DND, the Canadian Armed Forces (CAF) and other government departments as well as public safety and national security communities the knowledge and technological advantage needed to defend and protect Canada's interests at home and abroad.

In 2012, the DRDC established the Canadian Safety and Security Program (CSSP), which aims to invest in science and technology projects that will strengthen Canada's ability to anticipate, prevent, mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime, and terrorism. The CSSP is led by DRDC's Centre for Security Science (CSS), in partnership with Public Safety Canada (PSC) and uses a collaborative model that gathers the best minds from government, industry, academia, response and emergency management agencies, and international organizations to work on the most pressing safety and security issues facing Canadians.

That collaborative model extends to the manner in which the CSSP/DRDC provides funding for various types of projects, which must meet CSSP requirements identified through risk and vulnerability assessments and are associated with the priorities established by the CSSP; one of which is border and transportation security. CSSP-funded projects allow public safety and security professionals to work with science and technology experts to identify challenges, develop knowledge and tools, and provide advice that will help protect Canada, its people, and institutions. Currently, the CSSP funds approximately 200 projects and activities which are led by either federal, provincial, territorial and municipal governments, or academic institutions, through federal contracting mechanisms managed by Public Works and Government Services Canada.

One of the funding avenues for the CSSP is the Call for Proposal process which invites all levels of government, industry, and academia to submit project proposals for innovative science and technology solutions to address identified risks, vulnerabilities, and gaps in public safety and security capabilities. In the spirit of the CSSP's collaborative framework, proposals often team up private sector expertise with government programs to address a specific issue. Upon approval by the DRDC of a proposal, the lead

[1] This section was adapted from multiple sections of the DRDC website found here: http://www.drdc-rddc.gc.ca/en/index.page.

organization is able to use the DRDC funds to hire its partners (identified in their proposal) to assist in project delivery.

C. CBSA Proposal and Project

In 2013, the CBSA submitted a proposal to the DRDC/CSSP via the Call for Proposal process to seek funding to test FR technology within a border context. The proposal included the following private sector and academia partners:

- Face 4 Systems (formerly known as NextGenID)
- ADGA Group Consultants Inc.
- Université du Québec – Montréal (specifically the École de Technologie Supérieure - ÉTS)

In 2014, based on the CBSA proposal, the DRDC awarded funds to the CBSA to assist in the testing of FR technology. In-kind funding by the CBSA through the use of employee resources, project management, and technical expertise was needed to ensure the project budget was appropriate.

Within the CBSA, the Information, Science and Technology Branch (ISTB), and specifically the Science and Engineering Directorate (SED), will lead the project in consultation with Programs Branch and Operations Branch. The Traveller Program Directorate is the Programs Branch sponsor and, in part, is the approving authority for this PIA. ISTB has led a working group consisting of working-level representatives from the following areas to ensure broad consultation and awareness of the project:

- Comptrollership (Security and Professional Standards)
- Corporate Affairs (Communications and ATIP Policy & Governance)
- Border Operations
- Enforcement and Intelligence Operations
- ISTB
- Traveller Program Directorate
- Traveller Program Transformation
- Greater Toronto Area Region (location of the demonstration – Pearson Airport)

The purpose of the project is to demonstrate the readiness of FR technology for potential screening applications. The CBSA anticipates the technology could assist in overcoming some of the limitations of name-based lists. Specifically, it can assist in identifying travellers who are known to be inadmissible who seek to enter Canada using false identity documents or documents issued under different names.

The demonstration period will begin in early 2016 (for period of six months) at Terminal 3, Toronto Pearson International Airport (YYZ). In order to demonstrate the solution, additional cameras will be installed and configured before the beginning of the six month-long demonstration period. In addition to camera installation, a secure server, workstation equipment, handheld devices, and software will also be installed. The cameras and associated wiring will operate separately from the existing CCTV network within the terminal and will be positioned and utilized in accordance with the CBSA's *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology;* it is noted that only images and video are captured by the project-specific cameras and audio will not be captured or used.

D. Project Roles and Responsibilities

The funding provided by the DRDC allows for the CBSA to procure the services and products of the partners identified in the proposal. Therefore, once the DRDC approved the funding, the CBSA was able to sole-source hardware, software, and consulting services from the proposal partners. In that regard, the following provides an overview of the roles and responsibilities of partners and stakeholders in this project:

1. Defence Research and Development Canada (DRDC)
   The *FOTM* project is managed by the DRDC's CSS with CBSA's SED providing the project management function. The DRDC provides oversight to ensure its funding is used appropriately.

2. CBSA Science and Engineering Directorate (SED)
   SED, a directorate under ISTB, will manage the project, coordinate all entities of the project, and is responsible for internal reporting (CBSA senior management) and external reporting (DRDC). The funds provided by the DRDC require quarterly reports as well as a final report which the SED is responsible for producing. From an IT Project Management perspective SED is the Project Authority and the Technical Authority.

3. Face4 Systems (formerly NextGenID)
   Face4 Systems is a Canadian-based (Ottawa) company which designs, develops, deploys and supports FR security products, services and solutions for government and private organizations around the world. Face4 Systems' products focus on live face capture and face image quality analysis and processing. The company is a value added re-seller of FR software made by Cognitec, which is headquartered in Dresden, Germany with satellite offices in the U.S., Australia, and Canada. For this project, Face4 Systems will provide the following:

   - Purchasing cameras, server, desktop workstation (for BSO Adjudicator) and the handheld devices (For BSO Rover)
   - Installation and removal of the above products
   - Training on the products
   - Component testing of the products
   - Technical support
   - Assist in evaluating the results of the demonstration

   Face4 Systems staff will have access to the PDD photos, images and videos taken from the cameras, and other personal information as part of its responsibility to assist in evaluating the demonstration. Access to all personal information will be limited to a CBSA location.

4. Université du Québec (École de Technologie Supérieure (ÉTS))
   Scientists from the ÉTS are not involved during the demonstration period, but will develop the test plan and system assessment methodology for post-demonstration scientific analysis during the evaluation period. After the demonstration, ÉTS staff will analyze performance data (match scores) from the Montreal campus of the University of Quebec. The performance data does not include any personal information.

5. ADGA Group Consultants, Inc.
   The ADGA Group is responsible for authoring the PIA for the project. The company and its consultants play no further role in the project.

As part of any CSSP-funded project, there are two additional participants that are best described as passive participants: the Community of Practice (CoP) and an External Advisory Committee.

1. Community of Practice
   Communities of Practice (CoPs) are groups of subject matter experts brought together by CSSP who share a common interest in a given area of expertise and work together to facilitate knowledge-sharing and collaboration. CoPs are an essential element of the CSSP, providing access to a rich pool of collective knowledge and experience to support the development of new or enhanced science and technology knowledge and capabilities and to provide advice and guidance in the development of evidence-based policy, decision-making and operational and strategic planning. Members of the CoP may be provided access to regular project updates, the final scientific analysis report, and may be invited by DRDC to attend a final presentation; however, none of the information provided to the CoP contains the personal information of actors or individuals from the PDD.

   For this project the CoP includes the following government institutions: Canadian Security Intelligence Service (CSIS), Transport Canada (TC), Royal Canadian Mounted Police (RCMP), and the CBSA.

2. External Advisory Committee
   The External Advisory Committee comprises organizations that have expertise or interest in the area of a DRDC-funded project; in this case, biometrics. The Committee meets quarterly and provides the project with feedback on relevant information from the subject area.

   For this project, the External Advisor Committee includes: CBSA, RCMP, PSC, TC, Calgary Police, the Office of the Privacy Commissioner of Ontario, and the U.S. Department of Homeland Security. These organizations have had prior experience or involvement in projects related to FR technology. For example, the Ontario Privacy Commissioner has experience with the implementation of FR in Ontario casinos to identify self-reported problem gamblers attempting to enter a casino. Also, the Calgary Police has implemented FR technology to match crime-scene photos to its collection of mug shots.

   The Committee is not provided any reports or verbal communication containing the personal information of actors or PDD.

E. Overview of the Technology Demonstration

Section 6 of this PIA provides a detailed explanation of the technology demonstration and how it will be deployed, utilized, and analyzed. The diagram and text that follows is provided as a high level explanation, which supports Section 6.

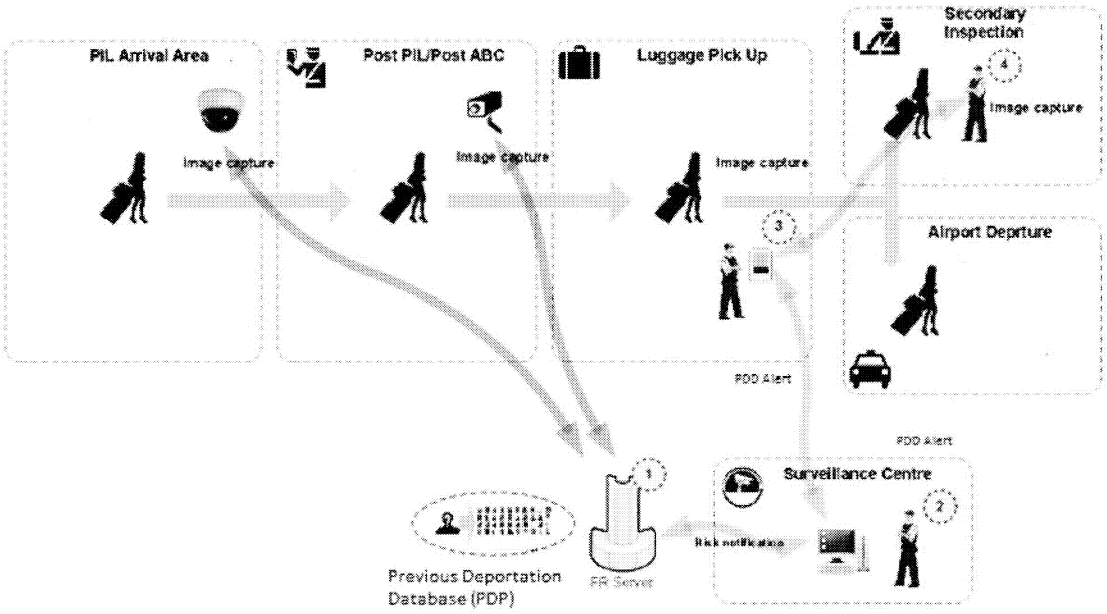

Figure 1: High-level System Overview

1 As part of the project, a dedicated server will be installed with no connection to any CBSA information system or to the existing CCTV network. The server will run the FR software and will be connected to the cameras that will be installed solely for this project. The server will also store personal information on two groups of individuals: the control group, who are actors from among volunteer CBSA employees; and the operational group, which consists of extracts from an existing inventory of Previously Deported Persons maintained within existing CBSA systems. The database that will be uploaded to the server will be limited to 5,000 individuals who have been previously deported and have attempted to return to Canada at least one time in violation of their removal order.

In this first step, the cameras will capture still images and video of individuals entering the CBSA-controlled area at Terminal 3 of Pearson International Airport. The images will be sent to the FR server and matched with the previously uploaded PDD and actors using FR software provided by Face4 Systems.

2 In Step 2, if the FR software identifies any potential matches, it sends a match notification to a Border Security Officer (BSO), identified for the purposes of this project as an "adjudicator". The dedicated workstation located inside a secure Surveillance Centre will have an application installed locally that receives the possible match notification from the FR server and prompts the adjudicator for a decision. The adjudicator is presented with an image of the match from the PDD and images from the Terminal 3 cameras to make the adjudication decision, as well as a five second video of the individual.

3 If the BSO adjudicator believes a match has occurred, a BSO Rover (BSO patrolling the CBSA-controlled section of the airport) is notified via a project-specific handheld device. Communication between the adjudicator workstation and the Rover BSO handheld device is over a cellular network consistent with the CBSA's *Policy on the Use of Wireless Technology*. The device will

provide the Rover BSO with an image of the individual, a five-second video taken from the project-specific cameras and data from the PDD (Name, DOB, FOSS ID#, and alerts). The Rover BSO will use this information to locate the individual and validate the adjudicator's match assessment.

4 Assuming the Rover BSO is confident that a match exists, the individual is referred to secondary examination at Terminal 3 where a BSO will assess the individual's identity and admissibility to Canada. Upon escorting the individual to secondary, the Rover BSO will inform the secondary BSO that a FOTM match has occurred. All BSOs working in Terminal 3 are aware of the FOTM demonstration and that any FOTM match requires independent validation using existing systems and procedures for potential matches of the PDD. FOTM procedures for secondary immigration BSOs will clearly state the requirement that any FOTM match requires independent identity validation using existing systems and procedures.

When an operational match results in action being taken with respect to a traveller, such as a referral to secondary examination, the match record, including all PDD information, live-capture photos, and scene video, will be exported to secondary storage (CD, USB, or similar) in accordance with CBSA policies, which require that any interaction with a traveller (i.e., referring the individual for secondary examination based on the FR demonstration) must be kept for two years. The storage device will be kept on the individual's file, so that a permanent record of the information that led to the action can be preserved; however, evidence supporting deportation will be limited to the identity validation efforts of the secondary immigration BSO. If deportation is the result of the secondary examination, then non-FOTM data, including video from existing Terminal 3 cameras, will be used to support the deportation proceeding. Only in rare and extraordinary cases does CBSA envision FOTM data being a supporting piece of information in a deportation proceeding.

For the four-step process outlined above and shown in Figure 1 above, the FR system will be configured to send a match notification to the adjudicator only if a potential match has a high probability of being a true positive match. This will reduce the number of false positives (where the system incorrectly matches a traveller's face with an image from the PDD sent to the BSOs.

F. Post-Demonstration Analysis and Report to DRDC

Once the six-month demonstration period is over, the technology will be removed from the airport for an additional three to six months of evaluation in a lab setting. The project will remove the FR server, cameras, wiring, adjudicator workstation, and the handheld devices. The only potential change to the removal plan is that the project cameras may be provided to the POE and be re-wired as they are no longer valuable to the demonstration after the demonstration period. At the writing of this PIA, a final decision on whether to provide these cameras to the POE had not been made.

Also following the demonstration period, representatives from the CBSA's SED (as the project lead), Face4Systems, and the ÉTS will analyze the demonstration data to scientifically examine the results. Face4 Systems staff will have access to the personal information that was used during the demonstration to determine the effectiveness of the software. Their access to personal information will be restricted to a CBSA location.

Additionally, scientists from the ÉTS will analyze performance data from the demonstration, which will not include any personal information. ÉTS access to the performance data will be performed outside of a CBSA location. ÉTS will be given access only to performance metrics (i.e., match scores) and not to personal information of particular cases/individuals.

G. Goals of the Project

It is critical to this PIA that there is a clear understanding regarding the goal and intent of the project, which is to scientifically test FR software in a border context.

Therefore, the goal of the project is simply to scientifically test the technology. This PIA and the project is not a Pilot Project to test a solution for possible future implementation. There is no underlying plan within the CBSA to implement the FR software after the demonstration. The test results of the solution may support future CBSA decisions on how to further test FR, but the CBSA is clearly in the very early stages of making a decision on whether FR technology can be used effectively in a border context.

As part of the funding provided by the DRDC, the project team is required to write a scientific report on the demonstration and the test results. The report will be made public on the DRDC website and disseminated to project stakeholders. The report may also be reviewed by members of the CoP and the Advisory Committee. It will not contain any personal information.

H. Scope of the PIA

The scope of this PIA is limited to the technology demonstration that is managed by the CBSA's SED and supported by the other CBSA Programs and external organizations as outlined in the previous section of this document. As this is substantially different from how the CBSA uses both video surveillance and biometric technologies, this PIA has been written to ensure the demonstration is considering the privacy implications of the project. By analyzing the privacy principles in conjunction with the demonstration, the CBSA is ensuring privacy and the scientific analysis of the technology are both considered when the Agency makes future decisions regarding FR technology.

This PIA identifies two sets of risks: one that are inherent to the demonstration itself and another that are anticipatory and based on the potential future testing and use of FR technology to identify individuals in CBSA controlled areas. The latter group of risks are advisory in nature and have no bearing on the actual scope of this PIA – the demonstration of the FR technology. Privacy considerations of the "actor" group have not been included in the scope of this PIA because this group consists of volunteer participants and will not be used for an administrative purpose.

The CBSA is committed to ensuring that privacy is strongly considered in relation to the use of audio-video monitoring and recording technology. If any future projects stem from the scientific results of this project, subsequent PIAs will be written to ensure privacy risks and their related mitigation strategies are identified before deployment. The CBSA will also ensure subsequent PIAs provide a detailed description of the scientific results of the current demonstration. Moreover, CBSA ATIP will continue to provide updates to the OPC on various privacy-related projects at the CBSA, including but not limited to, any further use of FR and audio-video monitoring and recording.

SECTION 2 – OVERVIEW AND INITIATION

Government Institution: Canada Border Services Agency

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the *Privacy Act*
Barry Kong, Director, Program Compliance and Outreach Division, CBSA	Dan Proulx, ATIP Director, CBSA

Name of Program or Activity of the Government Institution:

Faces on the Move: Multi-camera Screening

Description of Program or Activity:

Faces on the Move: Multi-camera Screening is a Project under the Canadian Safety and Security Program (CSSP) managed by Defence Research and Development Canada (DRDC). The purpose of the project is to demonstrate the operational readiness of FR technology.

The CBSA will demonstrate FR technology to assess its potential for supporting existing programs as an integral part of its security framework to support its admissibility determination and immigration enforcement processes. The use of FR technologies could support the Enforcement, Facilitated Border, and Conventional Border programs, and could increase the CBSA's ability to meet its mandate and its ability to protect the public and its employees. These potential uses provide the necessary justification for CBSA being involved in the testing project, but the project is only intended to test the effectiveness of a FR-based traveller processing solution and provide a scientific assessment of the technology's readiness level. That assessment will be used by the CBSA, and other members of the CoP, to better enable the Border and Transportation Security Community on the current state of FR technology.

Most cameras deployed for this project will monitor and record still images of travellers' faces in the CBSA-controlled areas of Terminal 3 of Toronto's Pearson International Airport. A smaller number of "scene cameras" will record video of travellers as they pass through this area. Areas or activities where travellers' facial images may be recorded include, but are not necessarily limited to: approaches to the arrivals hall, approaches to PIL booths, during PIL interviews, and the approach to immigration point.

Recorded facial images will be compared automatically to a database of persons of interest to CBSA. No audio will be collected or used in the FOTM project. The database will consist of facial photographs and basic biographical information (name, date of birth, FOSS ID#, and alerts) of actors and from CBSA's existing Previously Deported Persons list. All potential matches that have a high likelihood being a true match between an arriving traveller and a person on the PDD will be adjudicated immediately by a CBSA officer. Potential matches with a low likelihood of being a true match will be reviewed, in bulk, for statistical analysis purposes between one to seven days after the travellers' facial images were recorded. For each potential match, a short video clip (from a scene camera) taken at the same time as the facial photograph will be stored on the FR server dedicated to this project (no connection to any CBSA information system). Verified high-likelihood, real-time matches will be communicated to roving CBSA officers in the airport, who will attempt to find the traveller and ask him or her to report to secondary examination for further discussion. The video clip will aid in identifying the traveller by showing what

the traveller is wearing and carrying. Verified lower-likelihood, non-real-time matches will be analyzed statistically, with an objective of reporting on system performance and limitations.

ADMISSIBILITY DETERMINATION

Through the Admissibility Determination program, the CBSA develops, maintains and administers the policies, regulations, procedures and partnerships that enable border services officers to intercept people that are inadmissible to Canada and to process legitimate people seeking entry into Canada within established service standards.

In the traveller stream, border services officers question people upon arrival to determine if they meet the requirements of applicable legislation and regulations to enter Canada. Border services officers will then make a decision to grant entry or refer a person for further processing (e.g. payment of duties and taxes, issuance of a document), and/or for a physical examination.

IMMIGRATION ENFORCEMENT

The Immigration Enforcement Program determines whether foreign nationals and permanent residents who are or may be inadmissible to Canada are identified and investigated, detained, monitored and/or removed from Canada.

Foreign nationals and permanent residents of Canada believed to be inadmissible are investigated and may have a report written against them by a CBSA inland enforcement officer. Depending on the type of inadmissibility, the merits of the report are reviewed. Subsequent to this review, a removal order may be issued against the foreign national or permanent resident in question. Removal orders issued against refugee claimants are conditional and do not come into force until the claim against the removal order is abandoned, withdrawn or denied by the IRB.

REMOVALS

The Removals Program (a sub-program of Immigration Enforcement) ensures that foreign nationals and permanent residents with an enforceable removal order are removed from Canada. Once a person is removal-ready, an interview is conducted to ensure that a travel document is available and that a pre-removal risk assessment is offered by a CBSA inland enforcement officer. Where a valid travel document is not available, CBSA inland enforcement officers liaise with foreign embassies to secure the required travel documents.

Note: This should align with the program named and described in the institution's Info Source Chapter as required under section 5 of the *Access to Information Act*. For institutions that develop a Program Activity Architecture (PAA) as per the Management, Resources, and Results Structure Policy, the institutional Info Source chapter must align with the programs, activities and sub-activities described in the PAA.

Description of the class of records associated with the program or activity:

CBSA BPD 1101

Records include audio/video footage of CBSA operations including primary inspection line (PIL) interviews; secondary examinations; interactions at CBSA information counters, cashier counters, commercial counters, in detention cells, and in interview rooms to record audio statements made under the *Immigration and Refugee Protection Act* (IRPA).

CBSA ENF 135

Records related to the Removals Program which enables the CBSA to remove from Canada

individuals who have contravened the *Immigration and Refugee Protection Act (IRPA)* and who are subject of an enforceable removal order. May include records related to the establishment or use of electronic systems used to administer or manage the program including the Global Case Management System (GCMS) and the National Case Management System (NCMS) and the Canadian Police Information Center (CPIC).

CBSA ENF 137

Information from the enforcement records of persons who have come under examination at a port of entry or an investigation at an inland office. Personal information may include name, address, birth date, country of birth, enforcement action undertaken (i.e. inadmissibility reports, arrest reports, hearing or removal under the *Immigration and Refugee Protection Act* (*IRPA*)), fingerprints, digital photographs, personal histories of refugee claimants, immigration applications and the date and place of each event in the process.

Class of Record Number: CBSA BPD 1101; TBS Registration: 20110287; Bank Number: CBSA PPU 1104

Class of Record Number: CBSA ENF 135; Bank Number: CBSA PPU 1301

Class of Record Number: CBSA ENF 137; TBS Registration: 005218; Bank Number: PPU 032

☐ Proposal for a New Personal Information Bank

N/A

☐ Proposed new Standard Personal Information Bank
☐ **Proposal to modify an existing Standard Personal Information Bank** - identify Standard PIB number and current description:

N/A

Legal Authority for Program or Activity:

Immigration and Refugee Protection Act

- Sections 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2)

Immigration and Refugee Protection Regulations

- Sections 28, 28(a), 28(b), 28(c), and 28(d)

Note: Prior to proceeding with the assessment it is essential that Parliamentary authority for the relevant program or activity be established. Generally, Parliamentary authority is usually contained in an Act of Parliament or subsequent regulations, or approval of expenditures proposed in the Estimates and authorized by an *Appropriations Act*. If legal authority is unclear consult your Legal Service to determine authority for the program or activity. (See question 1 of **Section V**)

Summary of the project / initiative / change:

The CBSA works to promote the free flow of travellers and goods into and out of Canada, while ensuring that security measures are in place to stop and remove potential threats. Keeping Canada's border open to travel and trade, but closed to criminal activity requires the CBSA to manage border operations effectively.

With a workforce of approximately 14,000 employees, the CBSA provides services at 1,200 points across Canada. The CBSA also administers more than 90 acts, regulations, and international agreements, many on behalf of other federal departments and agencies, the provinces, and the territories. In calendar year 2013, the CBSA processed 99.7 million travellers and 14 million commercial shipments.

The CBSA will demonstrate FR technology to assess its potential to support existing programs as an integral part of its security framework to support its admissibility determination process. The use of FR technology may increase the CBSA's ability to meet its mandate and its ability to determine the admissibility of persons seeking entry to Canada. However, the intent of the FOTM project is to test the solution and assist CBSA senior management in any decisions to further explore FR technology.

Project -specific cameras will monitor and photograph travellers' faces and record video of their overall appearance in the CBSA-controlled areas of Terminal 3 of Pearson International Airport. Areas and activities that may be monitored and photographed include, but are not limited to: approaches to the arrivals hall, approaches to PIL booths, during PIL interviews, approaches to immigration point, and within immigration secondary.

Currently, signage at Terminal 3 includes a bilingual placard that states the following:

> "This area is under video surveillance. Recordings may be used and shared in accordance with applicable federal legislation. For more information on the CBSA's use of these recordings, please ask to speak with a supervisor or visit www.cbsa-asfc.gc.ca"

At the CBSA, the location of monitoring and recording signage must adhere to three Agency-developed principles:

1. Signs must be posted anywhere video recording technology is being used (Note that the *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology* places limitations on the use of AV technology).

2. Signs must be posted (in order of preference) in at least one of the following areas: just prior to entry to a CBSA-controlled area; at entry points to a CBSA-controlled area, or as soon as possible after entry to a CBSA-controlled area.

3. Signs must be hung in conspicuous locations to allow travelers a reasonable opportunity to know that the area that they are in, or about to enter, is under surveillance.

FR technology will compare the facial images collected from arriving travellers and compare them with images of persons of interest on the pre-generated PDD. When the FR system finds a potential match between a traveller and a PDD entry, it will attach a short video clip of the traveller (taken by a *FOTM* scene camera). If a potential match has a high likelihood of being true, the FR system will immediately notify a CBSA Border Services Officer (BSO) in the Surveillance Centre. The BSO will manually review the collected image, video, and the PDD image and make a final adjudication as to the accuracy of the match. The BSO will send an alert about the verified match to roving BSOs in the immigration hall using wireless technology. The roving officer will receive the alert via a handheld device provided for this demonstration (this handheld device is unique to the *FOTM* demonstration and will not be used for any other purpose; these devices will be removed at the end of the demonstration). The roving BSO will search for the identified person and, upon finding the person, direct him or her to secondary examination. In secondary examination, existing systems and procedures will be used to process the traveller. BSOs working immigration secondary have been made aware of the FOTM demonstration and new procedures require them to validate the identity of the individual separate from the FOTM match.

FR could assist the CBSA in ensuring the integrity of the border by capturing information relating to persons who contravene the *Immigration and Refugee Protection Act* (*IRPA*). For example, FR could assist in detecting contraventions of the following sections of the act:

- *IRPA* section 15, which grants the CBSA the authority to examine persons applying to enter Canada
- *IRPA* section 16, which requires persons making such applications to respond truthfully to the examination
- *IRPA* section 18, which requires every person seeking to enter Canada to appear for an examination to determine the person's admissibility to Canada

Cameras will not be placed in any area where CBSA business is not conducted, or in any area where there would be a heightened expectation of privacy, such as public or employee washrooms, lunch rooms and locker rooms. Information related to travellers, facility employees (non-CBSA) or other members of the public (transport drivers, flight attendants, brokers clearing goods, etc.) is considered to be personal information as defined in section 3 of the *Privacy Act*. For the purposes of this activity and this PIA, any CBSA employee information captured in facial photographs that relates to the function or the position of the employee is not considered to be personal information, in accordance with paragraph 3(j) of the *Privacy Act*. Any information captured related to an employee that does not specifically relate to his/her function or position will be treated as personal information per section 3 of the *Privacy Act*.

The CBSA recognizes that it has broad authorities to stop, question, search, detain and arrest travellers and seize goods and information in the border context. It further recognizes that, in order to carry out its mandate to ensure the safety and security of the Canadian border, it collects and is entrusted with a wide variety of personal information. The CBSA is committed to adhering to all privacy laws and to ensuring that not only are individuals appropriately notified of any collection of personal information, but that all of the information collected is appropriately protected.

The use of FR technology is a new activity. Use of this technology will be guided by the CBSA's overarching policy on the use, retention, disclosure and disposal of audio and video equipment and recordings. Standard Operating Procedures will be drafted to govern the specifics of the *FOTM* project. The CBSA is conducting this PIA to ensure that the privacy risks associated with using, retaining, disclosing and disposing of personal information collected in the course of demonstrating FR technology are adequately addressed.

This PIA reflects the CBSA's planned use of FR technology at Pearson International Airport beginning in early 2016 for period of six months, during which project personnel will analyze the performance of the technology. This will be followed by a three- to six-month lab evaluation phase where the technology's performance in relation to the information collected during the demonstration will be further assessed. At this time, the CBSA has no plans to deploy FR technology for ongoing operational use, regardless of the performance of the technology in this limited demonstration. The testing results may assist future senior management decision on further exploration of FR at the CBSA, but at this time, there are no definitive plans to implement such technology.

This PIA has been drafted using the *AV Policy* as well as the associated Directives, the *Privacy Act* and the *Privacy Regulations*, and the *Immigration and Refugee Protection Act* as references. The *AV Policy* was implemented on August 15, 2011 and revised in July 2013. No audio will be collected or used in the FOTM project. The Agency recognizes that the use of the AV policy for traveller processing is a new use which is not currently included in this Policy.

The FOTM project is a project of the Canadian Safety and Security Program (CSSP), managed by Defence Research and Development Canada's (DRDC) Centre for Security Science (CSS). The CBSA is the government lead for the project.

SECTION 3 – FOUR-PART TEST

The section provides a discussion related to the scope of this PIA and an assessment against the four-part test.

The CBSA recognizes that the four-part test, in part, requires an assessment as to whether the initiative will be effective in achieving a specific purpose. However, this initiative is unique in that it is not a Pilot Project or a Proof of Concept that is being tested so the tested solution can be modified for future use. Instead, the purpose of this project is to provide a foundational dataset regarding the effectiveness of this technology as a whole. This may be used by the CBSA, or its partners, to inform any future plans to deploy FR technology. This careful approach has been taken in recognition of privacy sensitivities inherent in a FR-based matching program.

The four part assessment below must be read with the understanding that it is limited to the scientific evaluation of an FR technology demonstration and does not apply to the application of FR technology within the CBSA's current traveller processing programs. Any future demonstration or testing of FR will result in a PIA that will draw upon the scientific research garnered from this project and be further assessed against the four-part test.

1. Is the measure demonstrably necessary to meet a specific need?

   There are many cases of non-Canadians using false names in attempts to enter Canada illegally.

   A report by the PBS television show "Frontline" explored how terrorists use fake identity documents to travel the world. The report focused on Ahmed Ressam, the so-called "Millennium Bomber", who first entered Canada in 1994 using a fake French passport. (see http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html).

   In 1970, Palestinian Mahmoud Mohammad Issa Mohammod was convicted in a Greek court of manslaughter and other charges related to an attack against an Israeli airliner that he participated in. This conviction made him inadmissible to Canada. Yet in 1987, he managed to enter Canada under a false name. It took until 2013 for him to be deported (see http://www.nanaimodailynews.com/news/palestinian-deported-from-canada-1.177617#).

   A U.S. citizen was a fugitive from American justice when he used a false name to enter Canada in 2008. He was eventually arrested and sentenced for crimes he committed in Canada before being deported back to the United States (see http://www2.canada.com/saskatoonstarphoenix/news/local/story.html?id=07cf4ad2-5d05-4e65-bf2f-fcebd0188783).

   In 2011, an Iranian man in Canada was ordered deported for the second time after being convicted of people smuggling. He provided false identity documents to smuggle Iranians to various countries, including Canada. He also used false passports to enter Canada in 2008 after being removed in 2007

(see http://news.nationalpost.com/2011/09/23/canada-orders-deportation-of-iranian-suspected-of-human-smuggling/).

A judgement was rendered in 2013 against a Portuguese citizen who had been previously deported from Canada five times. On at least one of those occasions, he tried to enter the country using a passport with a false name. In this most recent case, he also used a false passport, although this time the name he was using was on a list (see http://visalawcanada.blogspot.ca/2013/12/portuguese-national-deported-five-times.html).

A man who entered Canada as a refugee in 2003 was arrested in 2014 in connection with a 2000 murder in Texas. Although the man claims he is not the person wanted in the murder case, fingerprints and photographs have led authorities to conclude he is the same person. According to the news report at http://bc.ctvnews.ca/cbsa-arrests-man-in-gruesome-2000-murder-in-texas-1.1765595, the man may have identity documents with several different names on them.

The examples above are cases that made the news of people using false names to evade the CBSA's name-based lists. The CBSA has statistics showing that, just at Terminal 3 of Pearson International Airport, an average of 16 travellers per year were detected using fraudulent, altered, or borrowed travel documents between April 2011 and March 2014. In other words, these people were using documents to claim they were someone else. There is no estimate available for how many people used such documents and were *not* detected.

2. Is it likely to be effective in meeting that need?

The purpose of the *FOTM* technology demonstration is to assess whether FR technology can be effective in detecting attempts by travellers to Canada to subvert name-based lists through false identity documents. The CBSA is committed to taking a careful and educated approach to exploring and potentially implementing FR technology; in part, the CBSA is committed to ensuring a solution is proven, effective, and can be deployed in a way that respects and protects privacy. That is the reason for this demonstration.

FR has been used in other jurisdictions for similar purposes with some success. A 2011 report explains how Ontario casinos use FR technology to identify self-reported problem gamblers if they try to enter a casino. The same report explains how the Canadian Bankers Association has been using FR since 2008 to investigate debit card fraud. See http://www.theglobeandmail.com/news/national/time-to-lead/canadian-casinos-banks-police-use-facial-recognition-technology/article590998/.

In November 2014, the Calgary Police Service announced it was implementing FR technology to match crime-scene photos to its collection of over 300,000 mug shots. It is the first police service in Canada to do so. (see http://www.cbc.ca/news/canada/calgary/facial-recognition-software-to-aid-calgary-police-in-future-investigations-1.2822592. The Toronto Police Service is considering similar technology (see http://www.huffingtonpost.ca/2014/11/13/toronto-police-facial-recognition-technology_n_6154200.html).

Law enforcement agencies in the U.S. have used FR to match images extracted from CCTV footage at crime scenes with photo databases (often based on drivers' licence photos) to identify criminals (http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html?hpid=z1).

FR technology is also being tested and deployed at airports around the world. (See, for example, http://www.govtech.com/public-safety/Sochi-Airport-Uses-Silicon-Valley-Facial-Recognition-Software.html (Sochi, Russia), http://www.biometricupdate.com/201407/brussels-airport-to-introduce-facial-recognition-scanners (Brussels, Belgium), and http://www.homelandsecuritynewswire.com/dr20140918-japan-to-adopt-automated-airport-gates-equipped-with-facial-recognition-technology (Tokyo, Japan))

3. Is the loss of privacy proportional to the need?

The *FOTM* demonstration is being deployed only for testing purposes for a limited time (six months). It targets only those persons who are already under an active removal order and who have previously demonstrated intent to return to Canada, despite having been previously deported multiple times.

The FR demonstration will take place only in CBSA-controlled areas of Terminal 3 at Pearson International Airport for a limited time, estimated at six months. After the demonstration, the technology will be removed from the airport for an additional three to six months of evaluation in a lab setting Personal information already collected at POEs includes a traveller's name; citizenship(s); country and place of residence; and sex. Travellers must also provide a piece of approved identification, such as a passport or enhanced driver's license. Persons seeking entry to Canada may also be required to provide the following information: address, or address of destination in Canada; date of birth (age); marital status; employment status; criminal history; fingerprints; and, information related to accompanying goods entering Canada, including purchases made abroad. FR technology, in addition to the elements mentioned, also captures the physical image of the traveller, which can assist in identifying individuals seeking entry into Canada who are using false identity documents. In all cases, the CBSA only collects the minimum amount of personal information required to make an admissibility decision.

The loss of privacy is minimal given the lower expectation of privacy in a border crossing context. This was noted in the PIA report on the Overt Use of Video Monitoring and Recording Technology submitted to the OPC in November 2013. The *FOTM* demonstration project represents only a nominal increase in the loss of privacy insofar as no different information is being collected above and beyond the CBSA's current use of CCTV technology. The main difference between CCTV and FR is in the technology being used to process the information. This nominal increase in privacy loss will affect mainly those travellers who try to subvert the admissibility determination process.

The CBSA fulfills its mandate through the administration or enforcement of over 90 Acts and Regulations. As a result the Agency is responsible for numerous and complex programs and operating activities, including deciding on traveller admissibility to Canada. In calendar year 2013, the CBSA provided border-related services for 99.7 million travellers arriving at our land, air, rail and marine ports of entry. There is a significant need to find ways to augment the admissibility determination process with automation that can improve efficiency and effectiveness without sacrificing privacy. The CBSA is testing FR technology to determine whether it can meet this need.

4. Is there a less privacy-invasive way of achieving the same end?

The goal of this project is to demonstrate the effectiveness of FR technology in an airport setting.FR is less invasive than other forms of biometric identification, such as fingerprints or retina scans. There is no need to touch or come into close proximity with a biometric scanning device; cameras can be mounted on walls, ceilings, and other architectural features and capture facial images without inconveniencing the traveller.

In terms of the goal of identifying travellers using false identity documents, the only other way to do FR at this time in a way that would be less privacy-invasive would be to have CBSA officers visually examine every arriving traveller and compare their faces with the PDD. Given that the demonstration PDD will contain thousands of photographs, it could take hours to process each traveller through manual FR. This is obviously a totally impractical approach to traveller identification.

Lastly, the CBSA is always balancing methods of enhancing security while expediting travel and commerce; a balance that is often difficult. If the FR technology proves successful, it may also serve a dual purpose: first, to better identify individuals who are attempting to illegally re-enter Canada; and two, by improving the effectiveness of and efficiency of identifying these individuals, reduce wait times at the Primary Inspection Lane (PIL).

SECTION 4 – RISK AREA IDENTIFICATION AND CATEGORIZATION

For Section 3, please check the appropriate box that describes the level of risk related to your program or activity and provide details as indicated in yellow.

A. Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual. The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.	☐ 1
Administration of Programs / Activity and Services Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).	☐ 2
Compliance / Regulatory investigations and enforcement Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	☒ 3
Criminal investigation and enforcement / National Security Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	☒ 4

Details:

Some personal information collected through the *FOTM* demonstration may be used in support of identifying persons who have been previously determined to be inadmissible to Canada because of known non-compliance with the *IRPA*. Therefore, this would be enforcement in a compliance and regulatory context. However, once a match occurs, CBSA secondary BSOs must independently validate the FOTM match with existing CBSA information systems.

Facial photographs may be disclosed to CBSA's Inland Enforcement Division (IED), but only in the rare chance that an identified match of the FOTM demonstration is identified but not intercepted before leaving the terminal. In those cases, IED will utilize the FOTM match as a tip requiring identity validation utilizing existing systems and procedures. FOTM photographic and video recordings may be used as evidence to support deportation; however, it is highly unlikely. Any validation made by secondary BSOs will be used in the deportation proceedings as will video from existing Terminal 3 cameras.

It is noted that if any PDD individuals are identified during the short-term project, they are immediately deported without any judicial review. As the PDD is comprised of individuals who have been deported and have re-entered Canada at least one time after the initial deportation, judicial

review is not available to them. Therefore, if any individual on the Previously Deported List is identified by the project, there is no sharing of the project data to the Department of Justice (DOJ), Public Prosecution Service of Canada (PPSC), Immigration and Refugee Board (IRB), or any other organization.

Privacy risk:

Some personal information collected through the *FOTM* demonstration may be disclosed to internal stakeholders, such as CBSA IED, for the purposes of compliance/regulatory enforcement.

Mitigation:

FOTM data will rarely, if ever, be used to support a deportation proceeding, but it is possible. As stated above, if a secondary BSO, using existing systems and procedures, identifies an individual as being on the Previously Deported list (maintained outside the FOTM FR system), then non-FOTM data, including video from existing Terminal 3 cameras will be used to support the deportation proceeding.

Facial photographs owned by the CBSA may be disclosed to Face4 Systems, the technology integrator, so that they can analyze and improve the effectiveness of the technology.

Facial photographs will only be disclosed in accordance with all relevant legislation and policy.

B. Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	☐ 1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	☐ 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	☒ 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	☐ 4

Details:

FOTM photographs contain only the physical appearance of the traveller's face, with no context other than a date/time stamp. Scene-video clips will contain the traveller's overall appearance, behaviour, and, possibly, carry-on items. The PDD will contain additional information such as name, date of birth, and any safety warnings (where the person is considered a potential danger or threat to CBSA employees). The project cameras will photograph all persons entering the CBSA-controlled areas of Pearson International Airport's Terminal 3; this could include minors and incompetent individuals. Facial photographs will be collected directly from the individuals. PDD information will come from the CBSA's existing Previously Deported Persons database. Such use is consistent with the purposes for

which the information was collected in the first instance.

Privacy risk:

The CBSA collects a wide variety of personal information through its activities. *FOTM* photographs, scene video, and the PDD will contain minimal information, such as facial image, name, date of birth, and security warnings. The presence of an individual's information on the PDD will indicate that the individual is inadmissible to Canada. The presence of an individual's photograph in the set of facial photographs could lead to the inference that the individual attempted to enter Canada at a certain date and time.

Mitigation:

The CBSA will collect only the personal information necessary to effectively carry out its mandate.

In accordance with the CBSA's audio-visual policy, information collected for the *FOTM* demonstration will be considered to be Protected B. All photographs, videos, and PDD information, regardless of storage medium, will be stored either in a locked cabinet (or container or a safe) or in a secure room designed in accordance with specifications approved by the Infrastructure and Information Security Division of CBSA.

All retention and disposal of facial photographs, video, and PDD information will be carried out in accordance with the relevant provisions of the *AV Policy*.

The retention period for facial photographs having no enduring value to the Agency will be the duration of the project (which is scheduled to end at the end of the lab phase). All information is required until the end of the project so that the technology's performance can be evaluated. For all photographs requiring further action on the part of the CBSA, the CBSA has established a minimum two-year retention period in accordance with paragraph 4(1)(a) of the *Privacy Regulations.* In addition, if an ATIP request or formal complaint is received within 30 days of the creation of a facial photograph, that photograph will also become subject to the minimum two-year retention period.

In the context of the proposed demonstration of *FOTM* technology, it is essential to take facial images captured at Terminal 3 and replay them in the lab to further test and investigate the performance of the technology. Thus, it is necessary to retain the facial images captured during the demonstration for the duration of the project.

The AV Policy requires that:

- All disclosure of audio-video or photographic records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.
- When an audio-video or photographic record is disclosed in response to an ATIP request from an individual whose information is contained in the record, the identity and other personal information of other individuals in the audio-video or photographic record who are not implicated in the request will be protected. If the personal information of a third party cannot be protected, and consent has not been provided for its disclosure, the audio-video or photographic record will not be disclosed.

C. Program or Activity Partners and Private Sector Involvement	Level of Risk
Within the institution (amongst one or more programs within the same institution)	☐ 1
With other federal institutions	☐ 2
With other or a combination of federal/ provincial and/or municipal government(s)	☐ 3
Private sector organizations or international organizations or foreign governments	☒ 4

Details:

Facial photographs, scene video, and PDD information will be disclosed to integration firm Face4 Systems so that they can "re-play" the photo stream in a lab setting and fine-tune the performance of the technology. The facial photographs, scene video, and PDD information may also be accessible to the telecommunications provider that will operate the wireless link that is part of the demonstration architecture.

Performance metrics will be shared with staff of ÉTS who will provide analytical assistance regarding project evaluation. ÉTS staff will not have access to any information defined as "personal information" by the *Privacy Act*.

Privacy risk:

Facial photographs, scene video, or PDD information will be disclosed to Face4 Systems. Facial photographs, scene video, or PDD information may be accessible by the telecommunications provider.

Mitigation:

The AV Policy states:

- All disclosure of audio-video or photographic records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.

In addition, the *Directives on the Overt Use of Audio-Video Monitoring and Recording Technology* state that:

- Any access to or disclosure of audio-video or photographic recordings must be noted in an audio-video monitoring log. The log entry must include the date and time when the data was accessed, which segment of the data was viewed, by whom and for what reason. Persons who access recordings must identify themselves by name and badge number if applicable. When a recording is disclosed, the authority for that disclosure must also be noted in the log.
- When audio-video or photographic recordings are copied or extracted in order to be disclosed within the CBSA or to other organizations, the CD, DVD or storage device must be stored in locked storage according to the security classification of the information contained in the audio-video recording. Facial photographs and related information are to be categorized as Protected B.
- Audio-video or photographic recordings, including records to be disclosed to organizations, may only be disclosed as authorized by the *Privacy Act*, s. 8, *Customs Act*, s. 107, and CBSA disclosure policy.
- Only the segment of the audio-video recording or the photograph or PDD information related to the request will be provided. Any unrelated data will be blacked-out, blurred, or obscured by a technique certified as tamper-proof by a credible certification body.

D. Duration of the Program or Activity	Level of risk
One time program or activity Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	☐ 1
Short–term program A program or an activity that supports a short-term goal with an established "sunset" date.	☒ 2
Long-term program Existing program that has been modified or is established with no clear "sunset".	☐ 3

Details:

The CBSA will deploy the *FOTM* technology in the short-term context of a technology demonstration. The technology will be installed in Terminal 3 of Pearson International Airport for a period of six months and then removed. The technology will be re-installed in a lab setting in Ottawa to allow researchers to further investigate and study its performance by replaying images retained from the live demonstration.

Privacy Risk:

The CBSA will collect personal information for *FOTM* for a limited time. Analysis of the results of the demonstration will contribute to senior management decisions on further testing and evaluation of FR technology.

Mitigation:

The CBSA will only retain personal information for the minimum amount of time necessary to ensure it is of no enduring value to the Agency, with all records scheduled to be destroyed at the end of the project.

In order to balance the privacy rights of individuals with the needs of the CBSA to ensure the safety and security of Canada, it has been established that the minimum retention period for facial photographs and scene video attached to matches will be the duration of the project. Scene video having no enduring value to the Agency (i.e., scene video that is not linked to any matched travellers) will be retained for 30 days, in accordance with the *AV Policy*. For all facial photographs, scene video, or PDD information requiring further action on the part of the CBSA, the CBSA has established a minimum two-year retention period in accordance with paragraph 4(1)(a) of the *Privacy Regulations*. In addition, if an ATIP request or formal complaint is received within 30 days of the creation of a recording, that recording will also become subject to the minimum two-year retention period.

E. Program Population	Level of Risk
The program affects certain employees for internal administrative purposes.	☐ 1
The program affects all employees for internal administrative purposes.	☐ 2
The program affects certain individuals for external administrative purposes.	☒ 3
The program affects all individuals for external administrative purposes.	☐ 4

Details:

Some information collected will be disclosed within the CBSA for the purpose of determining a traveller's admissibility to Canada.

Privacy Risk:

Facial photographs of travellers, scene videos, or PDD information used to refer an individual who matches to the PDD may be disclosed within the CBSA.

Mitigation:

The CBSA will ensure that any disclosure of facial photographs, scene video, or PDD information is made in accordance with the relevant policies and legislation. After the initial six-month demonstration at Terminal 3 of Pearson International Airport, the system will be re-located to the CBSA's SED lab (Ottawa) for up to six more months of further tests. This includes re-running the photographs taken in Terminal 3 against the PDD and modifying the matching parameters in tests to improve system performance.

F. Technology and Privacy

6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	☒ YES ☐ NO
6.2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	☐ YES ☒ NO
6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:	
6.3.1 Enhanced identification methods: This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic). Please specify: The CBSA will use *FOTM* in approaches to the arrivals hall, approaches to PIL booths, during PIL interviews, and approaches to immigration point to identify persons of interest to the CBSA through matching facial images with PDD images.	☒ YES ☐ NO
6.3.2 Use of Surveillance: This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc. Please specify: *FOTM* will use cameras to overtly photograph travellers' faces and to record scene video of the travellers' overall appearances (e.g., clothing, luggage, companions).	☒ YES ☐ NO

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

☒ YES
☐ NO

For the purposes of the Directive on PIA, government institutions are to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Please specify:

The CBSA will use *FOTM* to compare images of arriving travellers' faces with facial photographs of persons of interest on a PDD. The technology will identify potential matches and notify CBSA officers, who will manually review and adjudicate the potential matches. Real-time matches that are verified by human review will be forwarded to roving CBSA officers for further action.

A **YES** response to any of the above indicates the potential for privacy concerns and risks that will need to be considered and if necessary mitigated.

6.1 Implementation of new cameras, FR servers, and wireless communications.

Privacy Risk:

The CBSA will implement cameras that have the capability to take facial photographs of any and all individuals found in CBSA-controlled and -monitored areas accessible to the travelling public. Facial images of immediately verified persons of interest will be transmitted wirelessly within the CBSA-controlled and CBSA-monitored areas to notify roving CBSA officers of the presence of a person of interest. The CBSA will also implement video cameras to take scene video of the same areas. The system will attach a short video clip (approximately 5 seconds) to each match record to provide context of the traveller within the airport.

Mitigation:

Facial photographs and scene video taken by the on-site cameras and information contained in the PDD will be accessible only to properly authorized and trained CBSA personnel. This information will be used only to identify persons of interest who have already been determined to be inadmissible to Canada and to perform post-demonstration tests and analysis on the FR technology in a CBSA lab setting. The facial photographs and scene video taken on-site will have no identifying information associated with them other than a date/time stamp. The PDD will contain only photographs, names, birthdates, and safety warnings. Information about potential matches will be retained for the duration of the project to generate metrics about the performance of the technology.

Live-captured facial photographs and scene video for matched travellers will be retained for the duration of the project. Unused scene video (i.e., video that is not linked to any matched travellers) will be retained for 30 days from the time of creation. PDD information will be retained for the duration of the project.

6.3.1 Enhanced identification methods

Privacy Risk:

The CBSA will use *FOTM* to compare photographs of travellers' faces with images stored in a PDD to identify persons who have already been determined to be inadmissible to Canada. There is a risk that an individual will be incorrectly matched with a PDD entry and be selected for secondary examination as a result of the false match. There is a further risk that a falsely matched traveller selected for secondary examination could learn the identity of the person of interest on the PDD against whom he or she was incorrectly matched.

Mitigation:

An important objective of the *FOTM* demonstration is to assess the readiness of the FR technology, including its ability to minimize false matches. Procedures will be developed to quickly ascertain the identity of travellers selected on the basis of *FOTM* for secondary examination using existing CBSA systems. Persons who have been deemed to be incorrectly matched with a PDD entry will be released as quickly as possible, assuming no other questions arise about the traveller's identity and admissibility (it is possible that a traveller matched incorrectly and selected for secondary examination is still found to be inadmissible for other reasons).

Furthermore, the CBSA will develop procedures to ensure that, when questioning a traveller who has been selected for secondary examination on the basis of *FOTM*, the traveller will not be told the name of the person on the PDD against whom the traveller has been matched. The traveller will not be shown the photograph of the person on the PDD. This will ensure that falsely matched travellers are not inadvertently given information about persons of interest.

6.3.2 Use of surveillance

Privacy Risk:

The CBSA will use cameras to overtly record travellers' facial images and physical appearance. Although there is a reduced expectation of privacy at an airport, travellers may perceive a risk that unauthorized personnel could access the images taken by *FOTM*.

Mitigation:

The CBSA will ensure that any disclosure of facial photographs, scene video, or PDD information is made in accordance with the relevant policies and legislation. In addition, the CBSA will take steps to ensure that recordings are not disclosed by third parties without the consent of the CBSA. After the initial six-month demonstration at Terminal 3 of Pearson International Airport, the system will be re-located to the CBSA's SED lab (Ottawa)for six more months of further tests. This includes re-running the photographs taken in Terminal 3 against the PDD and modifying the matching parameters in tests to improve system performance.

The CBSA's AV Policy states:

- All disclosure of audio-video or photographic records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.

In addition, the CBSA's *Directives on the Overt Use of Audio-Video Monitoring and Recording Technology* state that:

- Any access to or disclosure of audio-video or photographic recordings must be noted in an audio-video monitoring log. The log entry must include the date and time when the data was accessed, which segment of the data was viewed, by whom and for what reason. Persons who access

recordings must identify themselves by name and badge number if applicable. When a recording is disclosed, the authority for that disclosure must also be noted in the log.

- When audio-video or photographic recordings are copied or extracted in order to be disclosed within the CBSA or to other organizations, the CD, DVD or storage device must be stored in locked storage according to the security classification of the information contained in the audio-video recording. Facial photographs and related information are to be categorized as Protected B.
- Audio-video or photographic recordings, including records to be disclosed to organizations, may only be disclosed as authorized by the *Privacy Act*, s. 8, *Customs Act*, s. 107, and CBSA disclosure policy.
- Only the segment of the audio-video recording or the photograph or PDD information related to the request will be provided. Any unrelated data will be blacked-out, blurred, or obscured by a technique certified as tamper-proof by a credible certification body.

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques

Privacy Risk:

The CBSA will use FR to compare photographs of travellers' faces with images stored in a PDD to identify persons who may be inadmissible to Canada. There is a risk that an individual will be incorrectly matched with a PDD entry and be selected for secondary examination as a result of the false match. There is a further risk that a falsely matched traveller selected for secondary examination could learn the identity of the person of interest on the PDD against whom he or she was incorrectly matched.

Mitigation:

An important objective of the *FOTM* demonstration is to assess the readiness of the FR technology, including its ability to minimize false matches. Procedures will be developed to quickly ascertain the identity of travellers selected for secondary examination on the basis of *FOTM* using existing CBSA systems. Persons who have been deemed to be incorrectly matched with a PDD entry will be released as quickly as possible, assuming no other questions arise about the traveller's identity and admissibility (it is possible that a traveller matched incorrectly and selected for secondary screening is still found to be inadmissible for other reasons).

Furthermore, the CBSA will develop procedures to ensure that, when questioning a traveller who has been selected for secondary examination on the basis of *FOTM*, the traveller will not be told the name of the person on the PDD against whom the traveller has been matched. The traveller will not be shown the photograph of the person on the PDD. This will ensure that falsely matched travellers are not inadvertently given information about persons of interest.

G. Personal Information Transmission	Level of Risk
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	☐ 1
The personal information is used in system that has connections to at least one other system.	☐ 2

The personal information is transferred to a portable device or is printed. USB key, diskette, laptop computer, any transfer of the personal information to a different medium.	☐ 3
The personal information is transmitted using wireless technologies.	☒ 4

Details:

Match alerts will be sent wirelessly from the match adjudication officer in the CBSA surveillance centre to roving CBSA officers in the CBSA-controlled areas of Terminal 3 of Pearson International Airport. Match alerts will contain a photo, a short video clip, and biographical information about the person of interest (name, date of birth, safety warning (if applicable)). The wireless technology used is most likely to be a commercially-operated cellular communications link (Wi-Fi service in Terminal 3 is inadequate for the demonstration).

Privacy Risk:

The personal information being transmitted on a wireless network may be compromised. A wireless network is necessary for match alerts because the receiving CBSA officer is patrolling the airport and cannot be reached via a wired connection.

Mitigation:

The CBSA will ensure that all wireless transmission of data is secure using appropriate encryption technologies. Any transmission of recordings over wireless networks must be done in accordance with the CBSA's *Policy on the Use of Wireless Technologies*. Wireless transmission of data not in compliance with these protocols must cease immediately and the wireless transmission can only resume when authorized by local IT and an official of the Physical Security Section of the Security and Professional Standards Directorate. A Security Assessment of *FOTM*, including wireless alert transmission, is underway and will be forwarded when it is complete.

H. Risk Impact to the Institution	Level of Risk
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	☐ 1
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	☒ 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	☐ 3
Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	☐ 4

Details:

The CBSA has implemented appropriate controls to safeguard the privacy of all persons affected by

FOTM. If the photographs, scene videos, or PDD information are compromised or otherwise released without authority to do so, the CBSA may have to review its programs and organizational structures to determine whether deficiencies in those programs and structures contributed to a privacy breach. Changes to the admissibility determination program and associated organizational structures may be required to prevent similar future breaches.

Privacy Risk:

Should records be inadvertently or inappropriately released, this may reflect on deficiencies in the CBSA's organizational structures and its admissibility determination program in terms of their ability to properly implement the required privacy controls.

Mitigation:

The CBSA will take steps as recommended in the accompanying Security Assessment Summary to ensure that the organization in general and the *FOTM* project in particular (as deployed at Terminal 3 of Pearson International Airport) are briefed and trained on the proper application of required privacy controls. Only those employees who require access to records as part of their official duties and who have a need to view them will be permitted to access them. Such permission will be granted in writing and all access to records will be monitored by way of access logs.

I. Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	☐ 1
Reputation harm, embarrassment.	☒ 2
Financial harm.	☐ 3
Physical harm.	☐ 4

Details:

The inadvertent disclosure of such information without authorization or to an improper party may lead to harm to reputation and/or embarrassment. For example, details surrounding an individual's travel including date, time, and location of arrival may be contained in recordings.

Privacy Risk:

Should recordings be inadvertently or inappropriately released, there is a risk that individuals whose information is contained in those recordings could suffer reputation harm or embarrassment given the sensitivities surrounding the information that is collected and the potential impact the release could have on those individuals.

Mitigation:

As above, the CBSA will take steps to ensure that disclosure of recordings is only made in accordance with the relevant legislation as indicated above. Only those employees with a minimum SECRET security clearance who require access to recordings as part of their official duties and who have a need to view them will be permitted to access them. Such permission will be granted in writing and all access to recordings will be monitored by way of access logs.

SECTION 5 – ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity presents a potential privacy risk at level 2-3-4 in "*Section 3 - Risk Identification and Categorization*" of the PIA.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Gender, physical attributes	Physical image of traveller when photo or scene video is captured.	• includes a person's race, ethnic origin, or colour • can include information related to a person's employment (e.g., from employment-related headwear or clothing) • can include information related to a person's religious affiliation (e.g., from clothing or accessories)	Visual Image Recording, stored as digital files	To identify persons known to be inadmissible. To assist in making admissibility decisions regarding the entry of persons to Canada. To ensure the integrity of the immigration program.
Gender, physical attributes, name, date of birth, safety warnings	Physical image of person and associated details when information is collected from existing sources for PDD.	• includes a person's race, ethnic origin, or colour • Name (and possibly known aliases) • Date of birth • Safety warnings (such as flight risk, risk of violence, etc.)	Electronic database entries, including digital images	To match against live-capture photos to identify persons inadmissible to Canada. To assist in making admissibility decisions regarding the entry of persons to Canada. To ensure the integrity of the immigration program.

Biometric Information	Biometric Information	• FR algorithm	Electronic database entries, including digital images	To match against live-capture photos to identify persons inadmissible to Canada. To assist in making admissibility decisions regarding the entry of persons to Canada. To ensure the integrity of the immigration program.

SECTION 6 - FLOW OF PERSONAL INFORMATION

Identify the flow of the personal information within and outside the institution's program or activity. Institutions may choose to outline the flow of personal information in the format of their choice.

FR Information Flow Model - Diagrams
The flow of personal information within the *FOTM* system is depicted using data flow diagrams (DFDs) on the following pages. There are four types of symbols used in these diagrams:

- Sharp-cornered rectangle: represents an external entity that provides information to the system or receives information from it
- Round-cornered rectangle: represents a process where information inputs are transformed into information outputs
- Open-ended rectangle: represents a repository where information is stored
- Arrow: represents a flow of information

Each shape is labelled to describe its purpose or content.

The DFDs are presented as a hierarchical model of the system. The first diagram is a high-level overview of the system, showing the system as a single process exchanging information with various external entities. The next diagram decomposes that single process into five sub-processes. The following diagrams decompose four of those sub-processes to a greater level of detail. The fifth sub-process is straightforward and requires no further decomposition.

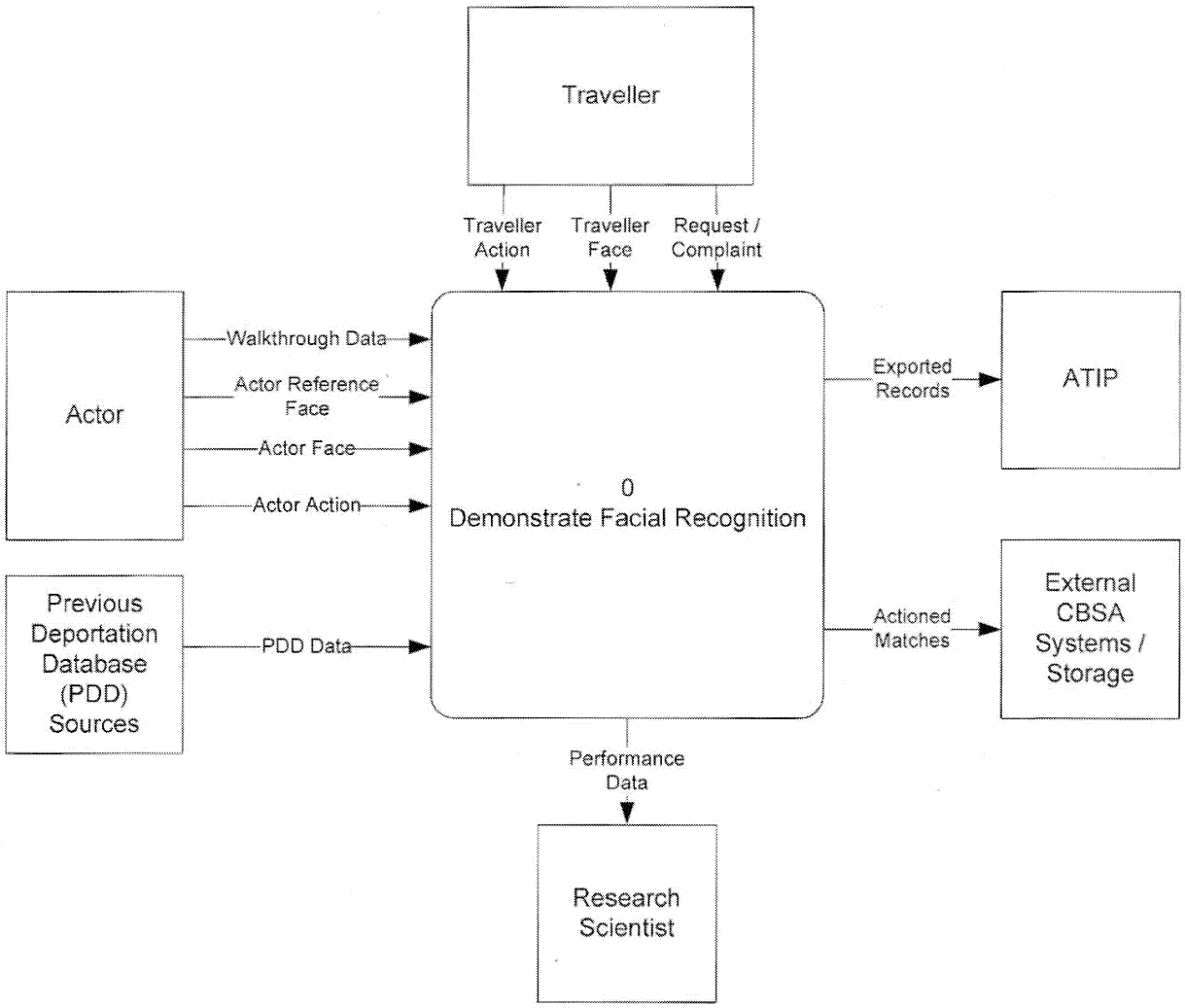

Figure 2: High-level Data Flow Diagram – Faces on the Move

The Traveller entity in
Figure 2 represents all travellers who pass through the international area of Terminal 3 of Pearson International Airport during the course of the *FOTM* demonstration. Travellers' faces and actions will be recorded as part of the main task of demonstrating FR. Travellers (or their representatives) may also file access to information requests or privacy complaints regarding the information collected from them.

The Actor entity represents CBSA employees who volunteer to participate in the *FOTM* demonstration to help researchers calibrate the FR technology. We cannot be certain that any travellers on the PDD will pass through the airport during the time of the demonstration. Actors are required to help demonstrate the readiness level of the technology by walking through the airport at known times. Actors' faces and actions will be recorded, just like those of travellers. In addition, actors will be enrolled into the PDD through a posed facial photograph (the "reference face" data flow). Finally, actors will provide information about each walkthrough (time and actor identity). The FR system will include actual photographs of the actors but with accompanying fictitious biographical data.

The PDD Sources entity represents all entities (external to *FOTM*) that provide the source data for constructing the operational PDD (i.e., the entries that do not come from actors). This is expected to include GTAR's existing database of Previously Deported Persons. All personal information will be handled in accordance with existing procedures and requirements.

The Research Scientist entity represents those individuals who will be analyzing and evaluating the performance of the FR technology, which will include individuals from the CBSA, Face4 Systems, and ÉTS; however, ÉTS will not have access to any personal information (performance metrics only).

The External CBSA Systems / Storage entity represents a CD, USB or similar device that would receive information related to travellers who have been directly affected by the *FOTM* demonstration. If the system and the primary adjudicator match a traveller to an entry on the operational PDD, CBSA will attempt to locate that traveller within the CBSA-controlled areas of Terminal 3 of Pearson International Airport and interact with him or her in accordance with existing procedures. According to current CBSA policies, the information that led to this interaction with the traveller must be kept for two years. The *FOTM* demonstration is only in operation for a short time, so information that led to action with respect to a matched traveller will be exported to other CBSA systems to be retained for the required period.

Information validated independently by the Immigration Secondary BSOs may be stored in existing CBSA systems, but not until an independent identity validation task has been completed.

The ATIP entity represents that branch of the CBSA (Access to Information and Privacy) that will extract information from the system to respond to traveller requests and complaints. The interaction between ATIP and the traveller is outside the scope of *FOTM* and is not directly represented in this model. below decomposes the high-level process into five numbered sub-processes.

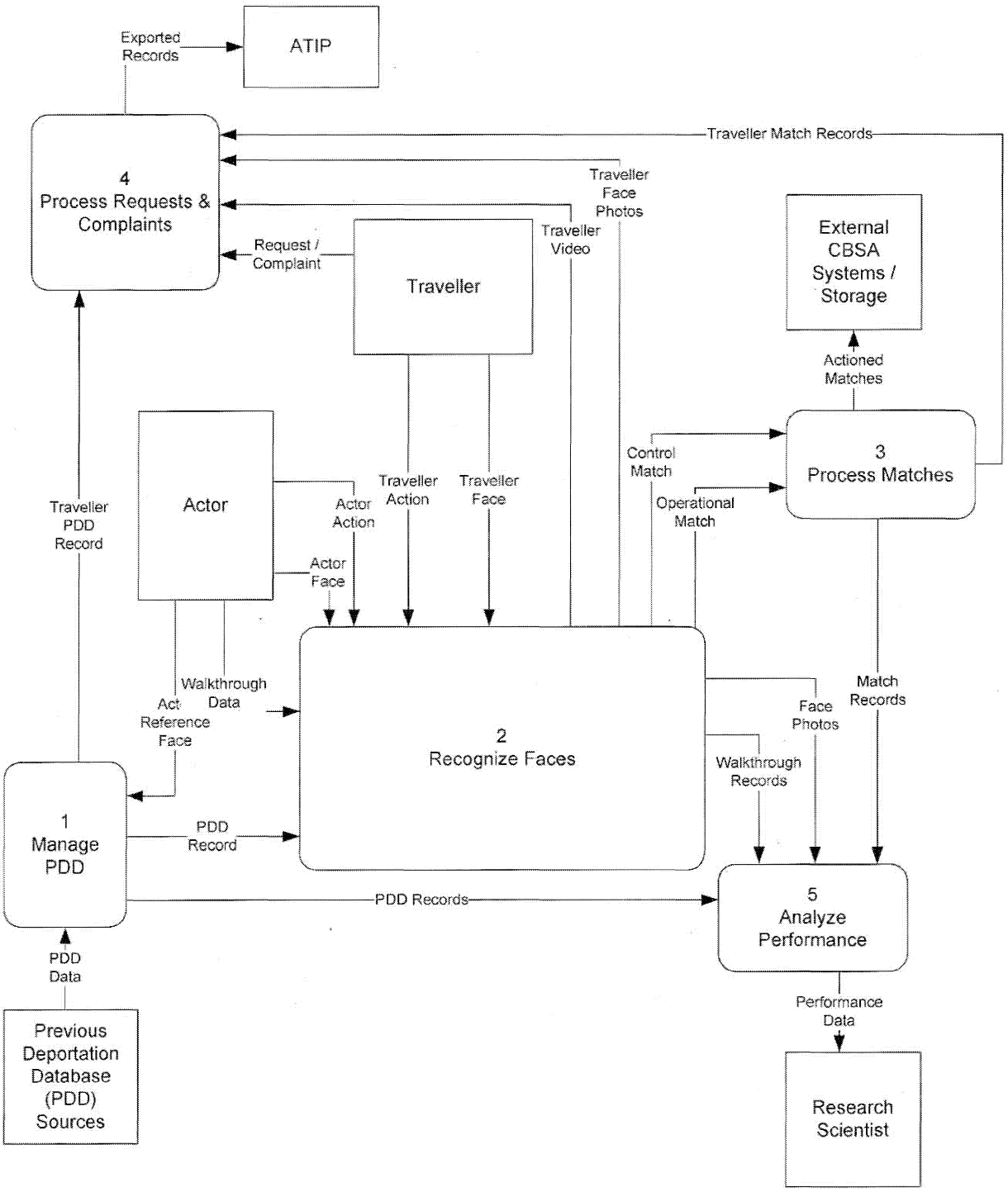

Figure 3: Data Flow Diagram – Demonstrate Facial Recognition

The five sub-processes are as follows:

1. Manage PDD – extract PDD data from external systems and actors and create PDD entries; present PDD records to other processes as needed
2. Recognize Faces – record the faces and actions of travellers and actors and identify those that match entries in the PDD; determine which matches are control (actor) matches and which are operational (traveller) matches; extract relevant video footage for operational matches
3. Process Matches – humans adjudicate each system-identified match either in real time or after the fact; act on adjudicated real-time operational matches; export match data to external systems when a matched traveller is affected
4. Process Requests & Complaints –find relevant records within the system for any traveller that submits a request or complaint about the personal information collected from him/her
5. Analyze Performance – evaluate how well the system identified actors; re-run the original photos while adjusting performance parameters to improve the detection rate while minimizing the false acceptance and false rejection rates

Figure 4 below expands the PDD process.

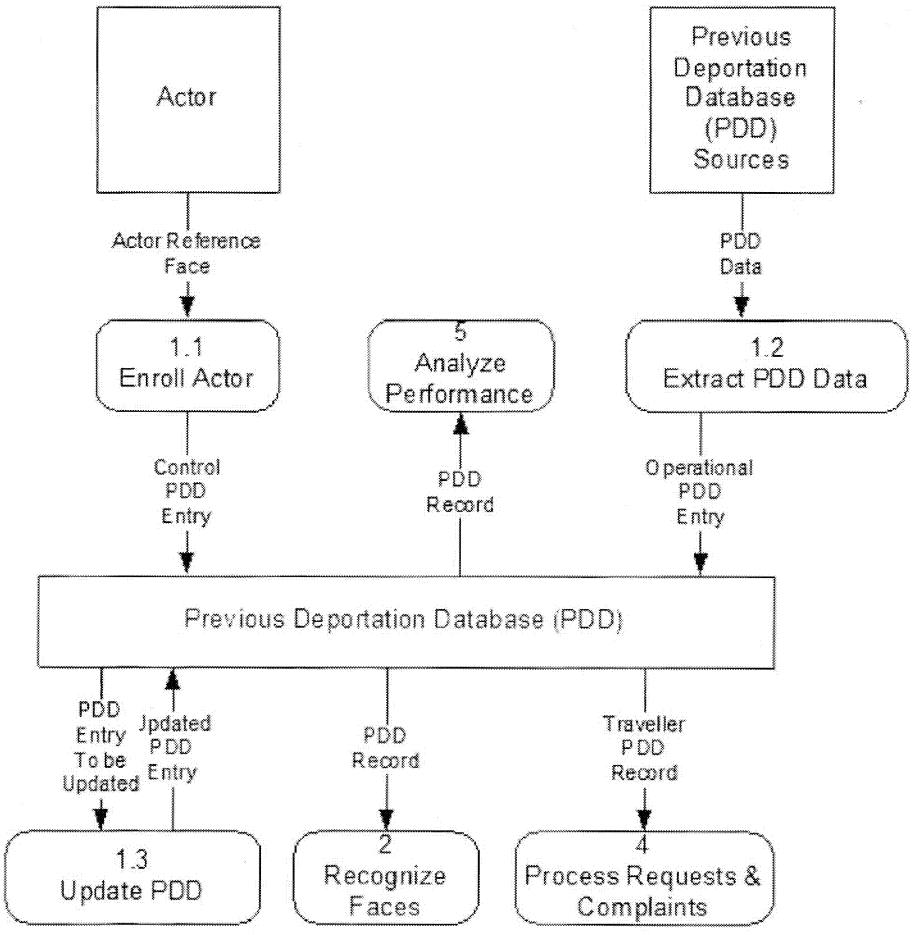

Figure 4: Data Flow Diagram - Manage Previous Deportation Database (PDD)

PDD data will be extracted from an existing CBSA regional database which stores information and photos on Previously Deported Persons (process 1.2). The size of the PDD will be limited to

approximately 5,000 records for the *FOTM* demonstration. The primary criterion for selecting records is that a person has been deported two or more times in the past three years; however, the project will not include any individual who meets this criterion if the photograph of the individual is not of sufficient quality to support the FR technology.

Each entry in the PDD will contain a photo of the person of interest (taken by CBSA before a prior deportation), the person's name, date of birth, a FOSS ID number (which links the entry to a record in the Field Operations Support System (FOSS)[2]), and any warnings associated with the person (such as safety warnings, threat warnings, health warnings, etc.).

PDD data will be extracted to allow the CBSA to carry out its mandate to detect and identify persons who have a record of failing to comply with the *Immigration and Refugee Protection Act*.

Control PDD data, including photos, will be collected directly from actors (CBSA employees who volunteer; process 1.1). The control PDD will contain information about known individuals who will, over the course of the demonstration, walk past the cameras to test the performance of the FR technology. These control PDD entries will be similar in structure to operational PDD entries, but with an extra note that they are control entries. The control photos will be of real individuals, but the biographical information will be test data.

All PDD entries (operational and control) will be securely stored as per CBSA policies on the storage of protected information (refer to Appendix: Comptrollership Manual - Security Volume – Chapter 6: Storage of Sensitive Information and Assets). The data store for PDD entries will be dedicated to the *FOTM* demonstration. This data store will not be connected to any other CBSA systems or programs. It is expected that the PDD entries will be in the form of relational database records, including the photo images.

The system will include a capability to allow PDD entries to be manually updated or deleted (process 1.3). New PDD entries may be added during the six months of the demonstration on an *ad hoc* basis. These *ad hoc* additions will use the same procedures as the initial entries and would include any new Previously Deported Person who meets the initial selection criteria or new actors

Figure 5 on the next page expands the Recognize Faces process.

[2] FOSS is in the process of being replaced by a new system called the Global Case Management System (GCMS), but "FOSS ID" is still the term used to refer to specific files or cases.

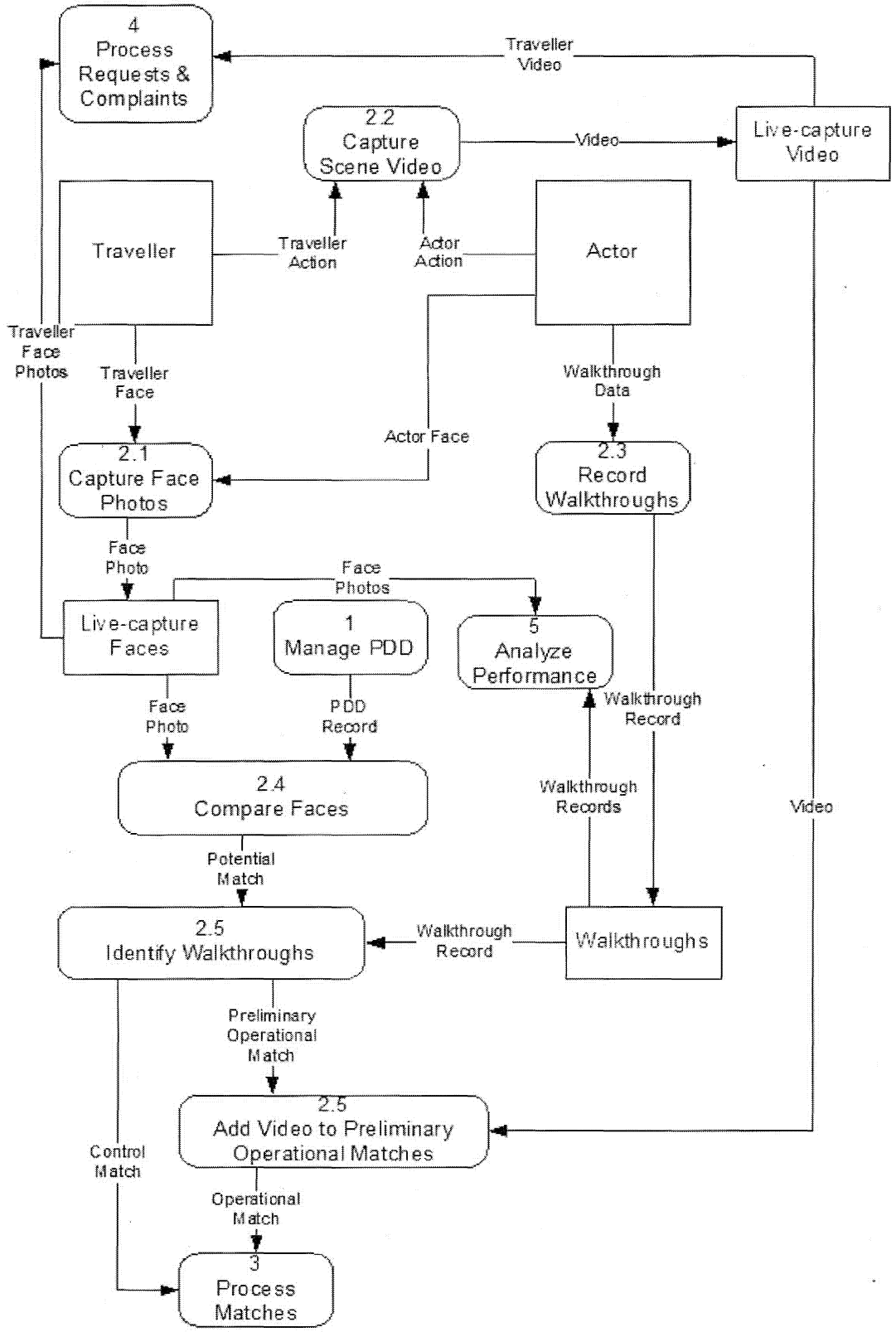

Figure 5: Data Flow Diagram - Recognize Faces

Travellers and actors will walk through the CBSA-controlled areas of Terminal 3, Pearson International Airport, such as the arrivals hall, the approaches to the PIL booths, the PIL booths themselves, and the approach to the immigration point. Actors will inform the system when they have performed a walkthrough (process 2.3). This will likely be by swiping an identification card at a special-purpose card reader. The date and time of the walkthrough and an identifier of the actor will be recorded as walkthrough data. This information is required to analyze performance and accuracy of the FR technology. This information will be stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

Dedicated project-cameras mounted at selected locations in the CBSA-controlled area of Terminal 3 at Pearson International Airport will record the faces of people walking through those areas (process 2.1). Dedicated project video cameras referred to as *scene cameras* will also record video of the travellers and actors (process 2.2). All facial photographs and scene video recordings will be securely stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets.) Photographs and video will be in the form of electronic media files.

Access to and control of any photography equipment is limited to qualified operators who are authorized to do so by the manager responsible for Terminal 3 of Pearson International Airport. Authorization is provided in writing and specifies the purposes for which access and or control is given.

As facial photographs of arriving passengers and of actors are captured, they are compared to the entries in the PDD (process 2.4).

If the FR system identifies a potential match between a live-captured photo and a PDD entry, the FR system will compare the match with the walkthrough data to determine whether the match is a test subject from the control group of actors (walkthrough; process 2.5). All potential matches that are not walkthroughs will be deemed operational. The FR system will attach to each preliminary operational match a video clip taken at the same approximate time and location as the matched face photo (process 2.5). This is to provide additional context for the match, such as the traveller's clothing, location, and companions.

All facial photographs will be retained until the end of the *FOTM* project. This is so that the stream of face photos can be re-run in a lab setting to assess and analyze the performance of the technology. All facial photographs will be securely stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets). Unused scene video recordings will be deleted 30 days after creation, in accordance with the CBSA's current policies for video recordings. Video clips that end up being used to support administrative action against a traveller will be retained for two years from the date of last administrative use, in accordance with the CBSA's current policies for video recordings. (Refer to the *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*.)

Figure 6 below expands the Process Matches process.

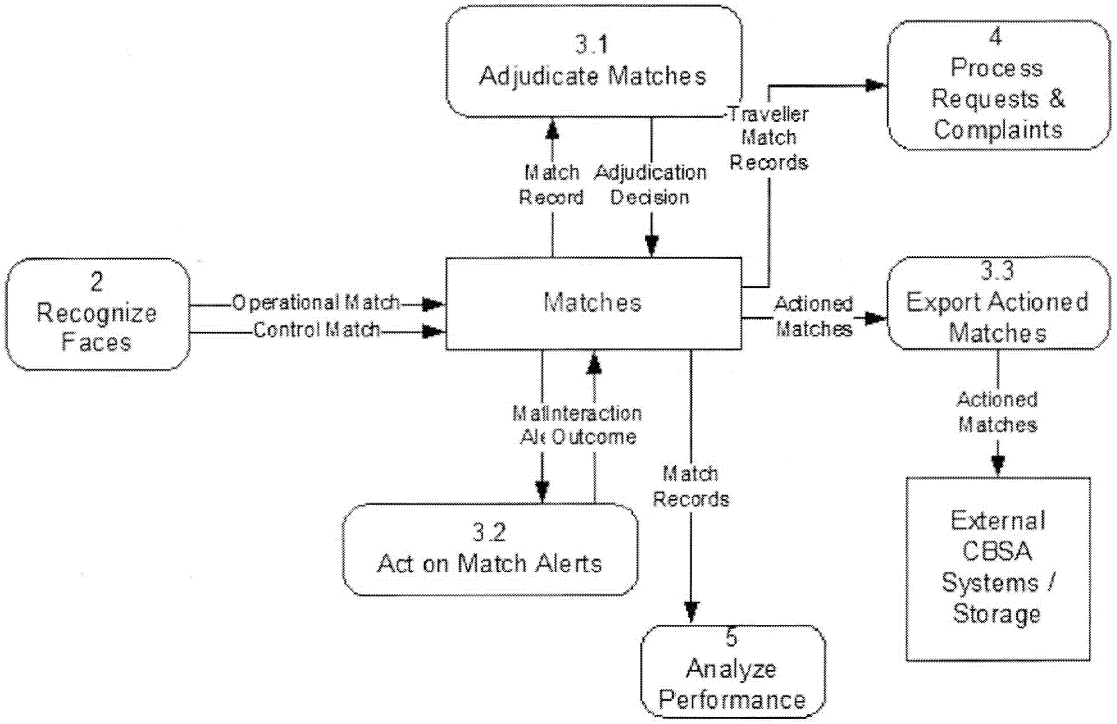

Figure 6: Data Flow Diagram - Process Matches

All matches, operational and control, will be stored in the *FOTM* system and displayed on a monitor in the Surveillance Centre. High-probability matches will be displayed immediately. Low-probability matches will be reviewed in bulk at a later time. A CBSA adjudicator (or, in the case of a low-probability match, a project scientist or technician) will review each potential match on the monitor and decide whether the match is valid (process 3.1).

The adjudicator records the adjudication decision (true or false match) in the match record in dedicated application available on a dedicated workstation; and stored on the FR server. The match record will link a live-capture image with a PDD entry. The FR system will indicate whether a match is control or operational and will link a related video clip to each operational match. The match record will also contain the adjudicator's decision to accept or reject the match.

If the match is accepted by the adjudicator and is real-time and operational (i.e., a traveller, not an actor), the FR system will send a notification over a wireless communication channel to one or more handheld devices carried by roving CBSA officers in the terminal. The adjudicator will also radio a superintendent to advise the superintendent that a match has been found and to describe verbally the physical appearance of the person, based on the scene video recording. The roving officer will use a project-specific application on the handheld device to access the match record. This allows the roving

officer to view photos, video, and information about the matched individual. The roving officer uses this information to search for and intercept the matched individual (process 3.2). If the match is rejected by the adjudicator or is a control match (i.e., an actor, not a traveller), the system takes no further action.

If the roving CBSA officer finds the matched individual, the officer will interact with the individual following standard CBSA protocols and procedures.

The CBSA officer will use the application on the handheld device to update the match record with the outcome of the officer's interaction with the matched individual or with the officer's failure to locate the matched individual. Outcomes may include: released, detained, referred to secondary, failed to intercept.

When an operational match results in action being taken with respect to a traveller, such as a referral to secondary examination, the match record, including all PDD information, live-capture photos, and scene video, will be exported to secondary storage (CD, USB or similar) in accordance with CBSA policies which require that any interaction with a traveller (i.e. referring the individual for secondary examination based on the FR solution) must be kept for two years. The storage device will be kept on the individual's file, so that a permanent record of the information that led to the action can be preserved; however, evidence supporting deportation will be limited to the identity validation efforts of the secondary immigration BSO. If deportation is the result of the secondary examination, then non-FOTM data, including video from existing Terminal 3 cameras, will be used to support the deportation proceeding. Only in rare and extraordinary cases does CBSA envision FOTM data being a supporting piece of information in a deportation proceeding.

Figure 7 below expands the Process Requests & Complaints process.

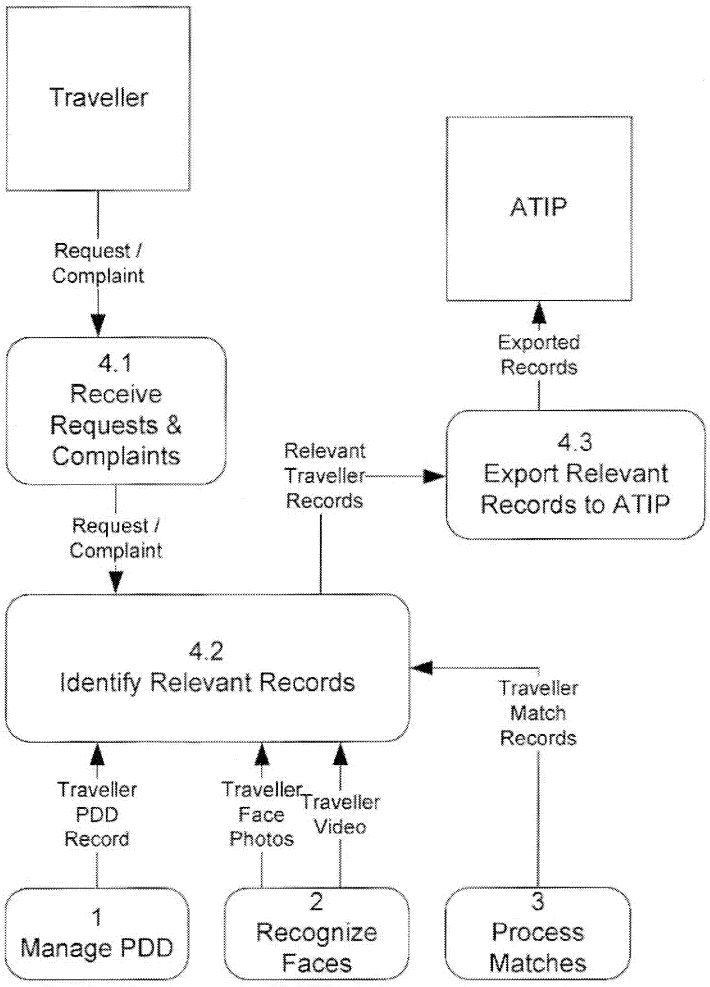

Figure 7: Data Flow Diagram - Process Requests & Complaints

If a traveller makes a formal access-to-information request or files a complaint with respect to the information gathered by the *FOTM* system within 30 days of the creation of a live-capture photo of the traveller (process 4.1), designated CBSA personnel will identify and retrieve from the system copies of records relevant to that traveller (process 4.2). Records could include PDD entries, face photos, video recordings, and match records. The relevant records will be copied to another storage medium such as a USB key or DVD and will be retained (process 4.3) for a minimum of two years in accordance with subsection 4(1) of the *Privacy Regulations*. All photo and PDD data and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets). CBSA's ATIP division will handle the request or complaint from then on in accordance with its normal policies and practices. ATIP's process is beyond the scope of this system.

All live-capture photos (whether matched or not), operational and control PDD entries, match records (whether accepted or rejected by an adjudicator), and actor walkthrough records will be retained in

storage until the end of the project. This will allow in-demonstration and post-demonstration analysis of the FR technology's performance. The photo stream may be re-run several times against the PDD in a lab setting as matching parameters are adjusted to determine the optimal settings for minimizing false acceptance rates and false rejection rates. The match records, particularly for control subjects (actors), will be analyzed to assess the accuracy and effectiveness of the technology. This data will not be disclosed outside the CBSA (although statistics and experimental findings on the technology's readiness will be summarized in a final report). This use of photos, the PDD, the match records, and the walkthrough records is a non-administrative use. A non-administrative-use security protocol has been developed to address proper handling of this information.

All data within the system will be deleted or disposed of after the *FOTM* project ends. Disposal of all data will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

The photos and related data will be deleted or disposed of two years from the date that the last administrative action is taken with respect to it. Disposal of all data will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

All recordings and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

Example of a Data Flow Model - Table

Source of the personal information for the program or activity

From whom or from what organization is the personal information collected? In other words, identify who is providing the personal information that is being used, will be used or available for use for the program or activity. There may be more than one source, indicate all sources:

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Only the individual.
A federal government institution (identify from what PIB the information is obtained)	Overt Audio-Video Surveillance (CBSA PPU 1104) CBSA Removals Program (CBSA PPU 1301)
Non-federal institutions	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A

SOURCE	IDENTIFY THE SOURCE
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

Internal Use and Disclosure

Where will that information circulate within the federal government institution? This must identify any related programs or activities and personal information banks as identified in the institution's Info Source chapter.

Program	Personal information bank
Ports of entry	CBSA PPU 1104; CBSA PPU 1301
Investigations	CBSA PPU 026
Intelligence	N/A
Inland Enforcement	CBSA PPU 020, CBSA PPU 026, CBSA PPU 1301

External Use and Disclosure

Where will that information circulate outside of the federal government institution? This includes any disclosure made to:

The individual or a representative	An individual or his/her representative may make an ATIP request with respect to his/her information.
A federal government institution	Records may be disclosed within CBSA for the purpose of enforcing federal legislation.
Non-federal institutions and private sector	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	Records will be disclosed to Face4 Systems, a private-sector organization that will assist the CBSA in analyzing and evaluating the FR technology during the project. Face4 will work with CBSA ISTB personnel to re-run the live-capture photos against the PDD and

	compile statistical information about true matches, false acceptances, and false rejections. They will modify system parameters that govern the matching processes to attempt to lower the false acceptance and false rejection rates as much as possible. Such disclosures will be made only for the purpose of assessing the performance of the technology. Such disclosures will only be made in accordance with the relevant legislative provisions and within the bounds of a clearly articulated contract. Note: ÉTS will not have access to personal information but will have access to derived information (scores of matches). They have no access to any of the match data, FOSS ID, photos, etc.
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

Retention / Storage

Where will the information be stored or retained (identify all organizations that will store the information – this includes duplicates of the databases containing the personal information or any back-ups):

A federal government institution – within the CBSA	Records will be stored at the location where they are made. The records will be housed on secure servers and in secure storage with access controls. When the live demonstration phase of the project is complete, all computing equipment, including storage devices and the records stored on them, will be moved to the CBSA's Science and Technology lab in Ottawa. The records will continue to be housed on the secure servers and in secure storage with access controls. In all cases where storage devices are used, they will be required to meet baseline physical security requirements based on the level of sensitivity of information gathered as per CBSA Security Volumes, depending on the recording medium. In cases where *FOTM* results in action being taken with respect to a matched traveller, relevant records will be exported to alternate systems or storage within CBSA. All such storage will comply with all security and privacy requirements. Records will not be disclosed to other federal government institutions. All personal information collected and held by the CBSA during this project will be deleted or disposed of at the end of the project in accordance with CBSA policies and procedures.
A Federal Records Center	N/A

Non federal institutions and private sector	
1. Provincial Government	N/A
2. Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
3. Located in Canada and Canadian Owned	N/A
4. Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Identify the areas / groups / divisions who are allowed to access and handle the personal information collected for the program or activity. Also, identify where these areas or groups are located (i.e. national capital region, within a province, in a foreign country, or several locations if teleworking) as well as the location of the personal information to uncover any potential trans-border or inter-jurisdictional issues. When reasonable to do so, by virtue of the size of the organization or the number of individuals, identify individual positions rather than the work area or group.

Federal government Institution responsible for program or activity: ***Canada Border Services Agency***		
Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
Ports of entry	Chiefs, Supervisors and select Border Service Officers have access as part of their official duties.	The CBSA will deploy this system at the international arrivals hall and related areas at Pearson International Airport, Terminal 3.
Inland Enforcement Division	Chiefs, Supervisors and Investigation Officers have access as part of their official duties.	The CBSA will deploy this system at the international arrivals hall and related areas at Pearson International Airport, Terminal 3.

Science and Technology	Research scientists	The CBSA will move the system and all its data to the Science and Technology Lab in Ottawa for post-demonstration analysis.
Other federal government Institution responsible for program or activity: (one table per institution):		
N/A		
Non Federal Institution or Private Sector: Face4 Systems: (one table per institution)		
Face4 Systems	Technicians, technologists, system analysts, developers	Face4 Systems will manage the system remotely from the CBSA Science and Technology Lab in Ottawa. They will also conduct post-demonstration analysis of the system and the data it collected, also at the CBSA's Ottawa lab.

SECTION 7 - PRIVACY COMPLIANCE ANALYSIS

Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* *(Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).*

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

1.1 ☒ Please specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Immigration and Refugee Protection Act, paragraphs 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2)

If legal authority is unclear consult your Legal Service to determine authority for the program or activity.

The CBSA's demonstration of FR is directly related to the cited paragraphs of the *IRPA*, which require all persons seeking entry to Canada to submit to an examination of their persons and documents. These paragraphs also allow for the presentation of photographic evidence of an applicant's identity.

Immigration and Refugee Protection Regulations, paragraphs 28, 28(a), 28(b), 28(c), and 28(d)

The cited regulations clarify that any person seeking to enter Canada is making an application under the terms of paragraphs 15 and 16 of the *IRPA*.

1.2 ☒ AND, ensure that the legal authority to collect the personal information is cited in the relevant PIB and in *"Section I – Overview and PIA Initiation"* of the PIA.

→ *Continue to Question 2*

No

1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your institution's legal advisors to determine if there is authority to proceed with the program or activity.

Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.

2.2 ☒ AND, implement controls and procedures to ensure the institution does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

→ *Continue to Question 3*

NO

2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in *"Section 3 – Analysis of Personal Information Elements"* to identify those that are "necessary" and not merely useful. Document any changes.

Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).

3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the institution is to occur on a routine or systematic basis

3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant PIB for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ *Continue to Question 4*

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ *Continue to Question 4*

Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6..2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

4.1 ☒ A "**Privacy Notice**" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must notify the individual of any of the following elements that apply (please check all appropriate boxes):

- ☒ a) The purpose and authority for the collection
- ☒ b) Any uses or disclosures that are consistent with the original purpose.
- ☐ c) Any uses or disclosures that are not related to the original purpose
- ☐ d) Any legal or administrative consequences for refusing to provide the personal information
- ☐ e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
- ☐ f) A reference to the PIB for the program or activity
- ☐ g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "**Consent Statement**" to the "**Privacy Notice**" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose or a consistent use, or, to authorize indirect collection of personal information.

4.2 ☐ The "**Consent Statement**" must include, as applicable, the following elements (please check all appropriate boxes):

- ☐ a) The purpose of the consent and the specific personal information involved.
- ☐ b) In the case of indirect collections, the sources that will be asked to provide the information.
- ☐ c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
- ☐ d) Any consequences that may result from withholding consent.
- ☐ e) Any alternatives to providing consent

4.3 ☐ AND, implement controls and procedures to ensure that the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

→ *Continue to Question 5*

NO

4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the institution, or from another institution, government or third party.

→ *Continue to Question 5*

Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

5.1 ☐ The notice and consent requirements stated at Question 4 apply. Please review the required elements listed under "**YES**" at Question 4 and check the corresponding boxes below to indicate the elements that need to be included in the "**Privacy Notice**" or the "**Consent Statement**" (check all that apply):

Privacy Notice	a)☐ b)☐ c)☐ d)☐ e)☐ f)☐ g)☐
Consent Statement	a)☐ b)☐ c)☐ d)☐ e)☐

5.2 ☐ AND, implement controls and procedures to ensure the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

→ *Continue to Question 6*

NO

5.4 ☒ → *Continue to Question 6*

Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

6.1 ☒ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

☒ a) The collection is a result of a disclosure to the institution under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

The CBSA will disclose previously collected information to populate the PDD as permitted by 8(2)(a) of the *Privacy Act*. The PDD is used for a purpose consistent with

the original collection, namely enforcing compliance with sections 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2) of the *Immigration and Refugee Protection Act* and sections 28, 28(a), 28(b), 28(c), and 28(d) of the *Immigration and Refugee Protection Regulations*.

☒ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided

If previously deported persons become aware that their faces are being photographed specifically for FR and that this is occurring only at Terminal 3 of Pearson International Airport, those persons may arrange to arrive at a different POE to avoid the FR or they may try to defeat the technology through head position, hats, glasses, etc.

☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.

6.2 ☒ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a PIA for the program or activity has been adequately documented in the description of the program or activity in "*Section I - Overview and PIA Initiation*" of the PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "**Privacy Notice**" or the "**Consent Statement**" includes all of the required elements listed under "**YES**" at Question 4.

→ *Continue to Question 7*

NO

6.5 ☐ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

→ *Continue to Question 7*

Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and

disposal schedule:

> For any record considered to be a transitory record, the RDA is MIDA 90/000: transitory records will be retained until the end of the project and will be destroyed within 15 days of the expiration of that retention period.
>
> Recordings of FR activity that are used to obtain or provide information or to investigate an allegation or complaint, or used as evidence in respect of an identifiable individual shall be kept for the longer of two (2) years following the date of their creation, or following the date of their last use in an administrative action as information or as evidence in respect of that person.
>
> A RDA has been requested from Library and Archives Canada for all records which are not considered to be transitory. The request has not yet been approved; however it is the intention of the CBSA to retain these records in accordance with paragraph 4(1)(a) of the *Privacy Regulations*, for a minimum of two years from the date of their creation.

7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act)

7.3 ☐ AND, if the institution intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.

7.4 ☒ AND, the institution must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

→ *Continue to Question 8*

NO

7.5 ☒ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.

The CBSA has requested a RDA for all audio-video records that are not considered to be transitory.

7.6 ☒ AND, obtain a RDA from Library and Archives Canada to allow the institution, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.

7.7 ☒ AND, ensure that all the other applicable requirements listed under "**YES**" at Question 7 are met.

→ *Continue to Question 8*

Accuracy of Personal Information

Will measures be adopted to ensure that personal information used by the institution for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☐ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the institution) where this is authorized, or where consent was obtained. Please briefly describe the data-matching process and the source(s) that will be used to ensure accuracy of the information:

8.1.3 ☒ In cases where direct collection or consent is not feasible, the institution will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use. Please identify the sources and procedures to be used to check the accuracy of the information:

Information for the PDD will be collected from existing CBSA sources, which are deemed to be accurate at the time of collection.

8.1.4 ☐ Technological methods will be used to identify errors and discrepancies. Please briefly describe these technological methods:

8.1.5 ☐ Other – please specify:

8.2 ☒ AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the institution must implement appropriate controls and procedures to ensure that:

a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;

b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;

c) personal information can only be modified or corrected by those within the institution who have the authority to do so; and

d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the institution are corrected / annotated.

8.3 ☐ AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant PIB are amended to identify the data-matching activity including the source(s).

→ *Continue to Question 9*

NO

8.4 ☐ Please explain why such measures will not be adopted:

→ *Continue to next Question 9*

Use of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties

9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "*Section IV – Flow of Personal Information*" of the PIA identify the areas, groups and individuals (e.g., the positions) within the institution who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the institution will adhere to the requirements and principles in its "***Privacy Protocol For Non-Administrative Purposes***", in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ *Continue to Question 10*

NO

9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the institution pursuant to subsection 8(2) of the *Privacy Act*:

9.5 ☐ AND, ensure that these other uses are reflected in the relevant PIB

9.6 ☐ AND, include a description of these other uses in the "**Privacy Notice**" or "**Consent Statement**", as appropriate,

☐ AND, ensure the all the other applicable requirements listed under "**YES**" at Question 9 are met.

→ *Continue to Question 10*

Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions

YES

10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the institution, please identify the branch and the program or activity.

10.1.1 ☒ Within the institution for another program or activity – specify

IED

10.1.2 ☐ Other federal government institutions – specify

10.1.3 ☐ Provincial, territorial or municipal governments institutions – specify

10.1.4 ☐ Foreign government institutions and entities thereof – specify

10.1.5 ☐ International organizations – specify

10.1.6 ☒ The private sector (e.g., contractor or other external service provider) – specify

- Face4 Systems, a contractor that is assisting in the deployment, management, maintenance, and post-demonstration analysis of the system.

10.1.7 ☐ Other – specify

10.2 ☒ AND, ensure that:

a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;

b) only personal information elements that are necessary for the intended purpose are disclosed;

c) the organization or third party receiving the personal information is authorized to do so;

d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);

e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant PIB in *Info Source*, including the specific purpose of the disclosure;

f) the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information; and,

g) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section IV – Flow of Personal Information*" of the PIA include details on the disclosed personal information:

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or trans-border flows of personal information. Such clauses must cover the following topics:

a) Control over personal information, where appropriate.

b) Limitations on the collection, retention, use and disclosure of personal information.

c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.

d) Measures governing the disposition of the personal information, where relevant

e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.

f) Obligations are to be extended to other parties such as subcontractors.

→ *Continue to Question 11*

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ *Continue to Question 11*

Accounting for New Uses or Disclosures Not Reported in Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in Info Source?

Statutory reference: Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

a) the head of the institution or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *Info Source*;

b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified forthwith regarding the new consistent use;

c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *Info Source* will only be made with the consent of the individual to whom the information relates;

d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *Info Source,* and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure

e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;

f) the Privacy Commissioner is notified forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or complied, but which is not reflected in the relevant PIB published in *Info Source*;

g) the relevant PIB is amended in time for the next edition of *Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and

h) the Privacy Commissioner is notified prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.

i) Other, specify

→ *Continue to Question 12*

NO

11.2 ☐ Please explain why such controls and procedures will not be implemented (provide adequate justification):

→ *Continue to Question 12*

Safeguards – Statement of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

YES

12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "*Section 2 - Risk Area Identification and Categorization*" of the PIA.

→ *Continue to Question 13*

NO

12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

→ *Continue to Question 13*

Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

YES

13.1 ☐ Reference the title of the TRA or other security assessment in "*Section VII – Supplementary Documents List*" and provide a brief synopsis of the assessment in the space below:

13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*.

→ *Continue to Question 14*

NO

13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

A Security Assessment is underway. It cannot be completed until the system design is finalized. Initial review of the in-progress design is that this is generally a low-risk system, mainly because it is not connected to any other CBSA systems and because it will exist for only a limited time. Internet connectivity for remote management is noted and identified as a concern. The final design will include a VPN to protect this interface.

→ *Continue to Question 14*

Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches
- ☐ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other – please describe

14.2 Physical safeguards

- ☒ Restricted access areas
- ☐ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☐ Combination locks
- ☒ Safes
- ☐ Cipher locks
- ☒ Key cards
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☐ Backups secured off-site
- ☐ Other – please describe

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☐ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☐ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Intrusion Detection System (IDS)
- ☒ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☐ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☐ Other – please describe

→ *Continue to Question 15*

Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

Statutory reference: Sections 4 to 10 of the *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of *Directive on Privacy Practices*

YES

15.1 ☐ The specific tracking technologies to be used is adequately described under Part F: Technology and Privacy of "*Section II – Risk Area Identification and Categorization*" of the PIA;

15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "*Section III – Analysis of Personal Information Elements*" of the PIA;

15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "**Privacy Notice**";

15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;

15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

→ *Continue to Question 16*

NO

15.6 ☒ Tracking technologies are not used to collect personal information about users.

→ *Continue to Question 16*

Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

Statutory reference: Sections 4 to 10 of *Privacy Act*, *section 4 of Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

16.1 ☒ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

16.2 ☒ AND, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Technology and Privacy of "*Section II – Risk Area Identification and Categorization*" of the PIA.

16.3 ☒ AND, any personal information collected or created as a result of such surveillance or

monitoring is described in the relevant PIB and in *Section III – Analysis of Personal Information Elements*" of the PIA.

16.4 ☒ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided, please explain why:

16.5 ☒ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ *Continue to Question 17*

NO

16.6 ☐ The new or modified program or activity will not result in surveillance or monitoring.

→ *Continue to Question 17*

Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, *section 4 of Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

The activity is undertaken in accordance with *Immigration and Refugee Protection Act*, paragraphs 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2) and *Immigration and Refugee Protection Regulations*, paragraphs 28, 28(a), 28(b), 28(c), and 28(d).

17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "*Section V – Privacy Compliance Analysis*" and in "*Section I – Overview and PIA Initiation* "of the PIA.

17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "*Section III – Analysis of Personal Information Elements*" of the PIA.

17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory

investigation or enforcement activities is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

☒ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided, please explain why:

If previously deported persons become aware that their faces are being photographed specifically for FR in support of immigration enforcement and that this is occurring only at Terminal 3 of Pearson International Airport, those persons may arrange to arrive at a different POE to avoid the FR or they may try to defeat the technology through head position, hats, glasses, etc.

NO

17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

Note: The table below can be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of *Section 5 – Privacy Compliance Analysis*)	Done	To be done
1	Legal authority for the program has been established and is reflected in the relevant PIB.	☒	☐
2	a) The categories and elements of personal information to be collected for the new program have been carefully assessed based, for example, on the institution's experience gained with the administration of a similar program. The personal data collected will be limited to only that which is required.)	☒	☐
	b) These categories and elements of personal information have been described in the relevant PIB for the program.	☐	☒
	c) Controls and procedures will be implemented to ensure that the institution does not collect more personal information than necessary for the program and that a continuing need exists for that information and its collection.	☒	☐
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the *Directive on Privacy Practices* have been drafted.(Texts of the notices and consent statements may be included here.) The following notices are posted in Terminal 3 of Pearson International Airport:	☒	☐

	"This area is under video surveillance. "Recordings may be used and shared in accordance with applicable federal legislation. For more information on the CBSA's use of these recordings, please ask to speak with a supervisor or visit www.cbsa-asfc.gc.ca."		
	b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the *Privacy Regulations*.	☒	☐
7	a) A Records Disposition Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.	☐	☒
	b) Controls and procedures have been implemented within the program and the ATIP Office to ensure that information that has been used for an administrative purpose will be keep for the minimum retention period established by the Privacy Regulations.	☒	☐
	c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	☐	☒
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	☒	☐

SECTION 8 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS

Four-Part Test

The use of biometrics to screen travellers against an active database is highly visible and may be controversial if privacy risks and societal implications are not considered at the outset. Although the PIA identified the pressing societal need for identifying illegitimate travellers at the border, the effectiveness and proportionality of using FR to match against databases has not yet been fully evaluated; such an evaluation is the goal of the *Faces on the Move (FOTM)* project.

A number of scientific studies have tested the accuracy of biometrically enabled matching in a laboratory setting. However, the CBSA has not yet evaluated the performance of these algorithms in an operational environment. The CBSA is unsure if FR technology will be effective and therefore cannot evaluate the proportionality of FR screening without first conducting this project.

The technical demonstration project is designed to produce the necessary data with minimal infringements on individual privacy. The testing area is confined to a single terminal at Pearson International Airport. The environmental conditions within the terminal have been optimized for lighting conditions and camera placement to ensure that the quality of facial images minimize the likelihood of false positive matches. The system is configured to only match against individuals on the Previously Deported Persons list, who have already been determined to be inadmissible to Canada and have demonstrated their intent to return to Canada under a false name. Multiple points of human intervention have been created to ensure that any actions taken as a result of a positive match have been reviewed independently by a trained BSO. Finally, a positive real-time match will only result in a referral to secondary examination where standard procedures to establish the traveller's identity will be followed. These safeguards have been implemented in order to minimally impact privacy while still enabling the CBSA to evaluate the readiness of FR matching in an operational setting.

The CBSA recognizes that it could test the system on a control group of "actors" exclusively, thereby eliminating the use of "live" data. However, the control group may not have the desired heterogeneity in lighting, resolution, and diversity which is required to properly evaluate the effectiveness of FR screening technology. Testing the system using an operational database will also enable the CBSA to identify any weaknesses in the photograph enrolment process caused by poor lighting, low resolution, or facial obstructions. Excluding the use of operational data may appear to be a less privacy invasive means of demonstrating the solution, however, the CBSA believes the use of actors and "live" data in a narrowly controlled environment will allow the Agency to identify and mitigate privacy risks in the future.

Risk: Poor performance of FR technology may cause a disproportionate impact on traveller privacy.

Mitigation: The CBSA has implemented a number of measures to improve accuracy of the system including controlling environmental conditions, limiting the population of the PDD, introducing multiple points of human intervention, and processing only high-probability matches in real time.

Recommendation: The CBSA will conduct a new four-part test for any facial recognition screening program it may implement in the future.

ACCOUNTABILITY

Within the CBSA

The CBSA has a robust administrative structure to ensure compliance with the *Privacy Act* and related policies and directives. In FY 2012-2013, a Privacy Oversight Committee (PoC) was established which consists of senior-level executives within the CBSA that meet regularly throughout the year to discuss privacy issues, as well as monitor the development of privacy policy instruments and PIAs. The PoC also helps identify a need to assess upcoming initiatives for potential PIAs.

Bi-monthly reports on the status of PIAs are provided routinely to the PoC and the Office of the Privacy Commissioner to ensure adequate planning for the completion of PIAs. The FOTM project was presented to the PoC in March 2015.

The ATIP Division is responsible for recommending the development of a PIA and/or other measures to ensure that existing or new programs / activities are privacy compliant. When contacted, the ATIP Division will provide program areas with the Privacy Impact Questionnaire (PIQ). The PIQ is a template that requests high-level information similar to sections 1 and 2 of the Core PIA template, and is used to develop and record any recommendations given by the ATIP Division concerning the program or activity. The PIQ enables the ATIP Division to make informed recommendations as to whether or not a PIA or other privacy compliant measures are required.

The ATIP Division is also a required stakeholder in the development of Written Collaborative Arrangements (WCAs) such as Memorandums of Understanding or Information Sharing Agreements. Aside from reviewing WCAs for compliance with the *Privacy Act* and Treasury Board of Canada Secretariat policies, directives, and guidelines, the ATIP Division also makes recommendations with respect to the conduct of a PIA before the implementation of WCAs.

In FY 2012-2013, the CBSA also developed two privacy policy instruments:

- The Privacy Breach Protocol; and
- The Directive on Non-Administrative Uses of Personal Information (Privacy Protocol)

The Privacy Breach Protocol ensures that all security violations which include personal information are reported to the ATIP Division in addition to the Security and Professional Standards Division, and outlines the roles and responsibilities of the Agency with respect to privacy breaches, which may include notification of the individuals, notification of the Office of the Privacy Commissioner, and the identification of mitigating measures.

The Directive on Non-Administrative Uses of Personal Information sets out the process, roles and responsibilities for the creation of a Privacy Protocol for those programs and initiatives the use personal information for non-administrative purposes, such as statistical reporting.

In FY 2013-2014 the CBSA introduced an online awareness course on Information Management (IM) and Access to Information and Privacy (ATIP). The course was jointly developed in FY 2012-2013 and seeks to educate employees on their IM and ATIP responsibilities. This course will be supplemented by current training activities, which include an in-depth session on the administration of the ATIP program at the CBSA, the development of PIAs, and Info Source training.

Specific to the Faces on the Move Project

Personal information collected from the six month testing phase will be disclosed to Face4 Systems for evaluation after the testing period has concluded and the system has been removed from Pearson Airport. The contract between Face4 Systems and the CBSA outlines a number of safeguards for handling personal information, including a clear date for when all personal information under its control must be destroyed (project end). Face4 Systems originally intended to evaluate the FOTM project at their premises in Ottawa. However, upon reflection during the PIA process, the CBSA determined that granting Face4 Systems personnel access to the CBSA's SED lab would enable the Agency to exercise greater accountability for personal information collected under the project.

Risk: *Face4 Systems may not abide by the terms and conditions stipulated in the contract.*

Mitigation: *The CBSA will ensure that access to match data and all personal information by Face4 Systems staff will be limited to the CBSA's SED Lab, and will reflect control procedures in accordance with the Face 4 contract and the CBSA FOTM demonstration procedures that have been established for data collection and analyses.*

IDENTIFYING PURPOSES

Within the CBSA

The CBSA maintains its *Info Source* chapter on its website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html. It conducts ongoing reviews of the chapter to ensure that it accurately and completely describes the personal information activities of the Agency. The CBSA also ensures that appropriate Privacy Notice Statements are reflected on forms and websites, unless such notice is not required pursuant to sub-section 5(3) of the *Privacy Act*.

Specific to the Faces on the Move Project

CBSA PIB PPU 1104 (Overt Audio Video Surveillance) reflects the types of information collected, the purpose, legislative authority, and the consistent uses of information collected by CBSA video surveillance cameras. The PIB does not currently reflect the use of video surveillance cameras for the purpose of FR screening. The Records Disposition Authority (RDA) and Retention and Disposal Standard (RDS) have not yet been published; both are currently reflected in the PIB as "under development". However, personal information collected under the FOTM project will be subject to the retention period specified under the contract with Face4 systems.

Risk: *CBSA PIB PPU 1104 (Overt Audio Video Surveillance) has not reflected a RDA or RDS in approximately two years. Moreover, if the FR solution were to be implemented or tested any further, the "Description" Section should include the personal information category of "biometric information". Also, the use of FR should be listed in the "consistent uses" section of the PIB.*

Recommendation: *The CBSA will update the RDA and RDS for CBSA PIB PPU 1104. The addition of "biometric information" and its use will be added to the "Description" and "Consistent Uses" section if biometric-based screening is considered for permanent deployment in the future.*

The CBSA already collects Overt Audio-Video Surveillance as part of its normal port operations. Although the FOTM project was developed in compliance with the CBSA's *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology,* the use of FR biometrics is not specifically identified within the Policy. The CBSA has chosen not to update the *Policy* at this time because the FOTM project is temporary and there are no plans to install this system permanently. At a minimum, the policy statements reflecting "permitted uses" would have to include FR. Also, additional guidance may also be necessary to ensure policy compliance.

Risk: *The FOTM project is not integrated into the CBSA's Policy on the Overt Use of Audio-Video Monitoring and Recording Technology.*

Recommendation: *The CBSA should align the use of FR screening into the Policy on the Overt Use of Audio-Video Monitoring and Recording Technology. In the interim, the CBSA will ensure the FOTM project is managed in accordance with the Policy.*

LIMITING USE, DISCLOSURE AND RETENTION

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs limit the use, disclosure, and retention of personal information to only that which is necessary to administer the program or activity.

In FY 2012-2013, the CBSA developed guidelines on the disclosure of customs information pursuant to s.107 of the *Customs Act*. These guidelines set out the specific provisions, their limitations, relevant considerations and the appropriate positions within the CBSA (employee, supervisor, senior manager) that can authorize specific disclosures or uses. Personal information that is also customs information is disclosed in accordance with s.107 of the Customs Act rather than ss. 8(2) of the Privacy Act.

A similar set of guidelines for s. 8(2) of the *Privacy Act* was implemented in FY 2013-2014.

Specific to Faces on the Move Project

The original scope of the project included disclosure to municipal police in the event that an individual was matched to the system but had already cleared the Primary Inspection Line before they could be intercepted. However, the privacy risk of disclosing inaccurate information to another law enforcement organization was deemed to be disproportional, particularly outside of the context of reduced

expectation of privacy at the border. Further, the CBSA considered including additional databases to match against but chose to limit the use of the FOTM project to a subset of the Previously Deported Persons list exclusively for the purposes described above. Finally, carefully monitored retention schedules have been put into place to ensure that the program is "torn-down" at its conclusion.

However, some personal information collected through the FOTM project may be disclosed to internal CBSA stakeholders, such as IED, if a rover officer is not able to intercept an individual before the individual leaves the airport. This will only include the information provided to the roving officer, including the traveller's name, FOSS ID, warnings, and possibly a scene photograph.

It is noted that if any PDD individuals are identified during the short-term project, they are immediately deported without any judicial review. As the PDD is comprised of individuals who have been deported and have re-entered Canada at least one time after the initial deportation, judicial review is not available to them. Therefore, if any individual on the PDD is identified by the project, there is no sharing of the project data to the Department of Justice (DOJ), Public Prosecution Service of Canada (PPSC), Immigration and Refugee Board (IRB), or any other organization. Sharing of information on individuals who are identified by the project but are not intercepted before leaving the airport, would be limited to disclosure to IED, who would utilize the information as any other tip and use existing procedures and CBSA systems (not the FOTM FR system) to validate the status of the individual as a Previously Deported Person and attempt to locate him/her.

Risk: *There is a risk that FR matches may be inappropriately used to support further investigation by the CBSA, which could later lead to proceedings under the Immigration and Refugee Protection Act, related regulations, or under the Criminal Code before the CBSA has had an opportunity to test the efficacy of the solution.*

Mitigation: *The CBSA will ensure that appropriate procedures are in place to support a match that is referred to CBSA investigators with the caveat that the accuracy of this information cannot be verified. Specifically, before such a disclosure occurs, significant human intervention will properly assess the data match and ramifications of using FOTM FR match in a deportation proceeding. Also, once the secondary BSO is notified of a match by the Rover BSO, existing identity validation procedures are taken before the individual is deported.*

Also, if an individual departs Pearson Airport prior to being intercepted, information on the individual may be shared with Inland Enforcement. In turn, Inland Enforcement will ensure that identification steps are taken before any deportation proceedings are initiated.

Risk: *There is a risk that project handheld devices may be viewable by individuals in the CBSA-controlled area of Terminal 3. Moreover, there is a risk that BSOs will inadvertently release personal information of PDD individuals to those individuals who were falsely identified by the FR system.*

Mitigation: *The CBSA will develop procedures to ensure that, when questioning a traveller who has been selected for secondary examination on the basis of FOTM, the traveller will not be told the name of the person on the PDD against whom the traveller has been matched. The traveller will not be shown the photograph of the person on the PDD. This will ensure that falsely matched travellers are not*

inadvertently given information about persons of interest. These same procedures, and related training, will instill in Rover BSOs the need to shield the handheld screen when in on the floor.

Risk: *The Standard Operating Procedures designed to support the activities of the CBSA staff at Terminal 3 have not yet been finalized and approved. These procedures will:*

- *support an expedited identity of travellers to determine if secondary examination is necessary;*
- *For false positives, require a quick release process;*
- *Ensure handheld device screens are shielded from view by individuals on the floor;*
- *Restrict disclosure of PDD data and the photograph; i.e. individuals who are interviewed by the Rover BSO and at secondary will not be shown PDD data/photos;*

Mitigation: *The CBSA should refrain from initiating the demonstration project until the procedures have been approved, communicated to staff, and appropriate training has been provided.*

ACCURACY

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs create a process for ensuring the accuracy of information as required, and that program areas are capable of handling requests for correction of personal information.

The correction process is coordinated centrally from the ATIP Division. Requests for correction are forwarded to the appropriate program area for action. A response letter is sent to the client indicating whether the correction was accepted or refused, whether the correction is made directly or notated to the file, and whether or not that information has been disclosed and that those recipients would be informed appropriately. The ATIP Division is looking at developing a more standardized approach and directive for the processing of correction requests.

Specific to the Faces on the Move Project

The CBSA recognizes that the accuracy of the matching algorithm has not yet been proven; the Agency has taken measures to mitigate this privacy risk. When installing the dedicated cameras, the CBSA will carefully calibrate the environment to ensure that light levels, camera angles, and lines of sight have been optimized to ensure that high-quality images are obtained. When the FOTM project becomes operational, the CBSA has also implemented policies and procedures to ensure that all matches produced by the system are first verified by a specially trained human operator before being actioned. Finally, the CBSA will continually refine these conditions to enhance the accuracy of the project throughout its duration. However, as the goal of the project is to test the accuracy of the system, there is a significant residual privacy risk to operational FR matching which cannot be mitigated without first conducting the FOTM project.

Risk: *The FOTM project may incorrectly refer travellers for secondary examination based on a false positive match.*

Mitigation: *The CBSA has implemented a number of measures to reduce the rate of false positives by controlling environmental factors, ensuring human verification, and verifying the accuracy of a match during the secondary examination process.*

Recommendation: *The CBSA should implement a limit to the rate of false positives and consider deactivating the project if it exceeds this rate.*

SAFEGUARDS

Within the CBSA

Typically the ATIP Division strongly recommends the completion of a TRA and SoS as part of the PIA process, and directs programs to contact Corporate Security for guidance with respect to those instruments. A summary of the risks identified in a TRA are appended to the PIA to ensure that all risks are identified and mitigated by the program area.

CBSA employees are required to take the online CBSA Security Awareness course when they begin employment, and to refresh their training every two years. CBSA managers are required to take both the CBSA Security Awareness course and a CBSA Security Awareness course for managers.

The Privacy Breach Protocol complements existing CBSA security policies, and ensures that all security violations which include personal information are reported to the ATIP Division in addition to the Security and Professional Standards Division, and outlines the roles and responsibilities of the Agency with respect to privacy breaches, which may include notification of the individuals, notification of the Office of the Privacy Commissioner, and the identification of mitigating measures.

Specific to Faces on the Move Project

Although a Threat and Risk Assessment (TRA) is currently underway, the CBSA has incorporated a number of safeguards to protect personal information under its control. Personal information used in this program been rated as Protected B and will be safeguarded in accordance with the *Management of Information Technology Security* (MITS) when it is installed. This includes, but is not limited to: securing physical assets in a location with limited access, restricting user access to the system, and encrypting all data transmission to prevent compromise. Further technical and administrative safeguards are currently being evaluated through the TRA process.

Further, the initial draft of this PIA did not examine the use of cellular networks for transmitting personal information to roving BSOs. A wireless network is necessary for match alerts because the receiving CBSA officer is patrolling the airport and the conditions of the terminal do not permit a Wi-Fi network to be created for technical reasons. The scope of the PIA was expanded to include this data flow and relevant program areas within the CBSA, including Corporate Security and Information Management, were engaged to ensure that the CBSA has proper safeguards and accountability mechanisms for personal information it transmits through these networks.

Risk: *The personal information being transmitted on a wireless network may be compromised.*

Recommendation: *The CBSA will ensure that all wireless transmission of data is secure using appropriate encryption technologies. Any transmission of recordings over wireless networks must be done in accordance with the CBSA's Policy on the Use of Wireless Technologies. Wireless transmission of data not in compliance with these protocols must cease immediately and the wireless transmission can only resume when authorized by local IT and an official of the Physical Security Section of the Security and Professional Standards Directorate. A Security Assessment of FOTM, including wireless alert transmission, is underway and will be forwarded when it is complete.*

Risk: *The system has been configured to enable remote access by system administrators.*

Recommendation: *Remote access should be secure using appropriate encryption techniques.*

OPENNESS

Within the CBSA

The CBSA manages its Info Source chapter directly on the CBSA website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html. The ATIP Division ensures that the descriptions of program privacy practices are kept complete and up-to-date.

The Directive on Privacy Impact Assessments requires departments to ensure that PIA summaries in both official languages are made available to the public. At a minimum the summary must address section 1 and 2 of the Core PIA Template. CBSA PIA summaries are posted at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html.

Upon completion of a PIA, PIA summaries are posted on the CBSA website, which also contains information on accessing personal information at the CBSA.

Specific to Faces on the Move Project

As reflected in Section 7 of this PIA (Question 17.5), notice of camera use to support the FOTM demonstration project will not be provided in any form. The CBSA already collects Overt Audio-Video Surveillance as part of its normal port operations. Signs throughout the facility indicate that travellers are under video surveillance and direct travellers to the CBSA's website or a supervisor for more information.

Failing to provide such notice is authorized pursuant to sub-section 5(3) of the *Privacy Act*.

In lieu of signage, the CBSA has developed a communications strategy, which includes posting an executive summary of this PIA, for communicating the general purposes of the FOTM project. The CBSA intends to proactively disseminate information about the FOTM project through a news release and a dedicated section on its corporate website. All communications materials will indicate the purposes and general function of the FOTM project but will not specify where it installed, which database it will use, or when it will be operational.

Risk: *The use of FR software is not supported by notice to individuals who enter the testing area.*

Mitigation: *The CBSA will not mitigate this risk by posting additional signage or modifying existing signage. Failure to provide notice in these circumstances is consistent with sub-section 5(3) of the Privacy Act which authorizes the CBSA to refrain from notice if, by providing such notice, may result in inaccurate information, may defeat the purpose of the collection, and/or may prejudice the use of the information collection.*

SECTION 9 - SUPPLEMENTARY DOCUMENTS LIST

Additional documents used or related to the PIA may include:

- *CBSA Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*
- *CBSA Directives on the Overt Use of Audio Video Monitoring and Recording Technology*
- CBSA PIA on the Overt Use of Video Monitoring and Recording Technology
- CBSA Comptrollership Manual – Security Volume Chapter 6: *Storage of Sensitive Information and Assets*
- CBSA Comptrollership Manual – Security Volume Chapter 8: *Disposal of Sensitive Information and Assets*
- *CBSA Policy on the Use of Wireless Technology*
- *CBSA Guidelines for the Directive on the Use of Wireless Technology*
- *Immigration and Refugee Protection Act*
- *CBSA Policy on the Disclosure of Customs Information: Section 107 of the Customs Act* (formerly D1-16-1 and D1-16-2)
- *CBSA Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act*
- CBSA Enforcement Manual Part 7 / Chapter 3
- CCTV Class of Records
- CCTV Personal Information Bank
- Video Recording and Monitoring Privacy Notice
- Video Surveillance Signage
- Audio and Video Signage
- Video Surveillance Sign Locations
- Privacy Notification given at interview rooms, primary inspection areas, secondary inspection areas and cash/information counters
- Inventory of Cameras
- PIA Action Plan
- Security Assessment Summary (work in progress)
- Security Action Plan
- *Canadian Safety and Security Program Project Charter — CSSP-2014-CP-2000*
- *OPC Report: Automated Facial Recognition In the Public and Private Sectors*
- *OPC Report: At Your Fingertips – Biometrics and the Challenges to Privacy*
- *OPC Guidance: Guidance for the Use of Body-Worn Cameras by Law Enforcement*

SECTION 10 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the PIA as they relate to the administration of the identified program or activity.

Martin Bolduc, Vice-President
Programs Branch

Signature of PIA lead for program or activity

22/01/2016
Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.

Dan Proulx, Director, ATIP Division,
Corporate Affairs Branch

Signature of Head of the institution or the delegate responsible for Section 10 under the Privacy Act

22/01/2016
Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks