

CONFIDENTIAL

**PRIVACY IMPACT ASSESSMENT
FOR:**

Passenger Protect Program

Public Safety Canada

February 2018

PRIVACY IMPACT ASSESSMENT

Section 1 – Privacy Impact Assessment Overview

Government Institution: Public Safety Canada

Government Official Responsible for the Privacy Impact Assessment	Head Institution / Delegate for section 10 of the Privacy Act
Director General, National Security Policy Directorate, National and Cyber Security Branch	Senior Assistant Deputy Minister, National and Cyber Security Branch

Name of Program or Activity of the Government Institution:

Passenger Protect Program

Description of Program or Activity:

The Passenger Protect Program (PPP) works with air carriers to screen commercial passenger flights to, from and within Canada, and uses specific, reasonable and necessary measures to address threats to transportation security, as well as to mitigate travel for the purpose of committing certain terrorism offences.

The PPP is administered by Public Safety Canada (PS) and Transport Canada (TC) in cooperation with a number of federal departments and agencies and in accordance with the *Secure Air Travel Act* (SATA), which provides the legislative framework for the PPP. As per subsection 8(1) of SATA, the Minister of Public Safety may establish a list of individuals (SATA list) whom the Minister has reasonable grounds to suspect will:

- engage or attempt to engage in an act that would threaten transportation security; or
- travel by air to commit certain terrorism offences, as defined in the *Criminal Code*, such as participating in or contributing to terrorist activities or funding, training and/or recruitment of a terrorist group.

The SATA list includes the name (given name, surname), any known alias, date of birth and gender of these persons.

Pursuant to subsection 9(1) of SATA, the Minister of Public Safety may direct an air carrier to take a specific, reasonable and necessary action to prevent a listed person from engaging in the acts described above. Actions could include directing an air carrier to deny transportation to a listed person, or requiring the listed person to undergo additional screening.

The SATA list is disclosed by PS to TC, pursuant to section 10 of SATA and communicated by TC to air carriers, pursuant to subsection 13(a) of SATA. As per the *Secure Air Travel Regulations*, air carriers are required to screen all passengers who appear to be 18 years of age or older prior to issuing them a boarding pass. When a passenger's personal information matches that of a listed person, the air carrier must confirm the person's identity and inform TC. TC, in turn, will contact PS for the purpose of issuing a direction, pursuant to subsection 9(1) of SATA. The direction made by the Minister of Public Safety, such as denying the listed person boarding or requiring them to undergo additional screening, will be communicated to the air carrier by TC, pursuant to subsection 13(c) of SATA.

The Minister of Public Safety determines who will be placed on the SATA list based on information provided by an Advisory Group chaired by PS-the Passenger Protect Advisory Group (PPAG). Nominating members of the PPAG include TC, the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and the Canada Border Services Agency (CBSA). Immigration, Refugees and Citizenship Canada (IRCC) and Justice Canada participate in meetings of the PPAG in an advisory capacity.

The PPAG considers names and supporting information provided by nominating members on individuals whom they suspect may pose a threat to transportation security or who may be seeking to travel by air for terrorism-related purposes. When making a recommendation for listing, the nominating member completes a case brief providing identifying information on an individual, as well as sufficient information necessary to support the addition of the individual's name to the SATA list. The information is collected by the nominating member, pursuant to their organization's statutory mandate and disclosed to PS and other PPAG members, pursuant to section 10 of SATA.

Pursuant to subsection 8(2) of SATA, the Minister of Public Safety must review the list every 90 days to determine whether the grounds for which each person's name was added to the list still exist and whether the person's name should remain on the list.

Note: This Privacy Impact Assessment focuses on the management of personal information in the context of Public Safety's responsibilities for the PPP in supporting the Minister of Public Safety in exercising the authorities set out in sections 8-11 of SATA. This includes the Minister of Public Safety's authorities to collect and disclose information; establish a list; review the list; and make directions.

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

Description: Includes records related to the Passenger Protect Program, which identifies individuals whom the Minister of Public Safety and Emergency Preparedness has reasonable grounds to suspect will engage or attempt to engage in an act that would threaten transportation security, or travel by air for the purpose of committing certain terrorism offences, as defined in the *Criminal Code*, as well as any directions issued by the Minister of Public Safety and Emergency Preparedness. Records include personal information related to persons considered for listing under the Passenger Protect Program, policy advice to senior decision makers and meeting documents.

Document Types: Memoranda, records of decision, threat and risk assessments, case briefs and other program-related information and correspondence.

Record Number: PS NCSB 05

Class of Record Number: _____

- ☒ Proposal for a New Personal Information Bank
☐ Proposal to modify an existing personal information bank - identify PIB registration number and current description:

Passenger Protect Program

Description: This bank describes information about individuals considered for listing under the Passenger Protect Program. This information is collected by persons or entities set out in section 10 of the *Secure Air Travel Act*, pursuant to their respective statutory mandates.

Personal information in this bank includes: name, contact information (including last known address), aliases, gender, birthdate, biographical information, citizenship status, passport/visa/residency document numbers, any other known government-issued identification number or document, any known financial information, descriptions of individuals (including photographs), descriptions of known or suspected acts or activities performed by an individual, any known fraudulent documentation presented or used by an individual, known affiliations with terrorist or criminal organizations, known criminal record and travel details, such as the name of the travel agency and agent, flight ticket information and itinerary details, and any other specific information that may be collected from air carriers or operators of a reservation system, pursuant to subsection 6(2) of the *Secure Air Travel Act*, for the purpose of identity verification and the issuance of a direction under subsection 9(1) of the *Secure Air Travel Act*.

Additional information compiled by Public Safety includes documents such as intelligence reports, threat and risk assessments, briefing notes and other correspondence obtained from persons or entities set out in section 10 of the *Secure Air Travel Act*.

Document Types: List established under subsection 8(1) of the *Secure Air Travel Act*, memoranda, records of decision, threat and risk assessments, case briefs and other program-related information and correspondence.

Record Number: PS NCSB 05

Legal Authority for Program or Activity:

The *Secure Air Travel Act* (SATA) came into force on August 1, 2015, to create a legislative framework for the PPP. SATA expanded the mandate of the PPP beyond aviation security to include the prevention of terrorist travel. Among other things, SATA clearly outlines the authorities of the Minister of Public Safety to list individuals; to share information related to the list with and among domestic partners under certain conditions; and to direct air carriers to deny boarding or take other measures with respect to listed individuals, such as requiring additional screening.

To support the administration of the PPP, the *Secure Air Travel Regulations* (SATR) came into force to align with the new statutory authorities set out in SATA. SATR sets out the obligations of air carriers to verify the identity of each traveller who appears to be 18 years of age or older, to inform the Minister of Transport of a match to the list, as well as to ensure compliance with other requirements.

In the context of the PPP, PS may collect information from Global Affairs Canada (GAC), pursuant to Crown prerogative, the *Privacy Act*, or the *Security of Canada Information Sharing Act*. This information would be disclosed by GAC in cases where a Canadian citizen on the SATA list were seeking consular assistance abroad because he/she faced travel restrictions. The information would be disclosed by GAC to PS in order to facilitate the Canadian citizen's return to Canada and for the purpose of facilitating the issuance of a direction by the Minister of Public Safety, pursuant to subsection 9(1) of SATA.

The Minister of Public Safety may also disclose SATA information to the Privy Council Office for the purpose of supporting the Prime Minister in matters related to national security (e.g., to inform the Prime Minister of a direction issued by the Minister of Public Safety). This information would be shared with the Privy Council Office, pursuant to constitutional convention for the purpose of supporting discussions between ministers.

Summary of the project / initiative / change

The PPP is an important part of Canada's national security framework. TC launched the PPP in 2007 to protect aviation by denying boarding to any specified person whom the Minister of Transport determined to be an immediate threat to aviation security. Sections of the *Aeronautics Act* and the *Identity Screening Regulations* were used in order to allow for the specifying of individuals, to respond to threats through an emergency direction, collecting and sharing information with air carriers, and for monitoring air carrier compliance with information-protection requirements.

In February of 2011, the PPP underwent machinery of government changes. An Order in Council transferred the responsibility for determining the individuals who should be included on the list from the Minister of Transport to the Minister of Public Safety. Communicating the list of names of these individuals to air carriers remained the responsibility of the Minister of Transport, as did the issuance of emergency directions to deny boarding in cases where an air carrier identified a potential match to a listed person, pursuant to paragraph 4.81(1)(b) of the *Aeronautics Act*.

In August 1, 2015, SATA came into force to provide a solid legislative framework for the PPP. Among its provisions, SATA:

- sets out authorities of the Minister of Public Safety and the Minister of Transport;
- clarifies authorities relating to the collection and disclosure of information;
- broadens the mandate of the PPP to include the prevention of travel by air for the purpose of committing certain terrorism offences, as defined in the *Criminal Code*, such as recruiting, training, or conducting attacks;
- transfers the authority for making directions to air carriers to take a specific, reasonable and necessary action against a listed person from the Minister of Transport to the Minister of Public Safety. The Minister of Transport remains responsible for communicating the list and any direction made by the Minister of Public Safety to air carriers, for disclosing information collected from air carriers and operators of aviation reservation systems to the Minister and any other person or entity referred to in section 10, as well as for ensuring compliance with aviation-related laws and regulations.

For more information on the PPP please visit the program's website at:

<https://www.publicsafety.gc.ca/cnt/ntnl-scrnt/cntr-trrrsm/pssngr-prtct/hw-pssngr-prtct-wrks-en.aspx>

Section II – RISK AREA IDENTIFICATION & CATEGORIZATION

Type of Program or Activity

Level of Risk to Privacy

Program or activity that does NOT involve a decision about an identifiable individual

☐ 1

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.

Administration of Programs / Activity and Services

☒ 2

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...).

Compliance / Regulatory investigations and enforcement

☐ 3

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).

Criminal investigation and enforcement / National Security

☐ 4

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).

Type of Personal Information Involved and Context

**Level of
risk to
privacy**

Only personal information provided by the individual – at the time of collection – relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities.

☐ 1

The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.

Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.

☐ 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

For example: the personal information by association indirectly reveals information on the health, financial situation, religious or lifestyle choices of the individual.

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

☒ 4

For example: the personal information by association indirectly reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and other individuals, such as relatives.

Program or Activity Partners and Private Sector Involvement

**Level of
risk to
privacy**

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

Duration of the Program or Activity

**Level of
risk to
privacy**

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or an activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Program Population

Level of risk to privacy

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

Technology & Privacy

Risk to privacy

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

Does the new or modified program or activity require any modifications to IT legacy systems and / or services?

☐ YES

☒ NO

The new or modified program or activity involve the implementation of one or more of the following technologies:

- Enhanced identification methods

☐ YES

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).

☒ NO

Identify the applicable category(ies):

- Use of Surveillance:

☐ YES

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...

☒ NO

Identify the applicable category(ies):

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

☐ YES

For the purposes of the Directive on PIA, government institution 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 behavior.

☒ NO

Identify the applicable category(ies):

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.

Personal Information Transmission

Level of
risk to
privacy

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

The personal information is used in a system that has connections to at least one other system.

☐ 2

The personal information is transferred to a portable device or is printed.

☐ 3

USB key, diskette, laptop computer, any transfer of the personal information to a different medium.

Note: For PS¹ internal record keeping purposes only, signed records of decision and memoranda containing personal information are scanned on a Top Secret accredited printer, transferred to a USB, then saved on a diskette on a stand-alone laptop computer for final transfer to a secure electronic communications system where the personal information is stored.¹

The personal information is transmitted using wireless technologies.

☒ 4

Risk Impact to the Institution

Level of
risk to
privacy

Managerial harm.

☐ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☐ 2

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.

Financial harm.

☐ 3

Lawsuit, additional moneys required, reallocation of financial resources.

Reputation harm, embarrassment, lost of credibility.

☒ 4

Decrease confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Risk Impact to the Individual or Employee

Level of
risk to
privacy

Inconvenience.

☐ 1

Reputation harm, embarrassment.

☐ 2

Financial harm.

☐ 3

Physical harm.

☒ 4

¹ Refers to a technology system that has been certified and accredited by the Communications Security Establishment Canada to meet Government of Canada security standards.

SECTION III - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Define each element of personal information collected	Define sub-elements of personal information associated with the element identified in the first column	How is the personal information recorded?
1. Listed person's name	Surname / given name / initial(s) / aliases	☒ Electronic ☒ Hard copy ☒ Visual Image Recordings
2. Address	Street name / street number / city / province / postal code of last known address or location	
3. Date of birth		
4. Place of birth		
5. Citizenship status		
6. Gender		
7. Physical description	Weight / height / Eye colour / hair colour / distinguishing features / photographs	
8. Government-issued identification	Passport / visa / residency / other document number	
9. Financial information		
10. Criminal history	Investigations / arrests / charges / conviction dates and locations	
11. Threat-related activities	Description of known or suspected activities / any known fraudulent documentation presented or used by the individual / any known affiliations with terrorist or criminal organizations	
12. Travel details	Name of travel agency and agent / travel itinerary / flight numbers	
13. Any other information that may be collected during the process of identity verification		

SECTION IV - 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.

Flow of Personal Information for Listing

The Minister of Public Safety, or his/her delegate, determines who will be placed on the SATA list based on recommendations made by the PPAG. Nominating members of the PPAG include TC, CSIS, the RCMP, and the CBSA. IRCC and Justice Canada (PS Legal Services) participate in meetings of the PPAG in an advisory capacity. The PPAG considers names and supporting information provided by nominating members on individuals whom they suspect may pose a threat to aviation security or who may be seeking to travel by air for terrorism-related purposes. When making a recommendation for listing, the nominating member completes a case brief, providing information on an individual, as well as sufficient information necessary to support the addition of the individual's name to the list. The information is sent to PS for consideration [REDACTED]

[REDACTED] pursuant to section 10 of SATA.

After a review of the information, the PPAG will provide a recommendation to the Minister of Public Safety, or his/her delegate, as to whether an individual should be listed, pursuant to subsection 8(1) of SATA. Should the Minister of Public Safety, or his/her delegate, agree with the recommendation, the SATA list will be updated accordingly. The list will be updated at a minimum every 90 days, as per subsection 8(2) of SATA, to determine whether the grounds for which each person's name was added to the list still exist and whether the person's name should remain on the list.

[REDACTED]

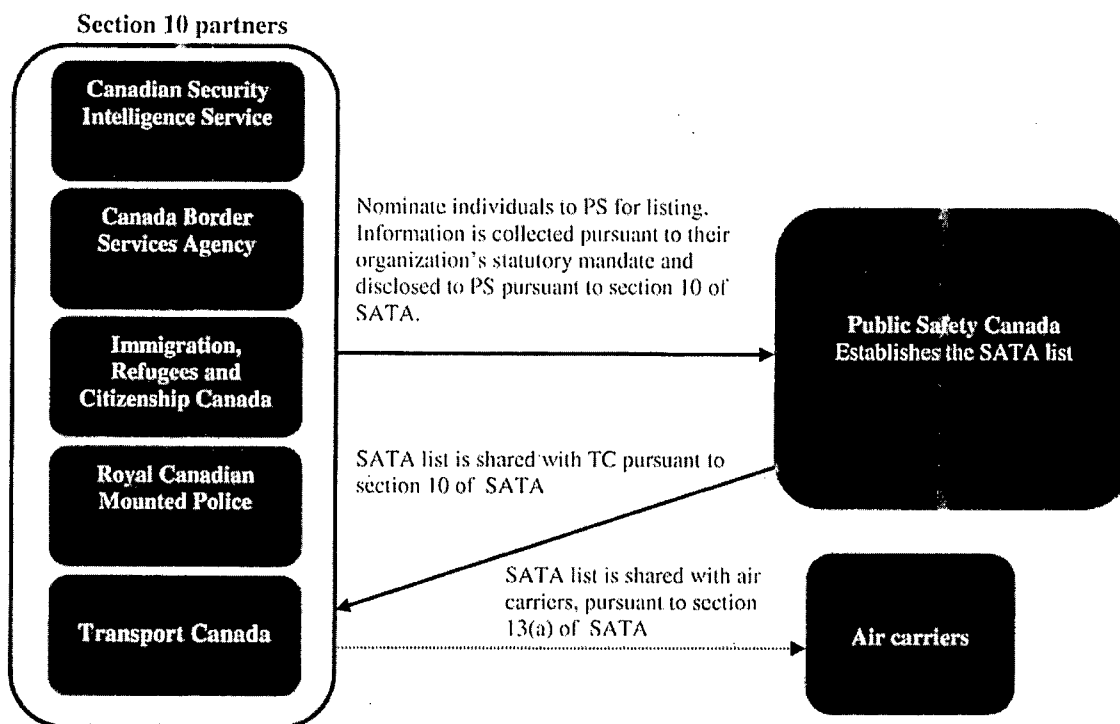
For further details, please refer to the Graphic A below.

Flow of Personal Information for Making Directions

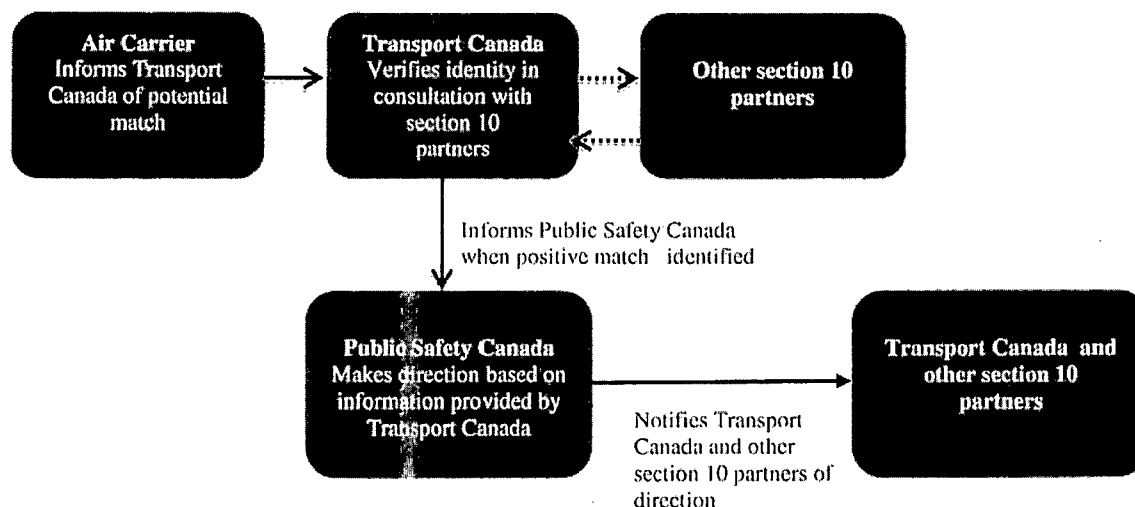
Should a listed person attempt to board an aircraft, TC communicates this information to the Minister of Public Safety, or his/her delegate, pursuant to subsection 13(d) of SATA. This information is [REDACTED]. Pursuant to section 9(1) of SATA, the Minister of Public Safety, or his/her delegate may then direct the air carrier to take a specific, reasonable and necessary action to prevent a listed person from engaging or attempting to engage in an act that would threaten transportation security, or from travelling by air to commit certain terrorism offences. The direction is communicated to the air carrier by TC, pursuant to section 13(c) of SATA.

For further details, please refer to the Graphic B below.

Graphic A. - Information flow for Listing



Graphic B. - Information Flow for Making Directions



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
A federal government institution (identify from what PIB the information is obtained)	As per section 10 of SATA, the following persons or entities may assist the Minister in the administration and enforcement of the PPP, by collecting information from, and disclosing information to the Minister of Public Safety and each other: - the Minister of Transport - the Minister of Citizenship and Immigration - a member of the RCMP or a civilian employee of that police force - the Director or an employee of CSIS - an officer or employee of the CBSA - any other person or entity prescribed by regulation The Minister of Public Safety or his/her delegate determines who will be placed on the list based on recommendations made by the PPAG, whose nominating members include representatives from TC, the RCMP, CSIS, and the CBSA. IRCC and Justice Canada participate in the PPAG in an advisory capacity. Members of the PPAG collect information pursuant to their organization's statutory mandate and disclose information to PS and other PPAG members pursuant to section 10 of SATA. Personal information may, therefore, be obtained from the following PIBs: - TC PPU 001 - CSIS PPU 070 - RCMP PPU 011 - CBSA PPU 035 - CIC PPU 081 In certain instances, PS may collect information from Global Affairs Canada (GAC). The information would be disclosed by GAC to PS, pursuant to the Crown prerogative, the <i>Privacy Act</i>, or SCISA, in cases where a Canadian citizen on the SATA list were seeking consular assistance abroad because he/she faced travel restrictions. The purpose of the disclosure would be to facilitate the Canadian citizen's return to Canada, specifically with respect to the issuance of a direction pursuant to subsection

	9(1) of SATA.
--	---------------

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
Passenger Protect Inquiries Office (PPIO)	Information may be disclosed to the PPIO in cases where a listed person had applied for administrative recourse, or where an individual had contacted the PPIO because he/she had experienced travel delays. Information would be disclosed pursuant to subsection 15(1) of SATA and would be found in PS PPU 0051.

External Use and Disclosure

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

SOURCE	IDENTIFY THE SOURCE
A federal government institution	Personal information may be disclosed to persons or entities assisting the Minister of Public Safety in the administration of the PPP, as per section 10 of SATA. This would include: - the Minister or Transport - the Minister of Citizenship and Immigration - a member of the RCMP or a civilian employee of that police force - the Director or an employee of CSIS - an officer or employee of the CBSA - any other person or entity prescribed by regulation Personal information may be found in the following PIBs: - TC PPU 001 - CSIS PPU 070 - RCMP PPU 011 - CBSA PPU 035 - CIC PPU 081 - JUS PPU 010 The Minister of Public Safety may disclose information to the Privy Council Office for the purpose of supporting the Prime Minister in matters related to national security (e.g., to inform the Prime

	Minister of a direction issued by the Minister of Public Safety). This information would be shared pursuant to constitutional convention. Information would be included in PCO PPU 005.
--	---

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	PS will store personal information related to listed persons in accordance with the Treasury Board of Canada Secretariat's <i>Policy on Government Security</i> and the <i>Operational Security Standard for Physical Security</i>. Given the sensitivity of individual data elements and the program overall, information pertaining to the listing of persons will be handled commensurate to the security level of Top Secret. Personal information will be stored on a Top Secret network, and in a Top Secret accredited safe in a high security zone, the security listings of which are outlined in the <i>Operational Security Standard for Physical Security</i>².  Information related to the PPP may also be stored and retained within the following organizations: TC, CSIS, the RCMP, the CBSA, IRCC, Justice Canada and the Privy Council Office. Any information would become part of the respective organization's holdings and therefore subject to its retention and disposal schedule. These organizations are also subject to the <i>Privacy Act</i> and are expected to comply with the legislation and store/handle personal information
----------------------------------	---

² A high security zone also referred to as a restricted access zone is defined as "an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications recommended in the Threat and Risk Assessment, monitored continuously, i.e., 24 hours a day and 7 days a week and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel."

	accordingly.
--	--------------

(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 trans-jurisdictional issues. Where 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:		
Identify Groups or Areas / or Divisions	Where appropriate - positions who have access or use the personal information	Geographical Location
Public Safety Canada		
Office of the Minister of Public Safety and Emergency Preparedness	Minister of Public Safety and Emergency Preparedness	National Capital Region
Office of the Deputy Minister of Public Safety	Deputy Minister of Public Safety Associate Deputy Minister of Public Safety	National Capital Region
Office of the Senior Assistant Deputy Minister, National and Cyber Security	Senior Assistant Deputy Minister,	National Capital Region
National Security Policy Directorate	Director General Director Manager Analysts Administrative Support Staff	National Capital Region
National Security Operations Directorate	Director General Director Manager Analysts Administrative Support Staff	National Capital Region
Office of the Assistant Deputy Minister, Emergency Management and Programs Branch	Assistant Deputy Minister	National Capital Region

Government Operations Centre		National Capital Region
Corporate Management Branch, [REDACTED]		National Capital Region
Chief Information Officer Directorate, [REDACTED] [REDACTED]		National Capital Region
PS Legal Services Unit (Department of Justice)		National Capital Region
Access to Information and Privacy (ATIP) Unit	ATIP Coordinator ATIP Analyst(s)	National Capital Region
Other federal government Institution responsible for program or activity:		
RCMP National Security, Federal Policing National Security		National Capital Region
CSIS [REDACTED]		National Capital Region
TC Aviation Security		National Capital Region
CBSA Enforcement and Intelligence Operations		National Capital Region
IRCC Case Management Branch		National Capital Region
Privy Council Office Security and Intelligence		National Capital Region

SECTION V - PRIVACY COMPLIANCE ANALYSIS

Collection Authority (Section 4 of the *Privacy Act*)

1. Has each element and sub-elements of personal information collected or to be collected been justified in terms of its necessity to the administration of the program or activity?

Note: "Necessary" is a higher standard than merely being useful.

☒ YES
☐ NO

Legal Requirement: s. 4 *Privacy Act*

Policy requirement

Limit the collection of personal information to what is demonstrably necessary for the program or activity. Institutions must abide by any applicable statutory prohibitions.

Comment:

Personal information is collected for the purposes of the PPP.

		The elements and sub-elements of personal information collected are necessary for the purposes of meeting the threshold for listing as set out in subsection 8(1) of SATA, for identity verification supporting the issuance of a direction to an air carrier related to a listed person, pursuant to subsection 9(1) of SATA and to mitigate the risk of false positive matches to a listed person.
2. Is the Social insurance Number (SIN) being collected?	☐ YES ☒ NO	

Direct Collection – Informed of Purpose (Section 5 of the <i>Privacy Act</i>)		
3. Is the information collected directly from the individual?	☒ YES ☒ NO	If NO ☒ Ensure that the requirements stated at Question 5 are met. <u>Policy requirement:</u> A detailed "Privacy Notice" is required where personal information is collected for an administrative purpose. <u>Legal Consideration:</u> Section 10 of the <i>Privacy Regulations</i> provides for the rights or actions under the act to be exercised or performed on behalf of a minor, an incompetent person, a deceased person or a person authorized by law to administer the affairs of that person. <u>Comment:</u> Under the <i>Privacy Act</i>, privacy notices are not required if the notification would result in the collection of inaccurate information, would defeat the purpose of the collection; or would compromise the use of the information collected. Individuals listed under the PPP are not informed of their listing. Notifying the individual of the use and purpose of the collection of their personal information could result in inaccurate information. It would also defeat the purpose of collection, and compromise the integrity of the PPP and other national security interests. When a potential match has been identified by an air carrier, information could be directly collected from the individual for the purpose of identity verification. This information would be provided to the Minister of Public Safety or his/her delegate, pursuant to subsection 6(2) of SATA, to inform the

		decision to issue a direction to an air carrier, pursuant to subsection 9(1) of SATA, such as denying the listed person boarding.
4. Is the information collected from another source with informed consent of the individual?	☐ YES ☒ NO	If NO — or if YES and NO ☒ Ensure that the requirements stated at Question 3 are met. Policy requirement: Inform the individual of what information will be collected, how the information will be used and what source will be asked to provide the information. Individuals should also be informed of any alternatives or consequences that may result from their refusal to authorize any indirect collection. Written authorization from the individual to whom the personal information pertains is required. Collection of personal information from another source may be required in order to ensure that the personal information is accurate and up-to-date. See Question 8 regarding accuracy requirements. Comment: Information holdings may include personal information that was collected for the purpose of determining eligibility for other government programs (i.e., passport application). In such cases, at the time of application, the individual would have consented to the collection, use and disclosure of his/her personal information as outlined in the Privacy Notice Statement.
5. Is the information collected from another source without notice to or consent from the individual? - Is the collection a result of a disclosure under subsection 8(2) of the Act? - Would direct notification of the individual result in the collection of inaccurate information? - Would direct notification of the individual defeat the purpose or prejudice the use for which the information is collected? - Is the information used for a non-administrative decision about the individual?	☐ YES ☒ NO ☒ YES ☐ NO ☒ YES ☐ NO ☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☒ Ensure that the personal information bank's description adequately reflects the nature of such activities. If NO Action Required to Support Legal & Policy Compliance: ☐ Direct collection must be adopted and the individual must be notified of the purpose of the collection. ☒ Ensure that the requirements stated at Question 3 are met. Policy principle The exception to direct collection should be used sparingly. It is primarily intended for use by investigative bodies in those circumstances where direct collection would jeopardize the

		investigation. <u>Comment:</u> Information is collected pursuant to section 10 of SATA. Persons or entities specified in section 10 of SATA collect information pursuant to their organization's statutory mandate.
6. Will the personal information collected only be used for: • The purpose for which it was collected or a purpose consistent with that purpose? • A purpose consistent with section 8(2) of the Act?	☒ YES ☐ NO ☒ YES ☐ NO	<u>Policy requirement</u> Inform the individual at the time of collection of any intended uses or disclosures that are not directly related to the program or activity for which the information is being collected. (This would be considered an indirect collection by other programs.) <u>Policy Requirement</u> Ensuring that individuals are notified in advance of follow-up activities including all means of communication to be expected by the government institution. The individuals will be in a position to recognize legitimate requests for personal information. This will help minimize the risk of individuals providing their personal information under a false pretext. <u>Comment:</u> Information collected is only used for the purpose for which it was collected. Information is collected pursuant to section 10 of SATA, for the purpose of establishing the SATA list, pursuant to subsection 8(1) of SATA, reviewing the list pursuant to subsection 8(2) of SATA or issuing a direction pursuant to subsection 9(1) of SATA.

Retention (Section 6 of the <i>Privacy Act</i>)		
7. Is the personal information being used to make a decision or as part of a process to make a decision that directly affects an identifiable individual? This includes use for verification/authentication purposes.	☒ YES ☐ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Prepare and obtain approval for a retention schedule based on your legal requirements and operational needs; AND ☒ Retain records for a minimum of 2 years as required by the <i>Privacy Regulations</i>; OR ☐ Obtain consent of the individual to dispose of the personal information earlier than the minimum 2 year retention period; AND ☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. <u>Policy requirement</u> Retain personal information for a minimum of two years, as detailed in section 4 of the <i>Privacy Regulations</i>. In accordance with the <i>Library and Archives of Canada Act</i>, only the Librarian and Archivist of Canada may authorize the

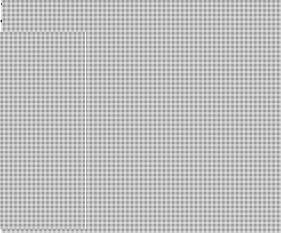
		disposition of government records by issuing Records Disposition Authorities (RDA). Comment: Information on listed individuals will be retained in accordance with the records retention and disposition schedule set at the following: - <u>Adult at time of listing:</u> 6 years after the name is removed from the list; - <u>Minor at time of listing:</u> 6 years + the difference between the age at time of listing and 18 years of age Any other personal information collected in the administration of the PPP will be retained for 2 years. After such time, records of archival value will be transferred to Library and Archives Canada. Those with no business value will be destroyed according to government standards.
Accuracy – (Section 6 (2) of the <i>Privacy Act</i>)		
8. What measures will be taken to ensure that the personal information used in administrative decisions is accurate, up-to-date and complete? (More than one option may apply) - Direct collection or validation with the individual. - Technological means to identify keystroke errors and discrepancies. - Personal information matching program to verify personal information integrity against a "reliable source" where authorized or where consent was obtained. - In cases where direct collection or consent is not feasible, obtain information from trusted sources (either public or private) and verify accuracy against existing personal information before use. If Other – please define below:	☒ YES ☐ YES ☒ YES ☒ YES ☐ YES	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that, if applicable, your institution's PIB mentions the use of periodic personal information matching as a consistent use. Legal and Policy Requirements Subsection 6(2) of the <i>Privacy Act</i> requires government institutions to take <i>all reasonable steps</i> to ensure that personal information that they use for an administrative purpose is as accurate, up-to-date and complete as possible. Decisions that directly affect individuals must be made on the basis of accurate, up-to-date and complete information as possible. If periodic personal information matching occurs for the purposes of ensuring accuracy of information, institutions must reflect this under the "consistent use" section of the relevant PIB. Comment: PS receives personal information for nominations of listed individuals from PPAG members, pursuant to section 10 of SATA, and relies on these members to ensure that information provided is accurate,

	complete and up-to-date. Governance documents for the PPP include clauses to ensure the quality of information. For instance, with respect to the PPAG, PPAG members are to challenge the accuracy of any information about listed persons, or those persons being recommended for listing. There is a requirement in subsection 8(2) of SATA for the Minister of Public Safety or his/her delegate to review the list every 90 days to determine whether the grounds for which each person's name was added to the list still exist and whether the person's name should remain on the list. As such, PPAG members are required, on a regular basis, to review their information holdings on listed persons to ensure the information that is considered by the PPAG is up-to-date and factually correct. When a positive match to a listed person is identified, pursuant to subsection 9(1) of SATA, the Minister of Public Safety or his/her delegate may direct the air carrier to take a specific action against the listed person, such as the denial of boarding. Prior to making this decision and issuing a direction to the air carrier, the Minister of Public Safety, or his/her delegate will take into consideration multiple data elements that have been gathered to ensure a positive match between the listed person and passenger information provided by the air carrier. This information may be collected directly from the person and is done for the purpose of limiting the chance of errors in matching and reducing the risk that a traveller will be falsely identified and potentially denied boarding an aircraft.
--	---

Use (Section 7 of the <i>Privacy Act</i>)		
9. Is there an activity log attached to the personal information record to record uses not described in the Personal Information Bank (Info Source)?	☒ YES ☐ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ An activity log is attached to personal information records when used for consistent but unreported use. ☐ The Privacy Commissioner is advised of this consistent use. ☐ The PIB description is amended, in time for the next edition of Info Source, to include the

	unreported use. Legal Requirements: Section 9(4) of the <i>Privacy Act</i> requires a government institution to report to the Privacy Commissioner any consistent use of personal information that has not been included in the Index, and to ensure that the use is included in the next statement of consistent uses set forth in the next edition of the Index. Policy Requirement If personal information used for a consistent purpose that is not identified in a personal information bank – the head of the institution or delegate must notify the Privacy Commissioner Comment: PS will be responsible for maintaining an activity log and reporting uses not described in the personal information bank to the Senior Assistant Deputy Minister of National and Cyber Security and the departmental ATIP coordinator.
--	---

Disclosure (Section 8 of the <i>Privacy Act</i>)		
10. Are processes in place to ensure that personal information will only be disclosed to individuals within and without the government institution who have a "need to know" and that there are adequate privacy practices to ensure the confidentiality and integrity of the personal information? This includes procedures to prevent against loss or theft. This covers the entire lifecycle of the personal information: • Collection • Use • Retention • Disposition. This includes disclosures to other government institutions, other levels of government, other jurisdictions, foreign governments, international organizations or private sector organizations	☒ YES ☐ NO	Policy requirement Government institutions are to ensure that adequate safeguards are in place when disclosing information. This includes having an action plan for privacy breaches (unauthorized disclosures) and measures (physical, logical, administrative) to ensure that only the people that "need to know" have access to the personal information. <i>See Directive on Privacy Practices</i> Comment: PS has consulted its Legal Services Unit, Information Technology Security Operations and Departmental Security Office to ensure that there are adequate information technology, administrative and security measures in place to ensure that disclosure is done in accordance with section 8 of the <i>Privacy Act</i>. A Departmental Security Policy is available on the PS intranet site to ensure employees are aware of the requirement of limiting access to personal / sensitive information to a strictly need-to-know basis. In addition, Privacy Breach Guidelines are available on the Intranet site to ensure that employees are aware of their responsibilities, if a breach should occur.

	In the context of the PPP and the PPAG, procedures for the collection, transmission, storage, disposal of personal information and access to it, are in compliance with the Treasury Board Secretariat's <i>Policy on Government Security</i> and <i>Operational Security Standards on Physical Security</i>, the <i>Privacy Act</i>, the <i>Security of Information Act</i>, the <i>Security of Canada Information Sharing Act</i>, the <i>Secure Air Travel Act</i> and <i>Secure Air Travel Regulations</i>, and the conditions described therein. Access to personal information is restricted to a small number of designated PS officials who are directly involved in the management of the PPP, and who have a need to know.  With respect to SATA, which provides the legislative framework for the PPP, section 10 sets out the persons or entities who may assist the Minister of Public Safety in the administration and enforcement of the Act, including by collecting information from, and disclosing information to, the Minister and each other. Information is collected, pursuant to section 10 of SATA, for the purpose of establishing the SATA list pursuant to subsection 8(1) of SATA, reviewing the list, pursuant to subsection 8(2) of SATA; or issuing a direction, pursuant to subsection 9(1) of SATA. Disclosure of information takes place in accordance with the provisions and restrictions set out in SATA and other relevant legislation. As per section 20 of SATA, it is prohibited to disclose the list or whether or not any individual is or was a listed person, except as required for certain purposes set out in SATA. Any contravention is considered an offence punishable on summary conviction. Caveats are attached to personal information being shared in order to indicate specific privacy limitations. Furthermore, the PPP's website contains
--	--

		information on the safeguards in place to protect personal information.
11. Is the disclosure of the personal information governed by: A Memorandum of understanding? An accord? An arrangement? A contract? If Other – please define below:	☒ YES ☐ YES ☐ YES ☐ YES	If YES Action Required to Support Legal & Policy Compliance: ☒ Ensure the PIB description identifies this use. ☐ Ensure that the notification or consent notice mentions this use. ☐ Ensure contractual clauses are included to protect personal information.
		Contracts that are established with private sector entities outline measures and provisions to address the following: ☐ Control over the personal information; ☐ Limitations on collection and handling as well as any prohibitions regarding the personal information for the purposes of the contract; ☐ Disposition of the personal information, where relevant; ☐ Administrative, technical and physical safeguards; and ☐ Obligations of other parties acting on behalf of the government institution. If NO Action Required to Support Legal & Policy Compliance: ☐ Prepare a written statement describing the nature of the information sharing and have it approved by the relevant parties. Policy on Privacy Protection Measures are to be established, when personal information is involved, to ensure that the government institution meets the requirements of the <u>Privacy Act</u> when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations. Ensure that appropriate privacy protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information. If any portion of the project (administration, service delivery, system maintenance or personal information storage) involves the use of a third-party contractor, care must be taken to ensure that institutions continue to fulfill their privacy obligations. Comment: Memoranda of Understanding are being drafted

		and/or updated, in consultation with PPAG members, and other partners, to reflect respective roles and information management practices related to the PPP. A Passenger Protect Program Manual (which includes standard operating procedures) is in the process of being finalized to govern Program operations.
--	--	--

Technology and Privacy

12. Will the system/software /program application employ cookies or other tracking methods to collect personal information about users and their transactions? If so, for what purposes will the collected information be used and how long will the information be retained? Please define purpose and retention period below:	☐ YES ☒ NO	
13. Does the new or modified program or activity result in an increased ability for surveillance or monitoring of a given target population?	☐ YES ☒ NO	

Privacy Considerations Related to Compliance / Regulatory Investigation and Enforcement

14. Is the legal authority for conducting compliance / regulatory investigation and enforcement the same as the legislative authority for the program or activity?	☒ YES ☐ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ The activities are listed in the Privacy Notice; ☒ The activities are listed in the PIB's description.
---	--	---

Privacy Considerations Related to Search and Seizure

15. What is the specific legal authority for conducting regulatory or criminal enforcement, surveillance or intelligence gathering? Not applicable.
--

Action Required to Support Legal & Policy Compliance:

☐ Request legal advice from your Legal Services Unit about compliance with section 8 of the *Charter of Rights and Freedoms*, the *Privacy Act* and other applicable acts

SECTION VI - Summary of Analysis and Recommendations (as applicable) Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified

Risk Area	Category/Description	Level of Risk	Conclusions and Actions
Type of Program or Activity	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 program/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...)	2	Personal information is collected in order to determine whether an individual meets the threshold for listing under the PPP, pursuant to subsection 8(1) of SATA. Individuals on the SATA list are those whom the Minister of Public Safety has reasonable grounds to suspect will engage or attempt to engage in an act that would threaten transportation security, or will travel by air for the purpose of committing certain terrorism offences, as defined in the <i>Criminal Code</i>. Based on a direction issued by the Minister of Public Safety or his/her delegate, pursuant to subsection 9(1) of SATA, these individuals could be denied transportation by an air carrier in order to prevent them from engaging in the acts described above. Several elements of personal information (e.g. passport number, date of birth) are collected by PPAG members to support this process and are necessary to mitigate the risk of false positives and to ensure that the intended individuals are listed under the PPP, pursuant to subsection 8(1) of SATA. In addition, PPAG members are required by law to collect information for purposes consistent with their respective mandates.
Type of Personal Information Involved and Context	Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. For example: the personal information by	4	Due to the national security implications of the PPP, sensitive personal information, including detailed profiles, is used to determine whether an individual meets the threshold to have his/her name added to the list pursuant to subsection 8(1) of SATA and whether a direction may need to be issued by the Minister of Public Safety or his/her delegate, pursuant to subsection 9(1) of SATA, to an air carrier to prevent the person from engaging in the acts described above.

	association indirectly reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and other individuals, such as relatives.		
Program or Activity Partners and Private Sector Involvement	With other federal institutions	2	Public Safety has overall responsibility for the PPP. It is, however, reliant on those persons or entities specified in section 10 of SATA to: - identify those individuals who should be recommended to the Minister of Public Safety or his/her delegate for listing under the PPP, pursuant to subsection 8(1) of SATA; - verify personal information for the purpose of confirming a match to a listed person before the Minister of Public Safety or his/her delegate issues a direction to an air carrier, pursuant to subsection 9(1) of SATA.
Duration of the Program or Activity	Long-term program Existing program that has been modified or is established with no clear "sunset"	3	The list is reviewed every 90 days, pursuant to subsection 8(2) of SATA, to determine whether the grounds for which a person's name was added to the list still exist and whether the person should still be listed. Once a person's name is removed from the list, personal information is retained in accordance with the records retention and disposition schedule.
Program Population	The program affects certain individuals for external administrative purposes	3	As per subsection 8(a) of SATA, the program affects individuals whom the Minister of Public Safety has reasonable grounds to suspect: - will engage or attempt to engage in an act that would threaten transportation security; or - are attempting to travel abroad to commit certain terrorism offences, as defined in the <i>Criminal Code</i>, such as terrorist attacks, funding for weapons, training and recruitment. As per section 20 of SATA, it is prohibited to disclose either the list, or whether or not any individual is or was a listed person, except under certain circumstances. Any contravention is considered an offence punishable on summary conviction.

			Under subsection 8(2) of SATA, the list is reviewed every 90 days, to determine whether the grounds for which each person's name was added to the list still exist and whether the person's name should remain on the list.
Personal Information Transmission	The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled. 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. The personal information is transmitted using wireless technologies.	4	Given the sensitivity of individual data elements and the program overall, information pertaining to the listing of persons is handled commensurate to the security level of Top Secret. Personal information will be stored on a Top Secret network, and in a Top Secret accredited safe in a high security zone, the security listings of which are outlined in the <i>Operational Security Standard for Physical Security</i>³.
Risk Impact to the Institution	Financial harm. Lawsuit, additional moneys required, reallocation of financial resources Reputation harm, embarrassment, loss of credibility.	4	As per section 20 of SATA, it is prohibited to disclose either the list, or whether or not any individual is or was a listed person, except under certain circumstances. Any contravention is considered an offence punishable on summary conviction.

³ A high security zone also referred to as a restricted access zone is defined as "an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications recommended in the Threat and Risk Assessment, monitored continuously, i.e., 24 hours a day and 7 days a week and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel."

	Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised and government priority compromised impact on the Government of Canada Outcome areas.		
Risk Impact to the Individual or Employee	Inconvenience. Reputation harm, embarrass Financial harm. Physical harm.	4	As per section 20 of SATA, it is prohibited to disclose either the list, or whether or not any individual is or was a listed person, except under certain circumstances. Any contravention is considered an offence punishable on summary conviction.

SECTION VII - SUPPLEMENTARY DOCUMENTS LIST

- PIB (Annex A)
- Class of Records (Annex B – Info Source)

SECTION VIII – 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 core PIA as they relate to the administration of the identified program or activity.



Signature of PIA lead for program or activity (DG or senior official with functional authority for program)

3/1/18

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.



Signature of Head of the institution or the delegate responsible for Section 10 under the Privacy Act (ADM or other delegated authority)

3/29/18

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

Template for Development of new Personal Information Banks

Name of Institution:	Public Safety Canada
ATIP Contact Name:	Jennifer Schofield
Phone Number:	613-991-2929
Email Address:	Jennifer.schofield@canada.ca
Title:	Passenger Protect Program
• Must be descriptive and reflect information being described by PIB. • It is helpful when the title gives a pointer to the program to which the PIB relates.	
Description:	This bank describes information about individuals considered for listing under the Passenger Protect Program. This information is collected by persons and entities set out in section 10 of the <i>Secure Air Travel Act</i>, pursuant to their respective statutory mandates. Personal information in this bank includes: name, contact information (including last known address), aliases, gender, birthdate, biographical information, citizenship status, passport/visa/residency document number, any other known government-issued identification number or document, any known financial information, descriptions of individuals (including photographs), descriptions of known or suspected acts or activities performed by an individual, any known fraudulent documentation presented or used by an individual, any known affiliations with terrorist or criminal organizations, any known criminal record and travel details, such as name of the travel agency and agent, flight ticket information and itinerary details, and any other specific information that may be collected from air carriers or operators of a reservation system, pursuant to subsection 6(2) of the <i>Secure Air Travel Act</i>, for the purpose of identity verification, or the issuance of a direction under subsection 9(1) of the <i>Secure Air Travel Act</i>. Additional information compiled by Public Safety includes documents such as intelligence reports, threat and risk assessments, briefing notes and other correspondence obtained from persons and entities set out in section 10 of the <i>Secure Air Travel Act</i>.
• An explanatory statement of the information described by the bank. • It should indicate the specific personal information elements contained in the records to which the bank relates, i.e. names, addresses, telephone numbers, age, sex, marital status, country of birth, citizenship, social insurance numbers, employee numbers, race, fingerprints, blood types, etc.	
Note:	

This is the only optional field. • May contain information about how to access the information described by the PIB, i.e. please provide Surname, given name and telephone number. • Should not contain "contact" information within the institution creating the PIB	
Class of Individuals:	Individuals considered for listing under the Passenger Protect Program
Identifies the group or category of individuals about whom the information relates, i.e. current and former employees, contractors, program applicants, etc.	Personal information described in this bank is used to assist the Minister of Public Safety and Emergency Preparedness, or his/her delegate, in deciding whether to list a person under the Passenger Protect Program, pursuant to subsection 8(1) of the <i>Secure Air Travel Act</i>, and to issue a direction to an air carrier, pursuant to subsection 9(1) of the <i>Secure Air Travel Act</i>. The authority to collect personal information is granted under section 10 of the <i>Secure Air Travel Act</i>.
Purpose: • Provides a clear and concise explanation of the reason for which the personal information was obtained or compiled. • The reason must be directly related to a government program or activity. • The purpose may be stated in terms of the kinds of decisions that are made, based on the information Consistent Uses: • Itemizes the potential or related uses for which the personal information may be used or disclosed. • Uses must conform with the original purpose for which the information was collected - which might reasonably be considered to be related. • Must have a reasonable and direct connection to the original purpose(s) • State all consistent uses of the information. Data matching activities and disclosures should be listed under this heading. • If there are no Consistent Uses, please include a statement to that effect. Note on Disclosure: There are circumstances under which personal information may be disclosed to third parties. If personal information is disclosed, state the third party involved.	Personal information may be disclosed to persons or entities set out in section 10 of the <i>Secure Air Travel Act</i>. This disclosure is governed by a Memorandum of Understanding. Within Public Safety Canada, personal information may be disclosed to the Government Operations Centre, pursuant to subsection 9(1) of the <i>Secure Air Travel Act</i>. It may also be disclosed to the Passenger Protect Inquiries Office to facilitate the review of individuals who have been denied transportation, pursuant to a direction under subsection 9(1)(a) of the <i>Secure Air Travel Act</i>, and have applied for recourse. Personal information may be used for internal audit, evaluation, research and/or statistical purposes.

Retention and Disposal Standards:	Information on persons 18 years of age or older at the time of listing is retained for six years after their name is removed from the list, pursuant to subsection 8(3) of the <i>Secure Air Travel Act</i>. Information on persons less than 18 years of age at the time of listing is retained for six years after their name is removed from the list, pursuant to subsection 8(3) of the <i>Secure Air Travel Act</i>, plus the difference between their age at the time of listing and the date upon which they turn 18 years of age. Any other personal information collected in the administration of the Passenger Protect Program will be retained for two years.
RDA Number: • A timetable for the length of time records are maintained within the institution, (when the records are no longer required to meet operational, legal or other requirements) & when the RDA can be applied to the record holdings for final disposition) • Include the disposition action applied to the records when the retention period is reached, i.e. destroyed, alienated or transferred to Library and Archives Canada as a historical record.	2013/002
Related Record Number: • Records Disposition Authority number assigned by the Library and Archives Canada. • RDA enables government institutions to dispose of records which no longer have operational utility.	PS NCSB 05
TBS Registration: Personal Information Banks must be cross-referenced to institutional Classes of Records (which are also described in Info Source: Sources of Federal Government Information).	
Bank Number: A unique number assigned by TBS once the PIB has been reviewed and approved by TBS.	Under development
Unique number created by institution using: • institution's Federal Identity Program acronym <u>or</u> commonly used acronym; • Personal Information Bank Code (PPU - general public, etc.); • institutional assigned reference number	

Modèle pour l'élaboration de nouveaux Fichiers de renseignements personnels (FRP)

Nom de l'institution :	Sécurité publique Canada
Nom de la personne-ressource d'AIPRP :	Jennifer Schofield
Numéro de téléphone :	613-991-2929
Courriel :	Jennifer.schofield@canada.ca
Titre :	Programme de protection des passagers
- Doit être descriptif et refléter l'information décrite dans le FRP. - Il est utile d'avoir dans le titre une indication du programme auquel le FRP a trait.	
Description :	La banque de données contient l'information sur les personnes susceptibles d'être inscrites à la liste du Programme de protection des passagers. Cette information est recueillie par les personnes et les entités énumérées à l'article 10 de la <i>Loi sur la sûreté des déplacements aériens</i> en vertu de leurs mandats statutaire. Les renseignements personnels contenus dans cette base de données peuvent comprendre: le nom, les coordonnées (y compris la dernière adresse connue), les alias, le sexe, la date de naissance, les renseignements biographiques, la citoyenneté, le numéro de passeport, de visa ou de document de résidence, tout autre numéro d'identification ou document connu émis par un gouvernement, tous les renseignements financiers connus, la description des personnes (y compris les photographies), la description des activités ou des agissements connus ou soupçonnés de la personne, les faux documents présentés ou utilisés par une personne, les affiliations connues avec les organisations terroristes ou criminelles, le casier judiciaire connu et les détails sur les voyages, comme le nom de l'agence et de l'agent de voyages, les renseignements sur le billet d'avion et les détails de l'itinéraire, et tous autre renseignements précis qui peuvent être recueillis auprès des transporteurs aériens ou des exploitants d'un système de réservation, en vertu du paragraphe 6(2) de la <i>Loi sur la sûreté des déplacements aériens</i>, aux fins de vérification d'identité ou de l'émission d'une directive en vertu du paragraphe 9(1) de la <i>Loi sur la sûreté des déplacements aériens</i>. Les renseignements additionnels compilés par Sécurité publique Canada comprennent des documents tels que des rapports de renseignement, des évaluations des menaces et des risques, des notes d'information et d'autre correspondance obtenues de personnes et d'organismes énumérés à l'article 10 de la <i>Loi sur la sûreté des</i>
- Énoncé explicatif de l'information décrite dans le fichier. - Elle devrait indiquer les renseignements personnels particuliers contenus dans les documents auxquels le fichier a trait, c.-à-d. nom, adresse, numéro de téléphone, âge, sexe, état matrimonial, pays de naissance, citoyenneté, numéro d'assurance-sociale, numéro d'employé, race, empreintes digitales, type sanguin, etc.	

		déplacements aériens.
Nota :		
	C'est le seul champ optionnel. • Peut contenir de l'information sur la façon d'avoir accès à l'information décrite dans le FRP, c.-à-d. en précisant le nom de famille, le prénom et le numéro de téléphone. • Ne devrait pas contenir le nom de la personne-ressource à l'institution créant le FRP	
Catégorie de personnes :		Personnes susceptibles d'être inscrites à la liste du Programme de protection des passagers
	Identifie le groupe ou la catégorie de personnes au sujet desquelles l'information a trait, c.-à-d. employés actuels et anciens, entrepreneurs, postulants à des programmes, etc.	
But :		Les renseignements personnels décrits dans cette banque sont utilisés pour aider le ministre de la Sécurité publique et de la Protection civile, ou son délégué, à décider s'il doit inscrire une personne à la liste du Programme de protection des passagers, conformément au paragraphe 8(1) de la <i>Loi sur la sûreté des déplacements aériens</i>, et à émettre une directive à un transporteur aérien, en application du paragraphe 9(1) de la <i>Loi sur la sûreté des déplacements aériens</i>. Le pouvoir de recueillir des renseignements personnels est accordé conformément à l'article 10 de la <i>Loi sur la sûreté des déplacements aériens</i>.
Usages compatibles :		Les renseignements personnels peuvent être divulgués aux personnes ou entités énumérés à l'article 10 de la <i>Loi sur la sûreté des déplacements aériens</i>. Cette divulgation est régie par un protocole d'entente. Au sein de Sécurité publique Canada, les renseignements personnels peuvent être divulgués au Centre des opérations du gouvernement, conformément au paragraphe 9(1) de la <i>Loi sur la sûreté des déplacements aériens</i>. Ils peuvent aussi être divulgués au Bureau des demandes de renseignements sur le Programme de protection des passagers pour faciliter l'examen des personnes qui ont été refusé le transport, conformément à une directive émise en application du paragraphe 9(1)(a) de la <i>Loi sur la sûreté des déplacements aériens</i>, et qui ont demandés un recours. L'information personnelle peut être utilisée aux fins de vérification interne, d'évaluation, de recherche ou de statistiques.
	• Énumère les usages potentiels ou connexes pour lesquels les renseignements personnels peuvent être utilisés ou divulgués. • Les usages doivent être conformes au but original pour lequel l'information a été recueillie – et pourraient raisonnablement être considérés connexes. • Doit avoir un lien raisonnable et direct au ou aux buts originaux • Énoncer tous les usages de l'information. Les activités de jumelage des données et les formes de divulgation doivent être énumérées sous cette rubrique. • S'il n'y a aucun usage compatible, prière d'ajouter un	

énoncé en ce sens. Note sur la divulgation : Il existe des circonstances en vertu desquelles les renseignements personnels peuvent être divulgués à un tiers. Le cas échéant, précisez le tiers en question.	
Normes de conservation et de destruction :	Lorsque le nom d'une personne inscrite à l'âge de 18 ans ou plus est enlevé de la liste, conformément au paragraphe 8(3) de la <i>Loi sur la sûreté des déplacements aériens</i>, les renseignements à son égard sont conservés pendant six ans. Lorsque le nom d'une personne inscrite à l'âge de moins de 18 ans est enlevé de la liste, conformément au paragraphe 8(3) de la <i>Loi sur la sûreté des déplacements aériens</i>, les renseignements à son égard sont conservés pendant six ans, plus le montant de temps entre le moment de l'ajout à la liste et le moment où elle aura 18 ans. Tout autre renseignement recueilli dans le cadre du Programme de protection des passagers sera conservé pendant deux ans.
• Calendrier indiquant la durée pendant laquelle les documents sont conservés par l'institution (quand les documents ne sont plus requis pour répondre aux exigences opérationnelles, légales ou autres et quand l'ADD peut être appliquée aux documents pour disposition finale) • Inclus la mesure de disposition appliquée aux documents à l'expiration de la période de conservation, c.-à-d. destruction, aliénation ou transfert aux Bibliothèque et Archives Canada (BAC) comme document historique.	
No. ADD :	2013/002
• Numéro d'autorisation de disposition de documents attribué par les Bibliothèque et Archives Canada (BAC). • L'ADD permet aux institutions gouvernementales de se défaire des documents qui n'ont plus d'utilité opérationnelle.	
Renvoi au dossier :	PS NCSB 05
Il faut établir des renvois entre les fichiers de renseignements personnels et les documents des programmes institutionnels (qui sont également décrits dans Info Source : Sources de renseignements fédéraux).	
Enregistrement (SCT) :	
Numéro unique attribué par le SCT une fois qu'il a examiné et approuvé le FRP.	

Numéro du fichier :		En cours d'élaboration
	Numéro unique créé par l'institution au moyen : • de l'acronyme du PCIM pour l'institution <u>ou</u> de l'acronyme utilisé couramment; • renseignements personnels (PPU – grand public, etc.); • du numéro de référence attribué par l'institution	

Classes of Records Template

Title:		Passenger Protect Program
Mandatory Must reflect the records being described.		
Description:		Includes records related to the Passenger Protect Program, which identifies individuals whom the Minister of Public Safety and Emergency Preparedness has reasonable grounds to suspect will engage or attempt to engage in an act that would threaten transportation security, or travel by air for the purpose of committing certain terrorism offences, as defined in the <i>Criminal Code</i> , as well as any directions issued by the Minister of Public Safety and Emergency Preparedness. Records include personal information related to persons considered for listing under the Passenger Protect Program, policy advice to senior decision makers and meeting documents.
Mandatory Identifies the records created, collected and maintained by the institution as evidence of and information about a particular institutional program or activity. Must provide sufficient information for the general public to understand the program/activity to which the records relate.		
Note:		
Optional Describes relevant information that is not captured by other fields; for example, former name of a program or date a program ceased.		
Document Types:		Memoranda, records of decision, threat and risk assessments, case briefs and other program-related information and correspondence
Mandatory Identifies specific document types. For example: contracts, statements of work, proposals, evaluation criteria, memoranda, procedures, policies, etc.		
Format:		

Optional Specifies <u>non-standard record format</u> . This field should be used <u>only</u> for non-standard record formats; e.g. audio tapes, video tapes, photographs, specific types of database software. <u>Note</u> : Do not list electronic or paper formats.	
Record Number:	PS NCSB 05
Mandatory Unique number created by institution using: • the institution's Federal Identity Program acronym <u>or</u> commonly used acronym • unique file/identification number used within the institution to identify the records.	

Modèle - Catégories de documents

Titre :		Programme de protection des passagers
Obligatoire	Doit correspondre aux documents qui sont décrits.	
Description :		Cela concerne également les documents relatifs au Programme de protection des passagers, qui identifie les personnes au sujet desquelles le ministre de la Sécurité publique et de la Protection civile a des motifs raisonnables de soupçonner qu'elle participera ou tentera de participer à un acte qui menacerait la sûreté des transports ou qu'elle se déplacera en aéronef dans le but de commettre certains actes terroristes, comme le définit le <i>Code criminel</i> , ainsi que toute directive diffusée par le ministre de la Sécurité publique et de la Protection civile. Les renseignements personnels des personnes susceptibles d'être inscrites à la liste du Programme de protection des passagers, les conseils stratégiques prodigués aux principaux décideurs et les documents des réunions font également partie de cette catégorie de documents.
Obligatoire	Identifier les documents créés, recueillis et conservés par l'institution comme éléments de preuve et des informations au sujet d'un programme ou activité spécifique à l'institution. Doit fournir suffisamment de détails pour permettre au lecteur moyen de comprendre le programme ou l'activité auquel le document se rapporte.	
Nota :		
Champ facultatif	Décrit les renseignements pertinents qui ne sont pas inscrits dans d'autres champs – par exemple, l'ancien nom d'un programme ou la date de la fin d'un programme.	
Types de documents :		Notes de service, comptes rendus des décisions, évaluations des menaces et des risques, mémoires et autres informations et correspondances relatives au Programme
Obligatoire	Précise les types de documents. par exemple : contrats, énoncé de travail, propositions, critères d'évaluation, notes de service, procédés, politiques, etc.	

Format :	
Champ facultatif Précise le support du dossier non standards. Ce champ devrait servir <u>seulement</u> pour des modes non standards; par exemple, bandes sonores, vidéocassettes, photographies, logiciels de base de données particuliers. <u>Nota :</u> Ne pas inclure les documents en format électronique et les documents sur papier.	
Numéro du document :	
Obligatoire Numéro exclusif attribué par l'institution et composé des éléments suivants : • acronyme du Programme de coordination de l'image de l'institution ou l'acronyme généralement utilisé; • numéro du dossier ou d'identification exclusif utilisé pour repérer le dossier dans le système officiel de gestion des dossiers.	PS NCSB 05

**Pages 42 to / à 43
are not relevant
sont non pertinentes**

CORE PRIVACY IMPACT ASSESSMENT FOR:

Governor in Council Appointments

Public Safety Canada PACB/CPES

CORE PRIVACY IMPACT ASSESSMENT

SECTION I - OVERVIEW & PIA INITIATION

Government Institution: Public Safety Canada (PS)

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the <i>Privacy Act</i>
Jean Cintrat, Director General, Cabinet and Parliamentary Affairs and Executive Services (CPES)	Jill Wherrett, A/ADM, Portfolio Affairs and Communications Branch (PACB)

Name of Program or Activity of the Government Institution: Governor in Council Appointments

Description of Program or Activity :

Processing of applications for Governor in Council (GIC) Appointments. This forms part of the internal Services of Public Safety as described in the PAA.

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:

Description: Includes records related to the establishment, organization, functions, activities and management of boards, committees, offices and commissions which are exclusive to a particular institution and which have been established to provide oversight, guidance and recommendations to the institution. Records may include information related to the nomination, appointment, resignation and/or termination of members including criteria for the identification and selection of members, terms and conditions of appointment (e.g. salary, honoraria, per diem rates) roles and responsibilities, and administrative support documentation. Records may also include correspondence among members and with the institution, as well as the relevant Minister's Office about the selection of individuals and with the Privy Council Office about GIC appointments.

Document Types: Terms of reference, agendas, minutes of meetings, notices, proceedings, recommendations documents, briefing and discussion papers, curricula vitae, travel claims, policy documents, photographs, videos, communications materials released in all formats (including institutional web sites), speeches, audit and evaluation documentation, copies of Annual Reports, Orders-in-Council, correspondence, backgrounders, reports, etc.

Record Number: PRN 938

Class of Record Number: Standard CoR PRN 938

- ☐ Proposal for a New Personal Information Bank
- ☐ Proposal to modify an existing personal information bank - identify PIB registration number and current description:

- ☐ Proposed new Standard Personal Information Bank
- ☐ Proposal to Modify an Existing Personal Information Bank - identify Standard PIB number and current description:

Legal Authority for Program or Activity:

The authority for GIC appointments is provided by statutes which generally specify the appointment authority, the length of term of the appointment and the qualifications required.

The GIC appointment process is within the mandate of the Privy Council Office (PCO) as the department of the Prime Minister from who PCO's authority derives. Order in Council 1935-3375 Prerogative of the Prime Minister provides the clerks functions.

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

Summary of the project / initiative / change:

The Department plays a central role in providing operational support and guidance to the Minister's office for all GIC appointments in the Public Safety Portfolio. Departmental key responsibilities/activities to support the Minister and the GIC appointment process include:

- Managing and coordinating open, transparent and merit-based selection processes for GIC positions (providing a single window for all GIC portfolio appointments);
- Developing notices of opportunity, selection criteria, interview questions, letters of notification and reference material (e.g. guidelines, action plans, presentations, briefing notes, etc.);
- Providing recommendations to the Minister; and
- Tracking and reporting on the status of current and upcoming vacancies across the portfolio.

Note: Short description of the institutions business objectives, project objectives, project / initiative / change scope, product scope, stakeholders and assumptions.

SECTION II RISK AREA IDENTIFICATION & CATEGORIZATION

Type of Program or Activity	Level of Risk to Privacy
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

Type of Personal Information Involved and Context	Level of risk to privacy
1.1 Only personal information provided by the individual – at the time of collection – relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities. 1.2 The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.	☐ 1
Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.	☐ 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 1.3 For example: the personal information by association indirectly reveals information on the health, financial situation, religious or lifestyle choices 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. 1.4 For example: the personal information by association indirectly reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and other individuals, such as relatives.	☐ 4

Program or Activity Partners and Private Sector Involvement	Level of risk to privacy
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

Duration of the Program or Activity	Level of risk to privacy
1.5 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
1.6 Short-term program	☐ 2

A program or an activity that supports a short-term goal with an established "sunset" date.	
1.7 Long-term program Existing program that has been modified or is established with no clear "sunset".	☒ 3

Program Population	Level of risk to privacy
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

Technology & Privacy	Risk to privacy
Does the new or modified program or activity involve the implementation of <u>a new electronic system</u> , 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
Does the new or modified program or activity require any modifications to <u>IT legacy systems and / or services</u> ?	☐ YES ☒ NO
The new or modified program or activity involve the implementation of one or more of the following technologies:	
- 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). Identify the applicable category(ies): 	☐ YES ☒ NO
- 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... Identify the applicable category(ies): 	☐ YES ☒ NO
- Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the Directive on PIA, government institution 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 behavior. Identify the applicable category(ies):	☐ YES ☒ NO

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.

Personal Information Transmission

Level of risk to privacy

- The personal information is used within a closed system. ☐ 1
 No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.
- 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. ☒ 3
 USB key, diskette, laptop computer, any transfer of the personal information to a different medium.
- The personal information is transmitted using wireless technologies. ☐ 4

Risk Impact to the Institution

Level of risk to privacy

- Managerial harm. ☐ 1
 Processes must be reviewed, tools must be changed, change in provider / partner.
- Organizational harm. ☐ 2
 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.
- Financial harm. ☐ 3
 Lawsuit, additional moneys required, reallocation of financial resources.
- Reputation harm, embarrassment, loss of credibility. ☒ 4
 Decrease confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Risk Impact to the Individual or Employee

Level of risk to privacy

- Inconvenience. ☐ 1
- Reputation harm, embarrassment. ☐ 2
- Financial harm. ☒ 3
- Physical harm. ☐ 4

SECTION III - 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 is identified as a potential privacy risk (level 2-3-4) in the Risk Area Identification and Categorization.

Define each element of personal information collected	Define sub-elements of personal information associated with the element identified in the first column	How is the personal information recorded?
GIC Application Cover Letter CV	Name Home address Telephone number Email address First official language Preferred language Title Proficiency in other official language Work and secondary telephone numbers Self-identification as a member of an employment equity group Employment history outside of government Education Possible volunteer history Expression of interest in particular appointment(s)	☒ Paper ☒ Electronic ☐ Audio Recordings ☐ Visual Image Recordings ☐ Human Biological Samples ☐ Other (Specify)
Assessment materials	Answers to written exam questions Answers to interview questions Evaluations of these answers Assessor's comments re: individual Conflict of Interest declarations Reference checks	☒ Paper ☒ Electronic ☐ Audio Recordings ☐ Visual Image Recordings ☐ Human Biological Samples ☐ Other (Specify)
Recommendations to Minister	Assessment of candidate's qualifications, assessment results, and overall eligibility and suitability for position.	☒ Paper ☒ Electronic ☐ Audio Recordings ☐ Visual Image Recordings ☐ Human Biological Samples ☐ Other (Specify)

SECTION IV - 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.

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	Applicants apply through the online GIC application, managed by PCO
A federal government institution (identify from what PIB the information is obtained)	PCO sends the application to the Director General, Cabinet and Parliamentary Affairs and Executive Services. The Director General will share with the Policy Advisor, Regulatory Affairs who will coordinate the selection process. Once assessed, personal information may be forwarded back to the Director General, Cabinet and Parliamentary Affairs and Executive Services from the portfolio agency/review body involved in assessment (i.e. the Parole Board of Canada (PBC) for board members). PS Portfolio organizations to which this process applies are the PBC, the Office of the Correctional Investigator (OCI), the Civilian Review and Complaints Commission for the RCMP (CRCC) and the RCMP External Review Committee (ERC).

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
GIC appointments, Cabinet, Parliamentary and Executive Services; Policy Advisor, Regulatory Affairs	Standard
ADM, Community Safety and Countering Crime Branch (CSCCB)	Standard
DMO (includes Associate DM)	Standard
MO	Standard

External Use and Disclosure

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

The individual	The individual will be advised of the decision concerning their appointment by PCO, or by the PBC in the case of membership positions at the PBC.
A federal government institution	PCO will be advised of the recommendation of the Minister. Personal information will be disclosed to members of the selection committee and supporting staff. Members of the selection committee are from the Department and, depending on the position, from the PBC, the CRCC or the ERC.

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	Public Safety: Personal information will be held in a Secret Cabinet that only the Policy Advisor, Regulatory Affairs; and the Director General of Cabinet and Parliamentary Affairs and Executive Services and his Executive Assistant will have access to. Electronic copies will be retained in RDIMS, with access limited to the above-noted individuals, as well as members of the selection committee if they are also PS employees. These files will have a standard naming convention of (PS-CCM# (if applicable) – Title (Subject, i.e. GICs) – Document type). Portfolio Agencies/Review Bodies: Under review – To be confirmed in 2017.
Records Office	Under review by IM – To be confirmed in 2017.

(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 transborder or transjurisdictional issues. Where 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:		
Identify Groups or Areas / or Divisions	Where appropriate - positions who have access or use the personal information	Geographical Location
<u>PACB – DG, CPES</u>	1 – DG + Executive Assistant + Policy Advisor, Regulatory Affairs	National Capital Region
<u>CSCCB – ADMO</u>	5 – ADM + staff	National Capital Region
<u>DMO</u>	DM+AsDM+staff	National Capital Region
<u>Minister's Office</u>	Minister+staff	National Capital Region
<u>CMB Records</u>	Records staff	National Capital Region
Other federal government Institution responsible for program or activity:		
PCO	ITSD, Personnel Secretariat ITSD, Site Management (as per PCO PIA)	National Capital Region

SECTION V - PRIVACY COMPLIANCE ANALYSIS

Collection Authority (Section 4 of the *Privacy Act*)

1. Has each element and sub-elements of personal information collected or to be collected been justified in terms of its necessity to the administration of the program or activity? <u>Note:</u> "Necessary" is a higher standard than merely being useful.	☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Review the proposed personal information elements and sub-elements outlined in the Personal information Analysis section to determine which pieces are "necessary" and not merely useful. Document any changes. Legal Requirement: s. 4 <i>Privacy Act</i> Policy requirement Limit the collection of personal information to what is demonstrably necessary for the program or activity. Institutions must abide by any applicable statutory prohibitions.
2. Is the Social insurance Number (SIN) being collected?	☐ YES ☒ NO	If YES Please state the legal and policy authority: Action Required to Support Legal & Policy Compliance in the absence of legal and policy authority to collect the SIN: ☐ Establish explicit legislative authority through legislative amendments. ☐ Establish legal and policy authority as outlined in the <i>Directive on SIN</i>. <u>Note:</u> Uses related to the <i>Income Tax Act</i> only apply to the administration of that Act. This authority does not extend to general program purposes that are not for income tax purposes.

Direct Collection – Informed of Purpose (Section 5 of the *Privacy Act*)

3. Is the information collected directly from the individual?	☐ YES ☒ NO	If NO ☒ Ensure that the requirements stated at Question 5 are met. Policy requirement: A detailed "Privacy Notice" is required where personal information is collected for an administrative purpose. Legal Consideration: Section 10 of the <i>Privacy Regulations</i> provides for the rights or actions under the act to be exercised or
--	--	--

		performed on behalf of a minor, an incompetent person, a deceased person or a person authorized by law to administer the affairs of that person.
4. Is the information collected from another source with informed consent of the individual?	☒ YES ☐ NO	If NO — or if YES and NO ☒ Ensure that the requirements stated at Question 3 are met. Policy requirement: Inform the individual of what information will be collected, how the information will be used and what source will be asked to provide the information. Individuals should also be informed of any alternatives or consequences that may result from their refusal to authorize any indirect collection. Written authorization from the individual to whom the personal information pertains is required. Collection of personal information from another source may be required in order to ensure that the personal information is accurate and up-to-date. See Question 8 regarding accuracy requirements.
5. Is the information collected from another source without notice to or consent from the individual? - Is the collection a result of a disclosure under subsection 8(2) of the Act? - Would direct notification of the individual result in the collection of inaccurate information? - Would direct notification of the individual defeat the purpose or prejudice the use for which the information is collected? - Is the information used for a non-administrative decision about the individual?	☒ YES ☐ NO ☐ YES ☒ NO ☐ YES ☒ NO ☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that the personal information bank's description adequately reflects the nature of such activities. If NO Action Required to Support Legal & Policy Compliance: ☐ Direct collection must be adopted and the individual must be notified of the purpose of the collection. ☐ Ensure that the requirements stated at Question 3 are met. Policy principle The exception to direct collection should be used sparingly. It is primarily intended for use by investigative bodies in those circumstances where direct collection would jeopardize the investigation.
6. Will the personal information collected only be used for: • The purpose for which it was collected or a purpose consistent with that purpose? • A purpose consistent with section 8(2) of the Act?	☒ YES ☐ NO ☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Identify all secondary purposes in the PIB description (i.e. other uses within the department or by another federal/provincial institution that has authority to collect the information). ☐ Integrate in the 'Privacy Notice', as appropriate, a listing for uses and disclosures

	that are not directly related to the purpose of the collection or consistent with that purpose. ☐ Ensure that the requirements stated at Questions 4 or 5 are met. Policy requirement Inform the individual at the time of collection of any intended uses or disclosures that are not directly related to the program or activity for which the information is being collected. (This would be considered an indirect collection by other programs.) Policy Requirement Ensuring that individuals are notified in advance of follow-up activities including all means of communication to be expected by the government institution. The individuals will be in a position to recognize legitimate requests for personal information. This will help minimize the risk of individuals providing their personal information under a false pretext.
--	---

Retention (Section 6 of the <i>Privacy Act</i>)		
7. Is the personal information being used to make a decision or as part of a process to make a decision that directly affects an identifiable individual? This includes use for verification/authentication purposes.	☒ YES ☐ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Prepare and obtain approval for a retention schedule based on your legal requirements and operational needs; AND ☐ Retain records for a minimum of 2 years as required by the <i>Privacy Regulations</i>; OR ☐ Obtain consent of the individual to dispose of the personal information earlier than the minimum 2 year retention period; AND ☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. ☒ Retain and dispose of transitory information in accordance to the retention period that will be established. If NO Action Required to Support Legal & Policy Compliance: ☐ Ensure that the policy requirements for Non-Administrative Privacy Protocol, outlined in the <i>Policy on Privacy Protection</i> are followed. ☐ Prepare and obtain approval for a retention schedule based on your legal requirements and operational needs.

	☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. <u>Policy requirement</u> Retain personal information for a minimum of two years, as detailed in section 4 of the <i>Privacy Regulations</i> . In accordance with the <i>Library and Archives of Canada Act</i> , only the Librarian and Archivist of Canada may authorize the disposition of government records by issuing Records Disposition Authorities (RDA).
--	---

Accuracy – (Section 6 (2) of the *Privacy Act*)

8. What measures will be taken to ensure that the personal information used in administrative decisions is accurate, up-to-date and complete? (More than one option may apply) - Direct collection or validation with the individual. - Technological means to identify keystroke errors and discrepancies. - Personal information matching program to verify personal information integrity against a "reliable source" where authorized or where consent was obtained. - In cases where direct collection or consent is not feasible, obtain information from trusted sources (either public or private) and verify accuracy against existing personal information before use. If Other – please define below:	☒ YES ☐ YES ☐ YES ☐ YES ☐ YES	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that, if applicable, your institution's PIB mentions the use of periodic personal information matching as a consistent use. If NO Please provide details as to why reasonable steps cannot be used. <u>Legal and Policy Requirements</u> Subsection 6(2) of the <i>Privacy Act</i> requires government institutions to take <i>all reasonable steps</i> to ensure that personal information that they use for an administrative purpose is as accurate, up-to-date and complete as possible. Decisions that directly affect individuals must be made on the basis of accurate, up-to-date and complete information as possible. If periodic personal information matching occurs for the purposes of ensuring accuracy of information, institutions must reflect this under the "consistent use" section of the relevant PIB.
---	---	---

Use (Section 7 of the *Privacy Act*)

9. Is there an activity log attached to the personal information record to record uses not described in the Personal Information Bank (Info Source)?	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ An activity log is attached to personal information records when used for consistent
--	--	---

	but unreported use. ☐ The Privacy Commissioner is advised of this consistent use. ☐ The PIB description is amended, in time for the next edition of Info Source, to include the unreported use. If NO Action Required to Support Legal & Policy Compliance: ☒ Institutions must put in place a means to record and identify uses that were not described in the Personal Information Bank. The Director General and Policy Advisor, Regulatory Affairs have been advised of the requirement and will inform the ATIP Coordinator immediately should be information be used for any other purpose. Legal Requirements: Section 9(4) of the <i>Privacy Act</i> requires a government institution to report to the Privacy Commissioner any consistent use of personal information that has not been included in the Index, and to ensure that the use is included in the next statement of consistent uses set forth in the next edition of the Index. Policy Requirement If personal information used for a consistent purpose that is not identified in a personal information bank – the head of the institution or delegate must notify the Privacy Commissioner
Disclosure (Section 8 of the <i>Privacy Act</i>)	
10. Are processes in place to ensure that personal information will only be disclosed to individuals within and without the government institution who have a "need to know" and that there are adequate privacy practices to ensure the confidentiality and integrity of the personal information? This includes procedures to prevent against loss or theft. This covers the entire lifecycle of the personal information: • Collection • Use • Retention	☒ YES ☐ NO If NO Action Required to Support Legal & Policy Compliance: ☐ Ensure that the requirements stated at Question 11 are met by the receiving institution. Policy requirement Government institutions are to ensure that adequate safeguards are in place when disclosing information This includes having an action plan for privacy breaches (unauthorized disclosures) and measures (physical, logical, administrative) to ensure that only the people that "need to know" have access to the personal information. See Directive on Privacy Practices

• Disposition. This includes disclosures to other government institutions, other levels of government, other jurisdictions, foreign governments, international organizations or private sector organizations		
11. Is the disclosure of the personal information governed by: A Memorandum of understanding? An accord? An arrangement? A contract? If Other – please define below:	☐ YES ☐ YES ☐ YES ☐ YES	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure the PIB description identifies this use. ☐ Ensure that the notification or consent notice mentions this use. ☐ Ensure contractual clauses are included to protect personal information. Contracts that are established with private sector entities outline measures and provisions to address the following: ☐ Control over the personal information; ☐ Limitations on collection and handling as well as any prohibitions regarding the personal information for the purposes of the contract; ☐ Disposition of the personal information, where relevant; ☐ Administrative, technical and physical safeguards; and ☐ Obligations of other parties acting on behalf of the government institution. If NO Action Required to Support Legal & Policy Compliance: ☒ Prepare a written statement describing the nature of the information sharing and have it approved by the relevant parties. Policy on Privacy Protection Measures are to be established, when personal information is involved, to ensure that the government institution meets the requirements of the <u>Privacy Act</u> when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations.

		Ensure that appropriate privacy protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information. If any portion of the project (administration, service delivery, system maintenance or personal information storage) involves the use of a third-party contractor, care must be taken to ensure that institutions continue to fulfill their privacy obligations.
Technology and Privacy		
12. Will the system/software /program application employ cookies or other tracking methods to collect personal information about users and their transactions? If so, for what purposes will the collected information be used and how long will the information be retained? Please define purpose and retention period below:	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Collection and use of personal information through these means must be reflected both in the PIB description and the Privacy Notice. ☐ Technology staff who have access to personal information collected through these methods must be aware of privacy and security policy requirements.
13. Does the new or modified program or activity result in an increased ability for surveillance or monitoring of a given target population?	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that the requirements in regards to awareness stated at Question 12 are met.

Privacy Considerations Related to Compliance / Regulatory Investigation and Enforcement		
14. Is the legal authority for conducting compliance / regulatory investigation and enforcement the same as the legislative authority for the program or activity?	☐ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: Identify legislative authority: ☐ Ensure that the requirements stated at Questions 3 and 6 are met. ☐ Ensure the activities are listed in the PIB's description. If YES Action Required to Support Legal & Policy Compliance: ☐ The activities are listed in the Privacy Notice; ☐ The activities are listed in the PIB's

	description.
--	--------------

Privacy Considerations Related to Search and Seizure

15. What is the specific legal authority for conducting regulatory or criminal enforcement, surveillance or intelligence gathering?

--

Action Required to Support Legal & Policy Compliance:

☐ Request legal advice from your Legal Services Unit about compliance with section 8 of the *Charter of Rights and Freedoms*, the *Privacy Act* and other applicable acts

SECTION VI - Summary of Analysis and Recommendations (as applicable) Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified

RISK: Each Agency is responsible for the access, storage and retention of the personal information sent to them.

MITIGATION: Each Agency is required to comply with the Policy on Government Security and the Privacy Act. It is up to them to monitor. When information is sent, it will include the following caveat "Personal information is being provided in accordance with paragraph 8(2)(a) of the Privacy Act. It is up to the receiving institution to ensure that access is limited to a need to know basis, and that the information is stored in a manner that is appropriate for its classification in accordance with the Policy on Government Security".

RISK: Disclosure of personal information by an Agency is not governed by a written agreement/MOU/contract/Information sharing agreement.

MITIGATION: See above.

RISK: Public Safety Canada is currently reviewing retention period for all records in the department; therefore, no specific retention period is set for GIC appointment information.

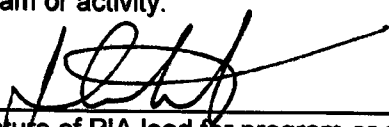
MITIGATION: Until a retention period is set, recommendations to the Minister with attachments will be retained for a year after the appointment has ended. At that time, records will be destroyed.

SECTION VII - SUPPLEMENTARY DOCUMENTS LIST

N/A

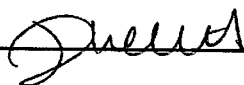
SECTION VIII – FORMAL APPROVAL

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 core PIA as they relate to the administration of the identified program or activity.

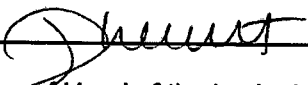

Signature of PIA lead for program or activity
(DG or senior official with functional authority for program)

APR 18 2017

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.


Signature of Head of the institution or the delegate responsible for Section 10 under the Privacy Act (ADM or other delegated authority)

APR 21 2017

Date

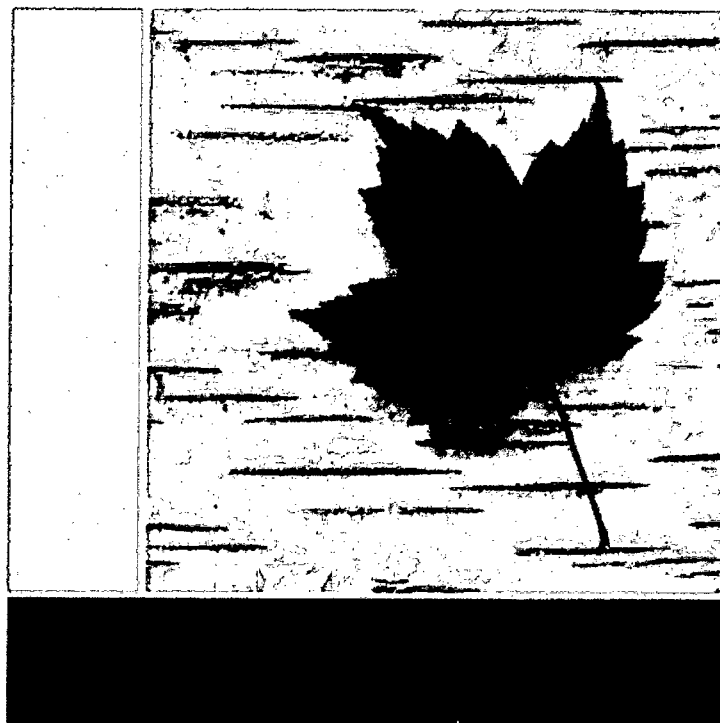
Note: Under the Privacy Act, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks



Public Safety
Canada

Sécurité publique
Canada

BUILDING A **SAFE AND RESILIENT CANADA**



Government Operations Centre

Privacy Impact Assessment

March 2015

000063

Document Version

Version	Date	Change Made By	Change
1	Dec 2011	Sheila Gordon	
2	Feb 2012	Sheila Gordon	Initial comments from Jennifer Schofield and input from PS Legal II
3	June 2012	Sheila Gordon	Comments from Richard Sarabura included
4	July 2012	Sheila Gordon	Comments from Jennifer Schofield included
5	Sept 2012	Sheila Gordon	Updated graphic and text edits.
6	Nov2012	Sheila Gordon	Updated with comments from PS legal
7	Jan 2013	Sheila Gordon	Final edits including MOU mitigation strategy. Added final comments from PS legal.
8	April 2013	Sheila Gordon	Added final comments from PS ATIP
9	December 2014	Elena Humeniuk/ Chris Currie	Update based on the recommendations from the Privacy Commission (Update based the Privacy Commission request)
10	March 2015	Elena Humeniuk/Michelle Dunn	Update based on consultation with the Policy, Privacy and Training Unit, ATIP Division

Table of Contents

<i>SECTION I – Overview and PIA Initiation</i>	5
Government Institution: Public Safety Canada	5
Name of Program or Activity of the Government Institution:	5
Description of Program or Activity:	5
Description of the class of records associated with the program or activity:	6
Legal Authority for Program or Activity:	7
Summary of the project / initiative / change:	8
 <i>SECTION II – Risk Area Identification & Categorization</i>	 9
 <i>SECTION III – Analysis of Personal Information Elements</i>	 13
Personal Information Elements and Sub-elements	13
 <i>SECTION IV – Flow of Personal Information</i>	 14
Source of the personal information for the program or activity:	15
Internal use and disclosure	16
External Use and Disclosure	16
Retention / Storage	17
Access to Information	18
 <i>SECTION V – Privacy Compliance Analysis</i>	 19
Collection Authority	19
Direct Collection – Informed of Purpose	19
Retention	22
Accuracy	23
Use	24
Disclosure	25
Technology and Privacy	27
Privacy Considerations Related to Compliance Regulatory Investigation & Enforcement	28
Privacy Considerations Related to Search and Seizure	28

<i>SECTION VI - Summary of Analysis and Risk Mitigation</i>	30
Risks and Mitigation	30
Policy on disposing of personal information:	32
 <i>SECTION VII – Supplementary Documents List</i>	 33
Federal Departments and Agencies - Dissemination Levels	33
 <i>SECTION VIII – Formal Approval</i>	 34
 <i>Appendix A - List of Acronyms</i>	 35
 <i>Appendix B – Public Safety Canada’s Personal Information Caveat</i>	 38

SECTION I – Overview and PIA Initiation

Government Institution: Public Safety Canada

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the <i>Privacy Act</i>
Director General, Government Operations Centre	Assistant Deputy Minister, Emergency Management and Programs Branch

Name of Program or Activity of the Government Institution:

Government Operations Centre – Collection of Personal Information

Description of Program or Activity:

1.4 Emergency Management

Without an all-hazards emergency management program, Canadians would be more vulnerable to a range of threats and disasters, and federal/provincial/territorial (FPT) governments would be unable to plan for and respond to, emergencies in a coordinated and systemic manner. Public Safety Canada (PS) works to protect Canada and Canadians by providing national leadership and setting a clear direction for emergency management and critical infrastructure protection for the Government of Canada, as provided for in the *Emergency Management Act* of 2007. This is achieved through emergency management policy and planning, provision of training and exercises, and research activities that support a unified emergency management system. The Department develops and maintains the federal government's capacity to manage emergencies; monitors and coordinates the federal response; and provides support to provinces and territories when federal assistance is needed. The Department also promotes public awareness of emergency management directly to Canadian citizens and businesses. Working closely with international counterparts, federal departments, provinces, territories, the first responder community and industry, to address all hazards (natural, technological and human induced), this program activity aims to foster a safe and resilient Canada through policy and program coordination across the four pillars of emergency management: prevention/mitigation, preparedness, response and recovery.

1.4.2 Emergency Response and Recovery

When provincial and territorial government resources are insufficient to respond to and/or recover from a large-scale natural or human-induced disaster, PS coordinates the federal response to the provincial or territorial government requesting assistance and may also provide financial assistance. Our network of Regional Offices across Canada serve as the Department's primary link to provincial and territorial emergency management counterparts, as well as federal departments in the region to enable a whole-of-government response. An integrated federal response to events of national significance is supported through 24/7 watch and early

warning, national-level situational awareness, integrated risk assessment, response planning, whole-of-government response management and support to senior officials' decision making. These services are provided to the Government of Canada and response organizations at the federal, provincial and territorial levels.

1.4.2.1 All- Hazards Emergency Management Coordination-

This program enables the delivery of an integrated federal emergency response to potential or actual disasters (natural or human-induced) that may threaten the safety and security of Canadians or the integrity of Canada's critical infrastructure. The program is delivered through the Government Operations Centre (GOC), a facility that coordinates a strategic-level response on behalf of the Government of Canada, in response to potential and occurring events that may affect the national interest. This program provides 24/7 watch and early warning for Government in support of partner mandates. The GOC provides national-level situational awareness (e.g. Notifications, Situation Reports, information products, and briefings) to partners, senior decision makers, senior officials, provincial governments and/or the private sector. The GOC enables a whole-of-government response capability, plans for and coordinates the federal response to incidents, develops recommendations for the deployment and utilization of federal resources and actions requests for emergency assistance from federal or provincial authorities. Working with the provinces and territories and international partners, the GOC is a key asset for DM and ADM communities, providing them with a mechanism for the implementation of their direction, keeping senior officials informed of evolving events, as well as identifying issues that need their engagement for resolution. The GOC improves the efficient use of Government of Canada strategic assets, and when offered, the resources of P/T governments. This program also aligns the work of regional offices with national efforts in order to support provincial and territorial partners in addressing emergencies.

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:

Emergency Management Operations

Description: Information on Government of Canada operational emergency response capabilities and programs including information pertaining to the Federal Emergency Response Plan, the National Emergency Response System, the Government Operations Centre (GOC) and the Canadian Cyber Incident Response Centre (CCIRC). Under this program, the GOC delivers an all-hazard integrated federal emergency response to events in the national interest. It provides 24/7 monitoring and reporting, national-level situational awareness, integrated risk assessments and warning products, as well as national-level planning and whole-of-government response management. In parallel and in collaboration with the GOC, CCIRC focuses on operational-level, cyber-only whole-of-government response.

Document Types: Memorandums, briefing notes and books, Question Period notes, reports, plans, presentations, evaluations, agreements, procedures, policies, maps, emails, lists, agendas, records of decision, letters, contracts and requests for proposals.

Class of Record Number: PS EMNS 050

- ☐ Proposal for a New Personal Information Bank
☐ Proposal to modify an existing personal information bank - PIB registration number and current description:

- ☒ New Class of Personal Information
☐ Proposed new Standard Personal Information Bank
☐ Proposal to Modify an Existing Personal Information Bank - Standard PIB number and current description:

NOTE: A new Class of Personal Information for **Departmental Subject Files** is currently being developed. The class will address personal information that is not used for administrative purposes or retrievable by personal identifiers. Any personal information potentially collected by the GOC will be covered under this new Class of Personal Information. Once finalized, we anticipate the Class of Personal Information to be available online in the new fiscal year once.

Legal Authority for Program or Activity:

The Government Operations Centre's (GOC) legal authority is based on the:

- (1) *Department of Public Safety and Emergency Preparedness Act (DPSEPA)*;
(2) *Emergency Management Act (EMA)*;

Section 4 and 6 of the DPSEPA gives the Minister of Public Safety and Emergency Preparedness broad powers, duties and functions relating to public safety and emergency preparedness.

In addition, sections 3, 4 and 5 of the EMA set out the responsibilities of the Minister in relation to emergency management. These responsibilities, among others, include (1) monitoring potential, imminent or actual emergencies and advising ministers accordingly; (2) establishing policies and programs related to emergency management; (3) facilitating the authorized sharing of information in order to enhance emergency management; (4) coordinating the Government of Canada's response to an emergency; and (5) participating in international emergency management activities including developing joint plans with the United States.

In applying these authorities the GOC, in some limited instances, receives personal information from partner agencies during the course of performing its mandated functions.

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

Summary of the project / initiative / change:

Under the authority of the EMA, a principal means by which the Minister of Public Safety exercises leadership for federal emergency management is through the activities of the Government Operations Centre (GOC). On behalf of the Government of Canada, the GOC allows Canadians to be better protected from major disasters, accidents and intentional acts by supporting and coordinating the response to events affecting the national interest. The GOC provides 24/7 monitoring and reporting, national-level situational awareness, warning products and integrated risk assessments, national-level response protocols, and whole-of-government response management.

Reporting Criteria to the GOC:

Consistent with the "all-hazards" approach to emergency management, the GOC monitors and collects information for situational awareness purposes with respect to a wide variety of potential, imminent or actual events that may develop into events of national interest. The kinds of events the GOC monitors are broadly established based upon GOC Reporting Criteria for situational awareness purposes. These criteria are reviewed annually by PS and other federal stakeholders. The Reporting Criteria currently include a diverse range of actual or potential events such as: Natural Hazards (e.g. Animal Health, Health Emergencies, and Extreme Weather), Man-made unintentional Hazards (e.g. Industrial Incidents, Telecommunication Outage, and Transportation Accidents), Man-made intentional Hazards (e.g. Death of Federal Representative on Duty, Threat to Canadian Assets, and Civic Disturbances). **Note:** No personal information is collected.

Reporting by the GOC:

The criteria for the GOC to start an enhanced monitoring and/or reporting on an event (which may occasionally include, protests or demonstrations) is for an event resulting in actual or potential, significant disruption to government operations, critical infrastructure and/or that pose a significant, actual or potential threat to public safety. The GOC compiles factual reports of events, but does not conduct any enforcement or surveillance investigations or activities. **Note:** The GOC reports do not include any personal information.

Coordination of response to events of national interest:

In fulfilling these EMA-authorized coordination responsibilities, the GOC works with all federal government institutions, provinces and territories, and, if required by the nature of the event, international partners. Personal information is on rare occasions provided to the GOC by partner agencies during certain types of events such as large-scale evacuations or repatriation of Canadians and their families from disaster-stricken areas abroad, when the collection of some personal information was required. Examples of this type of incidental collection are evacuee/repatriation manifest lists during the Lebanon evacuation of 2006 and the Haitian earthquake of 2010. Collection of personal information during these kinds of events by the federal government enables other government institutions (usually provinces/territories) to swiftly prepare appropriate emergency reception, medical care, housing, social services and resettlement arrangements for evacuees.

Note: Short description of the institutions business objectives, project objectives, project / initiative / change scope, product scope, stakeholders and assumptions.

SECTION II – Risk Area Identification & Categorization

Type of Program or Activity

Level of Risk to Privacy

Program or activity that does NOT involve a decision about an identifiable individual

☒ 1

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.

Administration of Programs / Activity and Services

☐ 2

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...).

Compliance / Regulatory investigations and enforcement

☐ 3

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).

Criminal investigation and enforcement / National Security

☐ 4

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).

Type of Personal Information Involved and Context

Level of risk to privacy

Only personal information provided by the individual – at the time of collection – relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities.

☐ 1

The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.

Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.

☐ 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

For example: the personal information by association indirectly reveals information on the health, financial situation, religious or lifestyle choices of the individual.

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

☐ 4

For example: the personal information by association indirectly reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and other individuals, such as relatives.

Program or Activity Partners and Private Sector Involvement

- Within the institution (amongst one or more programs within the same institution)
- With other federal institutions
- With other or a combination of federal/ provincial and/or municipal government(s)
- Private sector organizations or international organizations or foreign governments

Level of risk to privacy

- ☐ 1
- ☐ 2
- ☐ 3
- ☒ 4

Duration of the Program or Activity

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.

Short-term program

A program or an activity that supports a short-term goal with an established "sunset" date.

Long-term program

Existing program that has been modified or is established with no clear "sunset".

Level of risk to privacy

- ☐ 1
- ☐ 2
- ☒ 3

Program Population

- The program affects certain employees for internal administrative purposes.
- The program affects all employees for internal administrative purposes.
- The program affects certain individuals for external administrative purposes.
- The program affects all individuals for external administrative purposes.

Level of risk to privacy

- ☐ 1
- ☐ 2
- ☒ 3
- ☐ 4

Technology & Privacy

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?

Does the new or modified program or activity require any modifications to IT legacy systems and / or services?

The new or modified program or activity involve the implementation of one or more of the following technologies:

Risk to privacy

- ☐ YES
- ☒ NO

- ☐ YES
- ☒ NO

- 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).

☐ YES

☒ NO

Identify the applicable category(ies):

- 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...

☐ YES

☒ NO

Identify the applicable category(ies):

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

For the purposes of the Directive on PIA, government institution 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 behavior.

☐ YES

☒ NO

Identify the applicable category(ies):

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.

Personal Information Transmission

Level of risk to privacy

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

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.

☐ 3

USB key, diskette, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies.

☒ 4

Risk Impact to the Institution

Level of risk to privacy

Managerial harm.

☒ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☐ 2

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.

Financial harm.

☐ 3

Lawsuit, additional moneys required, reallocation of financial resources.

Reputation harm, embarrassment, loss of credibility.

☐ 4

Decrease confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Risk Impact to the Individual or Employee

**Level of
risk to
privacy**

Inconvenience.

☐ 1

Reputation harm, embarrassment.

☐ 2

Financial harm.

☒ 3

Physical harm.

☐ 4

SECTION III – Analysis of Personal Information Elements

Personal Information Elements and Sub-elements

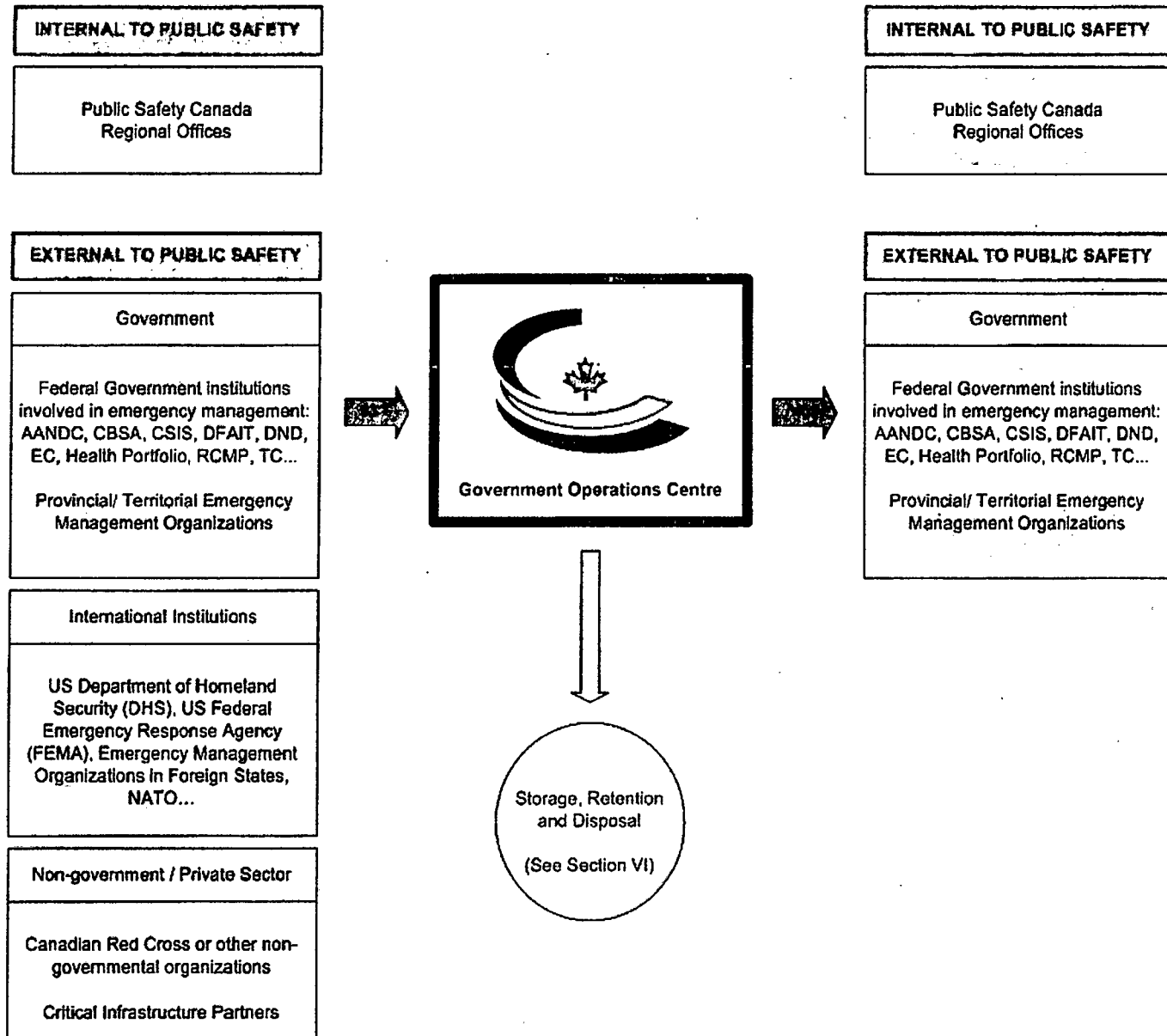
Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity is identified as a potential privacy risk (level 2-3-4) in the Risk Area Identification and Categorization.

Define each element of personal information collected	Define sub-elements of personal information associated with the element identified in the first column	How is the personal information recorded?
1) Name 2) Nationality 3) Date of Birth 4) Address 5) Passport Number 6) Emergency Medical Conditions/ Injuries / Special Needs 7) Contact details 8) Health Insurance	1) First / middle / last name 2) Citizenship, Canadian or other 3) Day / month / year 4) Street address / city / province / postal code / country 5) Passport number / place of birth 6) Basic injuries, medical conditions, or special needs requiring immediate attention for persons being moved/evacuated from a disaster area 7) Phone numbers / email addresses 8) Health card number	☒ Paper ☒ Electronic ☒ Audio Recordings ☐ Visual Image Recordings ☐ Human Biological Samples ☐ Other (Specify)

SECTION IV – Flow of Personal Information

Sources of personal
information:

Data shared with:



For an explanation of the acronyms above, please see **Appendix A – List of Acronyms**

Source of the personal information for the program or activity:

The source is the organization from which the personal information was collected. As there can be more than one source, all possible sources are identified.

SOURCE	DETAILS <i>(Including Info Source Information)</i>
Federal Government - Internal to Public Safety	
Public Safety Canada Regional Offices (PS RO)	
Federal Government - External to Public Safety	
Aboriginal Affairs and Northern Development Canada (AANDC), formerly Indian and Northern Affairs Canada (INAC)	Emergency Management Assistance Program (INA DMO 090)
Canada Border Services Agency (CBSA)	National Risk Assessment Centre (NRAC) (CBSA PRO 001, CBSA IST 001, CBSA PPU 008)
Canadian Security and Intelligence Service (CSIS)	Passenger Protect Program, Security Screening (CSIS PPU 070, CSIS DDS 052)
Department of Foreign Affairs and International Trade (DFAIT)	Emergency Watch and Response Centre (DFAIT PPU 010, DFAIT CLD 917, DFAIT CED 908, DFAIT CLD 918)
National Defence (DND)	International Disaster Relief and Humanitarian Response Operations, Search and Rescue, Situational Awareness, CSE Foreign Intelligence Files (DND PPB 140, DND ADO 275, DND PPU 050, DND MIS 080, DND PPU 040)
Environment Canada (EC)	Environmental Emergencies (EC SMW 313)
Health Portfolio (HC and PHAC)	Health Portfolio Emergency Operations Centre (PHAC 010 0048)
Royal Canadian Mounted Police (RCMP)	National Operations Centre (NOC) (RCMP OPS 002, RCMP PPU 011)
Transport Canada (TC)	Transport Canada Situation Centre (TC ASA 001, TC ASE 001, TC HRM 002)
Non-federal Government	
Provincial/Territorial Government	Emergency Management Organizations

International	
Foreign State	U.S. Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security (DHS)
International Organization	NATO, United Nations
Private Sector	
Non-governmental Organization or Charity	Canadian Red Cross, St. John's Ambulance (information would usually be reported through the province/territory)

Internal use and disclosure

The location where the information will circulate within the federal organization, including related programs.

The personal information collected through the Government Operations Centre (GOC) may be sent to the P S Regional Offices (PS RO) to be further disseminated as needed to provincial/ territorial authorities. The PS ROs operate under the same framework of emergency management and for the purposes of using personal information, have the same mandate as the GOC to support response coordination of events affecting the national interest. Neither the GOC nor the PS ROs directly use the personal information collected.

Program	
Government Operations Centre	Emergency Management Operations (PS EMNS 050)

External Use and Disclosure

The organizations to which personal information could be disclosed under this program.

Federal Government - Internal to Public Safety	
Public Safety Canada Regional Offices (PS RO)	
Federal Government - External to Public Safety	
Aboriginal Affairs and Northern Development Canada (AANDC), formerly Indian and Northern Affairs Canada (INAC)	Emergency Management Assistance Program (INA DMO 090)
Canada Border Services Agency (CBSA)	National Risk Assessment Centre (NRAC) (CBSA PRO 001, CBSA IST 001, CBSA PPU 008)
Canadian Security and Intelligence Service (CSIS)	Passenger Protect Program, Security Screening (CSIS PPU 070, CSIS DDS 052)
Department of Foreign Affairs and International Trade (DFAIT)	Emergency Watch and Response Centre (DFAIT PPU 010, DFAIT CLD 917, DFAIT CED 908, DFAIT

	CLD 918)
National Defence (DND)	International Disaster Relief and Humanitarian Response Operations, Search and Rescue, Situational Awareness, CSE Foreign Intelligence Files (DND PPB 140, DND ADO 275, DND PPU 050, DND MIS 080, DND PPU 040)
Environment Canada (EC)	Environmental Emergencies (EC SMW 313)
Health Portfolio (HC and PHAC)	Health Portfolio Emergency Operations Centre (PHAC 010 0048)
Royal Canadian Mounted Police (RCMP)	National Operations Centre (NOC) (RCMP OPS 002, RCMP PPU 011)
Transport Canada (TC)	Transport Canada Situation Centre (TC ASA 001, TC ASE 001, TC HRM 002)
Non-federal Government	
Provincial/Territorial Government	Emergency Management Organizations

Retention / Storage

The organizations that will store the personal information including duplicates or backups of databases.

Since the GOC itself does not use the personal information for any administrative purpose it is not retained after an incident is closed. The GOC tracks the receipt, storage, dissemination and destruction of the personal information within the organization.

The GOC is unable to confirm which, if any, organizations store the information beyond the termination of the incident or emergency event being managed, since organizations receiving personal information are responsible for handling, storing, and disposing of it in accordance with all applicable legislation. The GOC logs all instances of dissemination of the personal information and attaches a "personal information disclosure caveat" to personal information transmissions.

The GOC limits the dissemination of any personal information to organizations that need that information for their own operational response. When necessary, the GOC places restrictions on the distribution of any kind of information through the use of its dissemination levels system for other organizations (See Section VII – Dissemination Levels). Information distributed by the GOC will indicate to relevant organizations if and to what extent the information may be shared internally and externally.

For internal purposes, the GOC has developed a Privacy Protocol that includes procedures for PS staff to follow in relation to logging in of a receipt of any personal information, limiting the dissemination of personal information within the GOC or with its partners, attaching a "personal information disclosure caveat", as well as steps for disposal of any personal information after the emergency period.

Access to Information

The organizations that can access or handle personal information collected for the program or activity. Locations and approximate sizes of groups are given where available.

Federal government Institution responsible for program or activity:		
Groups, Areas, Divisions	Positions who have access to or use the personal information *	Geographical Location
Government Operations Centre (GOC)	Approximately 35 individuals	National Capital Region
Public Safety Canada's Regional Offices (PS RO)	Approximately 50-75 individuals	Vancouver, Winnipeg, Toronto, Montreal, Dartmouth
Other federal government Institution responsible for program or activity:		
Aboriginal Affairs and Northern Development Canada (AANDC), formerly Indian and Northern Affairs Canada (INAC)	Unknown	National Capital Region
Canada Border Services Agency (CBSA)	Unknown	National Capital Region
Canadian Security and Intelligence Service (CSIS)	Unknown	National Capital Region
Department of Foreign Affairs and International Trade (DFAIT)	Unknown	National Capital Region
National Defence (DND)	Unknown	National Capital Region
Environment Canada (EC)	Unknown	National Capital Region
Health Portfolio (HC and PHAC)	Unknown	National Capital Region
Royal Canadian Mounted Police (RCMP)	Unknown	National Capital Region
Transport Canada (TC)	Unknown	National Capital Region
Non-federal institution or private sector:		
Provincial/Territorial Government – Emergency Management Organization (EMO)	Unknown	Across Canada
Municipal Government	Unknown	Across Canada
Aboriginal Government/ Council	Unknown	Across Canada

* It is important to note that not all positions/groups listed in this column will have access to the personal information collected for a particular response. This is the number of people who potentially have access to information, depending on the nature of the incident or event.

SECTION V – Privacy Compliance Analysis

Collection Authority (Section 4 of the *Privacy Act*)

1. Has each element and sub-elements of personal information collected or to be collected been justified in terms of its necessity to the administration of the program or activity? <i>Note: "Necessary" is a higher standard than merely being useful.</i>	☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Review the proposed personal information elements and sub-elements outlined in the Personal information Analysis section to determine which pieces are "necessary" and not merely useful. Document any changes.
2. Is the Social insurance Number (SIN) being collected?	☐ YES ☒ NO	If YES Please state the legal and policy authority: Action Required to Support Legal & Policy Compliance in the absence of legal and policy authority to collect the SIN: ☐ Establish explicit legislative authority through legislative amendments. ☐ Establish legal and policy authority as outlined in the <i>Directive on SIN</i>.

Direct Collection – Informed of Purpose (Section 5 of the *Privacy Act*)

3. Is the information collected directly from the individual?	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Draft a detailed 'Privacy Notice' that integrates the required elements outlined below ☐ Integrate to the 'Privacy Notice', as appropriate, a request for consent for uses and disclosures that are not directly related to the purpose of the collection. The request for consent must include the required elements outlined in the <i>Directive on Privacy Practices</i>. The privacy notice must state all of the following: ☐ The purpose and authority for the collection; ☐ Any uses or disclosures that are consistent with
--	--	--

		the original purpose; ☐ Any uses or disclosures that are not related to the original purpose; ☐ Any legal or administrative consequences for refusing to provide the personal information; and ☐ The rights of access to, correction of and protection of personal information under the <i>Privacy Act</i>. *Adapting the privacy notice for either written or verbal communication at the time of collection. Written notices are to include a reference to the PIB described in Info Source. The Consent Form must state all of the following: ☐ The purpose of the consent and the specific personal information involved; ☐ The sources who will be asked to provide the information, in the case of indirect collections; ☐ Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought; ☐ Any consequences that may result from withholding consent; and ☐ Any alternatives to providing consent. Note: The above is supplementary to the information in the privacy notice. If NO ☒ Ensure that the requirements stated at Question 5 are met. <u>Policy requirement:</u> A detailed "Privacy Notice" is required where personal information is collected for an administrative purpose. <u>Legal Consideration:</u> Section 10 of the <i>Privacy Regulations</i> provides for the rights or actions under the act to be exercised or performed on behalf of a minor, an incompetent person, a deceased person or a person authorized by law to administer the affairs of that person.
--	--	---

4. Is the information collected from another source with informed consent of the individual?	☒ YES ☐ NO	If <u>NO</u> — or if YES and NO ☐ Ensure that the requirements stated at Question 3 are met. <u>Policy requirement:</u> Inform the individual of what information will be collected, how the information will be used and what source will be asked to provide the information. Individuals should also be informed of any alternatives or consequences that may result from their refusal to authorize any indirect collection. Written authorization from the individual to whom the personal information pertains is required. Collection of personal information from another source may be required in order to ensure that the personal information is accurate and up-to-date. See Question 8 regarding accuracy requirements.
5. Is the information collected from another source without notice to or consent from the individual? - Is the collection a result of a disclosure under subsection 8(2) of the Act? - Would direct notification of the individual result in the collection of inaccurate information? - Would direct notification of the individual defeat the purpose or prejudice the use for which the information is collected? - Is the information used for a non-administrative decision about the individual?	☐ YES ☒ NO ☐ YES ☒ NO ☐ YES ☒ NO ☐ YES ☒ NO	If <u>YES</u> Action Required to Support Legal & Policy Compliance: ☐ Ensure that the personal information bank's description adequately reflects the nature of such activities. If <u>NO</u> Action Required to Support Legal & Policy Compliance: ☐ Direct collection must be adopted and the individual must be notified of the purpose of the collection. ☐ Ensure that the requirements stated at Question 3 are met. ➤ Comment: Direct collection and notification is not applicable. ➤ Information is not directly collected since the GOC does not have any direct contact with individual members of the public affected by an incident. The GOC may be the recipient of personal information collected by other authorities who may be directly involved in responding to an incident. ➤ Consequently as the GOC is not in direct contact with individuals it is not feasible to notify individuals about the purpose of collection due to the emergency nature of the situation. Events such as evacuations can occur rapidly and often there is no possible

		way to establish contact. <u>Policy principle</u> The exception to direct collection should be used sparingly. It is primarily intended for use by investigative bodies in those circumstances where direct collection would jeopardize the investigation.
6. Will the personal information collected only be used for: • The purpose for which it was collected or a purpose consistent with that purpose? • A purpose consistent with section 8(2) of the Act?	☒ YES ☐ NO ☒ YES ☐ NO	If <u>NO</u> Action Required to Support Legal & Policy Compliance: ☐ Identify all secondary purposes in the PIB description (i.e. other uses within the department or by another federal/provincial institution that has authority to collect the information). ☐ Integrate in the 'Privacy Notice', as appropriate, a listing for uses and disclosures that are not directly related to the purpose of the collection or consistent with that purpose. ☐ Ensure that the requirements stated at Questions 4 or 5 are met. <u>Policy requirement</u> Inform the individual at the time of collection of any intended uses or disclosures that are not directly related to the program or activity for which the information is being collected. (This would be considered an indirect collection by other programs.) <u>Policy Requirement</u> Ensuring that individuals are notified in advance of follow-up activities including all means of communication to be expected by the government institution. The individuals will be in a position to recognize legitimate requests for personal information. This will help minimize the risk of individuals providing their personal information under a false pretext.
Retention (Section 6 of the <i>Privacy Act</i>)		
7. Is the personal information being used to make a decision or as part of a process to make a decision that directly affects an identifiable individual? This includes use for verification/authentication purposes.	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Prepare and obtain approval for a retention schedule based on your legal requirements and operational needs; AND ☐ Retain records for a minimum of 2 years as required by the <i>Privacy Regulations</i>; OR ☐ Obtain consent of the individual to dispose of the personal information earlier than the minimum 2 year retention period; AND

	☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. If NO Action Required to Support Legal & Policy Compliance: ☐ Ensure that the policy requirements for Non-Administrative Privacy Protocol, outlined in the <i>Policy on Privacy Protection</i> are followed. ➤ Public Safety Canada's Privacy Protocol is in the approval stages. In the meantime, information is retrieved and treated in accordance with the <i>Privacy Act</i>. ☐ Prepare and obtain approval for a retention schedule based on your legal requirements and operational needs. ➤ Since the personal information collected is transitory in nature, the GOC does not retain it beyond the termination of an incident. ☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. ➤ Since the personal information collected is transitory in nature, the GOC is not required to obtain a disposition authority. The GOC is responsible for determining appropriate retention time and subsequently disposing of the information in accordance with departmental standards. This time may vary based on the type of incident being responded to. <u>Policy requirement</u> Retain personal information for a minimum of two years, as detailed in section 4 of the <i>Privacy Regulations</i>. In accordance with the <i>Library and Archives of Canada Act</i>, only the Librarian and Archivist of Canada may authorize the disposition of government records by issuing Records Disposition Authorities (RDA).
--	---

Accuracy – (Section 6 (2) of the <i>Privacy Act</i>)		
8. What measures will be taken to ensure that the personal information used in		If YES

administrative decisions is accurate, up-to-date and complete? (More than one option may apply) - Direct collection or validation with the individual. - Technological means to identify keystroke errors and discrepancies. - Personal information matching program to verify personal information integrity against a "reliable source" where authorized or where consent was obtained. - In cases where direct collection or consent is not feasible, obtain information from trusted sources (either public or private) and verify accuracy against existing personal information before use. If Other – please define below:	☐ YES ☐ YES ☐ YES ☐ YES ☐ YES	Action Required to Support Legal & Policy Compliance: ☐ Ensure that, if applicable, your institution's PIB mentions the use of periodic personal information matching as a consistent use. If NO Please provide details as to why reasonable steps cannot be used. ➤ Not applicable <u>Legal and Policy Requirements</u> Subsection 6(2) of the <i>Privacy Act</i> requires government institutions to take <i>all reasonable steps</i> to ensure that personal information that they use for an administrative purpose is as accurate, up-to-date and complete as possible. Decisions that directly affect individuals must be made on the basis of accurate, up-to-date and complete information as possible. If periodic personal information matching occurs for the purposes of ensuring accuracy of information, institutions must reflect this under the "consistent use" section of the relevant PIB.
--	---	--

Use (Section 7 of the <i>Privacy Act</i>)		
9. Is there an activity log attached to the personal information record to record uses not described in the Personal Information Bank (Info Source)?	☒ YES ☐ NO	If YES Action Required to Support Legal & Policy Compliance: ☒ An activity log is attached to personal information records when used for consistent but unreported use. ➤ The GOC maintains a detailed duty and information log that details how information is used and exactly where and when it is disclosed. Should use of personal information outside the scope of the PIA occurs, it is reported to the departmental ATIP Coordinator. The ATIP Coordinator ensures that the Privacy Commissioner and TBS are advised and, if necessary, updates the GOC's description of information use on

		Info Source. ☒ The Privacy Commissioner is advised of this consistent use. ☐ The PIB description is amended, in time for the next edition of Info Source, to include the unreported use. If NO Action Required to Support Legal & Policy Compliance: ☐ Institutions must put in place a means to record and identify uses that were not described in the Personal Information Bank. Legal Requirements: Section 9(4) of the <i>Privacy Act</i> requires a government institution to report to the Privacy Commissioner any consistent use of personal information that has not been included in the Index, and to ensure that the use is included in the next statement of consistent uses set forth in the next edition of the Index. Policy Requirement If personal information used for a consistent purpose that is not identified in a personal information bank – the head of the institution or delegate must notify the Privacy Commissioner
Disclosure (Section 8 of the <i>Privacy Act</i>)		
10. Are processes in place to ensure that personal information will only be disclosed to individuals within and without the government institution who have a "need to know" and that there are adequate privacy practices to ensure the confidentiality and integrity of the personal information? This includes procedures to prevent against loss or theft. This covers the entire lifecycle of the personal information: • Collection • Use • Retention • Disposition.	☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Ensure that the requirements stated at Question 11 are met by the receiving institution. <u>Policy requirement</u> Government institutions are to ensure that adequate safeguards are in place when disclosing information. This includes having an action plan for privacy breaches (unauthorized disclosures) and measures (physical, logical, administrative) to ensure that only the people that "need to know" have access to the personal information. See <i>Directive on Privacy Practices</i> ➤ The GOC uses the appropriate document classification levels so that information is protected when disclosing to other organizations.

This includes disclosures to other government institutions, other levels of government, other jurisdictions, foreign governments, international organizations or private sector organizations		➤ The GOC also uses a system of dissemination levels when releasing information; this system tells the recipient group the extent to which they are allowed to share that information internally and externally to their organization. ➤ The GOC applies caveats, when releasing any personal information to our partners that highlights the fact that the information is being shared and should be treated in accordance with the applicable privacy laws. ➤ Non-federal organizations are subject to both (1) the <i>Personal Information Protection and Electronic Documents Act</i> (PIPEDA); and in some cases (2) provincial/municipal privacy legislations/regulations. As such, the GOC expects these organizations to be in compliance with the applicable legislation and regulations and store/handle personal information accordingly. ➤ Since federal organizations are subject to the <i>Privacy Act</i>, these organizations are expected to be in compliance with this legislation and handle personal information accordingly.
11. Is the disclosure of the personal information governed by: A Memorandum of understanding? An accord? An arrangement? A contract? If Other – please define below: The GOC developed an internal process for those rare occasions when personal information is included in the information being disseminated to our partners (within and outside of the federal government). When this is the case,	☐ YES ☐ YES ☐ YES ☐ YES	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure the PIB description identifies this use. ☐ Ensure that the notification or consent notice mentions this use. ☐ Ensure contractual clauses are included to protect personal information. Contracts that are established with private sector entities outline measures and provisions to address the following: ☐ Control over the personal information; ☐ Limitations on collection and handling as well

partners will receive a personal information caveat (Appendix B) that highlights the fact that the information is being shared and should be treated in accordance with the applicable privacy laws.	as any prohibitions regarding the personal information for the purposes of the contract; ☐ Disposition of the personal information, where relevant; ☐ Administrative, technical and physical safeguards; and ☐ Obligations of other parties acting on behalf of the government institution. If NO Action Required to Support Legal & Policy Compliance: ☐ Prepare a written statement describing the nature of the information sharing and have it approved by the relevant parties. Policy on Privacy Protection Measures are to be established, when personal information is involved, to ensure that the government institution meets the requirements of the <i>Privacy Act</i> when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations. Ensure that appropriate privacy protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information. If any portion of the project (administration, service delivery, system maintenance or personal information storage) involves the use of a third-party contractor, care must be taken to ensure that institutions continue to fulfill their privacy obligations.
Technology and Privacy	
12. Will the system/software /program application employ cookies or other tracking methods to collect personal information about users and their transactions? If so, for what purposes will the collected information be used and how long will the information be retained? Please define purpose and retention period below:	☐ YES ☒ NO If YES Action Required to Support Legal & Policy Compliance: ☐ Collection and use of personal information through these means must be reflected both in the PIB description and the Privacy Notice. ☐ Technology staff who have access to personal information collected through these methods must be aware of privacy and security policy requirements.

13. Does the new or modified program or activity result in an increased ability for surveillance or monitoring of a given target population?	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that the requirements in regards to awareness stated at Question 12 are met.
---	--	--

Privacy Considerations Related to Compliance Regulatory Investigation & Enforcement		
14. Is the legal authority for conducting compliance / regulatory investigation and enforcement the same as the legislative authority for the program or activity?	☐ YES ☐ NO ☒ N/A	If NO Action Required to Support Legal & Policy Compliance: Identify legislative authority: ☐ Ensure that the requirements stated at Questions 3 and 6 are met. ☐ Ensure the activities are listed in the PIB's description. If YES Action Required to Support Legal & Policy compliance: ☐ The activities are listed in the Privacy Notice; ☐ The activities are listed in the PIB's description. ➤ Not applicable - the GOC does not conduct investigations or enforcement activities.

Privacy Considerations Related to Search and Seizure
15. What is the specific legal authority for conducting regulatory or criminal enforcement, surveillance or intelligence gathering? Not applicable – the GOC does not conduct any enforcement or surveillance investigations or activities. Action Required to Support Legal & Policy Compliance: ☐ Request legal advice from your Legal Services Unit about compliance with section 8 of the <u>Charter of Rights and Freedoms</u>, the <u>Privacy Act</u> and other applicable acts

SECTION VI - Summary of Analysis and Risk Mitigation

Risks and Mitigation

The Government Operations Centre's (GOC) use of personal information is inherently low-risk for three reasons. First, personal information is rarely received by the GOC. Only for exceptional and often large-scale events involving, for example, an evacuation or repatriation is personal information sometimes involved. Secondly, the GOC's use of personal information is limited solely to transmission to the appropriate partner; no analysis of personal data is necessary within the GOC. Lastly, no personal information is retained by the GOC beyond the termination of the event, because that data is not relevant to any decision making, administration, strategic objective or reporting.

Nevertheless, risks do exist for the use of personal information at the GOC in three phases: collection, storage and disclosure. These risks and the GOC's proposed mitigation strategies for each are outlined in the table below. In general, the GOC reduces risk by strengthening processes already in place, continual training, evaluation, and the implementation of lessons learned.

Collection Phase	RISK:
	While the GOC does not directly collect personal information, it does on rare occasions accept data from a trusted partner. The risk is two-fold. First, the GOC must assume that the personal information collected was done so in accordance with appropriate legislation. Secondly, there is a risk of the GOC accepting personal information that is unnecessary for operations and may have been sent by a partner either in error or with a misunderstanding of the GOC's mandate and information requirements.
	MITIGATION: To address the risk of collecting unnecessary personal information, the GOC returns to sender any personal data that may be inadvertently or mistakenly sent to the GOC. This may include, but is not limited to, replying to the email and informing the sender that the GOC does not require or want such information and does not intend to retain such information. Follow-ups with the organization(s) responsible may be required and are conducted when necessary. Any personal information contained in the original message is then deleted from all GOC systems, including electronic and hard-copy formats. The GOC has developed a Privacy Protocol for the GOC staff on collection of the personal information by the GOC. Dissemination levels (DL) are another means by which the GOC and its federal partners can appropriately limit the sharing of information, thus helping to reduce the risk associated with the collection of personal information. A specific DL is assigned to information by the originator and corresponds to an agreed-upon group or level for distribution. In this way, the originator has a degree of control over the spread of the information. More information on DLs can be found in Section VII.

Storage Phase	RISK: For the duration of the event, any personal information that is received by the GOC and deemed to be necessary to emergency management operations is <u>temporarily stored</u> within the GOC. This may include electronic records or hard copies. The risk in the storage phase is to the confidentiality of the personal information. Anyone with access to the operations centre or the GOC servers could theoretically view personal information. There is also a risk that the information may not be promptly deleted and may reside longer than necessary on GOC systems. MITIGATION: The risk associated with storing the personal information during an event is best mitigated if the transfer, copying, circulation, saving and printing of personal information is minimized wherever possible. While some people may need to know that certain personal data has arrived at the GOC, few, if any, GOC staff actually need to view the information itself. Emails, conversations and reports should therefore refer to but not contain the personal data. Best practice is to keep a copy of the personal information only in the format in which it was received, and transfer it to the relevant partner/organization using the same means. This mitigation strategy of keeping personal information on only one system limits access and helps reduce unnecessary diffusion. The GOC has developed a Privacy Protocol for the GOC staff on storage of the personal information collected by the GOC.
Disclosure Phase	RISK: The final risk identified for the GOC's use of personal information is the disclosure to partners for emergency management purposes. Similar to risk associated with data collection, the GOC must assume that recipients of personal information transmitted through the GOC use the data in accordance with all appropriate legislation. The GOC is also responsible for deciding to which organization or group the personal information needs to be sent. This decision carries the risk of human error or poor judgement. MITIGATION: The risk associated with the disclosure of personal information by the GOC is largely mitigated by selective targeting of groups or organizations to which the information is sent. Generally, the GOC shares its information with a large number of partners to facilitate a whole-of-government response and to ensure all organizations are kept informed of events. With personal information, however, it is important for watch teams to be selective in their disclosure in order to keep distribution on a need-to-know basis. As with the first two mitigation strategies, staff training on this issue will reduce risk. The GOC has developed a Privacy Protocol for the GOC staff on dissemination of the personal information collected by the GOC. If personal information must be shared:

	a. A "personal information disclosure caveat" would be attached to the transmission that would highlight that the personal information is being shared and should be treated in accordance with the applicable Privacy laws; b. Detailed log would be developed that would show what personal information was shared, with whom and on what day; c. At the end of the emergency period (at the point of closing an event), all the personal information received by the GOC would be destroyed and a follow up will be conducted with the organizations that received some private information from the GOC stating that the emergency period has ended and reminding them about their obligations under the privacy laws applicable to them. As mentioned above in the Collection Phase mitigation section, Dissemination Levels (DLs) can be used by the originator of the information to appropriately limit its sharing and distribution. This is another tool that can be used to mitigate the risk associated with Information disclosure. More information on DLs can be found below in Section VII.
--	--

Policy on disposing of personal information:

Personal information that is stored electronically is destroyed appropriately according to its level of classification. At the classification "Protected B" and lower, all electronic copies of the information are deleted (including attachments to emails and saved versions), and then the computer's recycling bin is emptied. From "Protected C" up to and including Secret level, electronic information is deleted securely using an approved disk sanitization utility. IM/IT Security is contacted if assistance is required. For Top Secret systems, IM/IT Security is contacted for approved document disposal.

For paper copies at any level of classification, the approved paper shredding device is used to dispose of personal information. If there is a large quantity of paper to be shredded, classified information up to and including Secret level is packed into 1ft cubic boxes for disposal by the Records Office. A Classified Document Disposal Form (<http://infocentral/cnt/is/admn/fat-eng.aspx#fat-02>) is required, and pickup is coordinated through the mailroom. More detailed can be found here: <http://infocentral/cnt/is/admn/rcrds-ffc/dstrctn-eng.aspx>.

Photocopying of personal information, even where classification levels allow, is avoided except when absolutely necessary, to limit the diffusion of the information.

More information on document disposal can be found at the following link for Transmission, Storage and Destruction of Designated and Classified Information: <http://infocentrale/cnt/is/sec/fl/tsd-eng.pdf>.

SECTION VII – Supplementary Documents List

Federal Departments and Agencies - Dissemination Levels

Guidelines for Information Sharing and Reporting Among Federal Operations Centre

Federal Operations Centres Working Group

Date of Issue: 09 Dec 2011

Version 1.0

(Excerpt)

USE OF DISSEMINATION LEVELS

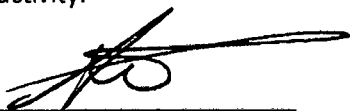
The Primary Department/originator should inform the GOC and other supporting Departments of any limitations on the further dissemination of any correspondence. There are five dissemination levels:

- a. *DL – 1 - Releasable to Critical Infrastructure Partners and the Public. This level would apply to information that is suitable for release CI Partners and the public. Level 1 assumes that distribution may still be limited and will be tailored for private partners and the public.*
- b. *DL – 2 - Releasable to All Federal Departments and Agencies. This level would apply to information that is suitable for release to all Federal Departments/Agencies and supporting organizations;*
- c. *DL – 3 - Releasable to Authorized Organizations and Key Decision-Makers. This level would apply to information that is required by authorized organizations/GOC and key decision-makers at all levels to determine the appropriate preventative and/or protective measures to mitigate against known threats. Level 3 assumes that distribution is limited;*
- d. *DL – 4 - Releasable to Authorized Federal Organizations. This level would apply to information that is suitable for release to specific federal organizations and the GOC (see note below). Level 4 assumes that distribution is authorized for select key partners with the necessary need to know; and*
- e. *DL -5 - No Further Dissemination Authorized. This level is designated for information releasable internally within the department/agency. Level 5 is the most restrictive level and would be applied to the most sensitive information. Level 5 assumes that only limited distribution is authorized based on strict need to know.*

All departments/agencies must follow the directions in any report containing a dissemination level. If the GOC or another department/agency feels that there are additional government departments that need to be informed, then the department holding the information must seek approval from the originator prior to disseminating any further. Any changes to a dissemination level should be communicated as soon as possible so that the information flows as efficiently as possible.

SECTION VIII - 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 core PIA as they relate to the administration of the identified program or activity.



Signature of PIA lead for program or activity (DG or senior official with functional authority for program)

MAR 24 2015

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.



Signature of Head of the institution or the delegate responsible for Section 10 under the Privacy Act (ADM or other delegated authority)

March 29 / 2015

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

Appendix A - List of Acronyms

English		Français	
Acronym	Definition	Définition	Acronyme
AAFC	Agriculture and Agri-Foods Canada	Agriculture et Agroalimentaire Canada	AAC
AANDC	Aboriginal Affairs and Northern Development Canada	Affaires autochtones et Développement du Nord Canada	AADNC
ADM	Assistant Deputy Minister	Sous-ministre adjoint/e	SMA
ATIP	Access to Information and Privacy	Accès à l'information et protection des renseignements personnels	AIPRP
CBSA	Canada Border Services Agency	Agence des services frontaliers du Canada	ASFC
CCG	Canadian Coast Guard	Garde côtière canadienne	GCC
CCIRC	Canadian Cyber Incident Response Centre (@PS)	Centre Canadien de réponse aux incidents cybernétiques (@SP)	CCRIC
CFIA	Canadian Food Inspection Agency	Agence canadienne d'inspection des aliments	ACIA
CHC	Canadian Hurricane Centre	Centre canadien de prévision d'ouragan	CCPO
CIC	Citizenship and Immigration Canada	Citoyenneté et Immigration Canada	CIC
CIDA	Canadian International Development Agency	Agence canadienne de développement international	ACDI
CNSC	Canadian Nuclear Safety Commission	Commission canadienne de sûreté nucléaire	CCSN
CRA	Canada Revenue Agency	Agence du revenu du Canada	ARC
CRC	Canadian Red Cross	Croix-Rouge canadienne	CRC
CSC	Correctional Service of Canada	Service correctionnel du Canada	SCC
CSE	Communications Security Establishment	Centre de la sécurité des télécommunications	CST
CSIS	Canadian Security Intelligence Service	Service canadien du renseignement de sécurité	SCRS
DFAIT	Department of Foreign Affairs and International Trade	Ministère des Affaires étrangères et du Commerce international	MAECI
DFO	Fisheries and Oceans Canada	Pêches et Océans Canada	MPO

English		Français	
Acronym	Definition	Définition	Acronyme
DG	Director General	Directeur général / Directrice générale	DG
DL	Dissemination Level	Niveau de diffusion	ND
DM	Deputy Minister	Sous-ministre	SM
DND	Department of National Defence	Ministère de la Défense nationale	MDN
DoJ	Department of Justice	Ministère de la Justice	MJ
EC	Environment Canada	Environnement Canada	EC
EM	Emergency Management	Gestion des urgences	GU
EMA	<i>Emergency Management Act</i>	Loi sur la gestion des urgences	LGU
EMRO	Emergency Management and Regional Operations (@PS)	Gestion des mesures d'urgence et opérations régionales (@SP)	GMUOR
FERP	Federal Emergency Response Plan	Plan fédéral d'intervention d'urgence	PFIU
GC	Government of Canada	Gouvernement du Canada	GC
GOC	Government Operation Centre	Centre des opérations du gouvernement	COG
HC	Health Canada	Santé Canada	SC
HP	Health Portfolio (HC, PHAC, & Emergency Operations centre @HC)	Portefeuille de la Santé (SC, ASPC, et COU @SC)	
IM	Information Management	Gestion de l'information	GI
MOA	Memorandum of Agreement	Protocole d'entente	PE
MOU	Memorandum of Understanding	Protocole d'entente	PE
NERS	National Emergency Response System	Système national d'intervention d'urgence	SNIU
NGO	Non-Governmental Organization	Organisation non gouvernementale	ONG
NPB	National Parole Board	Commission des libérations conditionnelles du Canada	CLCC

English		Français	
Acronym	Definition	Définition	Acronyme
NRC	National Research Council of Canada	Conseil national de recherches Canada	CNRC
NRCan	Natural Resources Canada	Ressources naturelles Canada	RNCan
NSERC	Natural Sciences and Engineering Research Council	Conseil de recherches en sciences naturelles et en génie	CRSNG
OGD	Other government department	Autres ministères du gouvernement	AMG
Opscen	Operations Centre	Centre des opérations	Opscen
PCO	Privy Council Office	Bureau du Conseil privé	BCP
PHAC	Public Health Agency of Canada	Agence de la santé publique du Canada	ASPC
PMO	Prime Minister's Office	Cabinet du Premier ministre	CPM
PS	Public Safety Canada	Sécurité publique Canada	SP
PSEPC	Public Safety and Emergency Preparedness Canada (former name for PS)	Sécurité publique et Protection civile Canada (ancien nom de SP)	SPPCC
PWGSC	Public Works and Government Services Canada	Travaux publics et Services gouvernementaux Canada	TPSGC
RCMP	Royal Canadian Mounted Police	Gendarmerie royale du Canada	GRC
RO	Regional Office	Bureau régional	BR
TBS	Treasury Board of Canada Secretariat	Secrétariat du Conseil du Trésor	SCT
TC	Transport Canada	Transports Canada	TC

Appendix B – Public Safety Canada's Personal Information Caveat

Public Safety Canada Personal Information Caveat

Personal information contained in the attached document(s) is provided in confidence by Public Safety Canada to the recipient solely for the purpose of *(enter purpose - i.e.: providing necessary health or social services)* as a result of the incident *(enter description of incident)*.

In accordance with applicable freedom of information and/or privacy laws and policies of the recipient, all reasonable measures must be taken to safeguard personal information against improper or unauthorized, use, disclosure, retention or disposition. This includes handling the information in accordance with the security markings.

Access to personal information is to be limited to those employees of the recipient whose duties **require access** to the personal information. Limit access by administrative, technical and physical means to protect the personal information.

Recipients shall not disseminate personal information to third parties without the prior written consent of the individual, to whom the information relates, except as authorized by law.

Personal information is to be destroyed or disposed of in accordance with the laws and policies applicable to the recipient.

Recipients are responsible for maintaining records relating to the receipt, transmission and disposal.



GOVERNMENT OPERATIONS CENTRE

CENTRE DES OPÉRATIONS DU GOUVERNEMENT

GOC Privacy Protocol

Use of Personal Information

DATE: March 9, 2015
RDIMS No.: 1240651



Government
of Canada

Gouvernement
du Canada

Canada  000100

TABLE OF CONTENTS

SECTION 1 - ADMINISTRATION & OVERVIEW-----	2
1.1 PURPOSE -----	2
1.2 SCOPE -----	2
1.3 SOP MAINTENANCE -----	2
1.4 AUTHORITIES AND REFERENCES-----	2
1.5 INTRODUCTION-----	2
1.6 GOC COMMITMENTS UNDER PRIVACY LEGISLATION -----	3
SECTION 2 – OPERATIONAL TASKS-----	3
2.1 COLLECTION PHASE-----	3
2.1.1 Risk-----	3
2.1.2 Mitigation Actions -----	3
3.1 STORAGE PHASE -----	4
3.1.1 Risk-----	4
3.1.2 Mitigation Actions -----	4
4.1 DISCLOSURE PHASE -----	4
4.1.1 Risk-----	4
4.1.2 Mitigation Actions -----	4
5.1 DISPOSAL PHASE -----	5
5.1.1 Risk-----	5
5.1.2 Mitigation Actions:-----	5
<u>Annex A: The Personal Information Collection, Dissemination and Disposal Tracking Sheet</u> -----	7
<u>Annex B: Public Safety Canada Personal Information Caveat</u> -----	8
<u>Annex C: Watch Staff Aide-Memoire</u> -----	9

SECTION 1 - ADMINISTRATION & OVERVIEW

1.1 PURPOSE

The aim of this Standard Operating Procedure (SOP) is to ensure that the personal information is handled properly and in accordance with the Privacy laws and GOC Privacy Impact Assessment (PIA).

1.2 SCOPE

This SOP addresses the procedures for GOC use of personal information, and should always be used in concurrence with other SOPs, where applicable. It is applicable to all GOC employees.

1.3 SOP MAINTENANCE

Editing of this SOP will be completed by the SOP Coordinator; if you have any suggestions or notice that the document requires corrections/updates, please submit via email to the SOP Coordinator.

SOP Contact Coordinator: Support Division.

SOP Storage: OCIP

1.4 AUTHORITIES AND REFERENCES

a. **GOC Privacy Impact Assessment (RDIMS No: #) To be updated, once new PIA is signed by the ADM, PDFed and saved in RDIMS.**

1.5 INTRODUCTION

As standard practice, the GOC does not actively collect, use, store or disclose personal information. However, in carrying out its mandate, the GOC occasionally receives and transmits personal information during events. Examples of this include the Lebanon evacuation of 2006 and the Haitian earthquake of 2010, where personal information was received and passed on to other partners by the GOC. Personal information used during these events included names, addresses, contact/passport info, and in some cases medical information for people being evacuated or repatriated. Collecting personal information during these kinds of events enables other government partners (usually provinces/territories) to prepare appropriate emergency reception, medical care, housing, social services and resettlement arrangements for evacuees.

Recognizing that occasional use of personal information is a part of our business, the GOC acknowledges that there are some risks associated with receiving and transmitting this type of information that need to be mitigated.

1.6 GOC COMMITMENTS UNDER PRIVACY LEGISLATION

Privacy legislation is in place to ensure personal information is protected and dissemination is limited to those that have a mandate to collect this type of information. The GOC completed a Privacy Impact Assessment. In this document, the GOC committed to several actions to mitigate the risks associated with our use and transmission of personal information.

SECTION 2 – OPERATIONAL TASKS

2.1 COLLECTION PHASE

2.1.1 Risk

While the GOC does not directly collect personal information, it is responsible for the acceptance of data from a trusted partner. This risk is two-fold. First, the GOC must assume that the personal information collected was done so in accordance with appropriate legislation. Secondly, there is a risk of the GOC accepting personal information that is unnecessary for operations and may have been sent by a partner either in error or with a misunderstanding of the GOC's mandate and information requirements.

2.1.2 Mitigation Actions

- If personal information was received in error:
 - a. Return to sender any personal data that may be inadvertently or mistakenly sent to the GOC. This may include, but is not limited to, replying to the email and informing the sender that the GOC does not require such information;
 - b. Delete/destroy all copies of personal information contained in the original message from all GOC systems, including electronic and hard-copy formats. See *Disposal Instructions* below;
- If personal information is required for the coordination of the response to an event:
 - a. Follow-up with the organization(s) responsible, if required, to clarify the GOC's information requirements;
 - b. If possible (when personal information is not required for the coordination of a response), remove all personal identifiers, while keeping other operational information;
 - c. Log the receipt of the information in *The Personal Information Collection, Dissemination and Disposal Template*. Please refer to Annex A.

3.1 STORAGE PHASE

3.1.1 Risk

For the duration of the event, any personal information that is received by the GOC and deemed to be necessary to emergency management operations is temporarily stored within the GOC. This may include electronic records or hard copies. The risk in the storage phase is to the confidentiality of the personal information. Anyone with access to the operations centre or the GOC servers could theoretically view personal information.

3.1.2 Mitigation Actions

- Store the personal information only in the format in which it was received and transfer it to the relevant partner/organization using the same means. Keeping personal information on only one system limits access and helps reduce unnecessary dissemination.
- All personal information stored at the GOC must be identified in the *Personal Information Collection, Dissemination and Disposal Tracking Sheet*. Please refer to Annex A (RDIMS #1288582).
- Minimize the transfer, copying, circulation, saving and printing of personal information wherever possible;
- Photocopying of personal information, even where classification levels allow, is avoided except when absolutely necessary, to limit the diffusion of the information;

4.1 DISCLOSURE PHASE

4.1.1 Risk

The risk identified for the GOC's use of personal information is the disclosure to partners for emergency management purposes. Similar to risk associated with data collection, the GOC assumes that recipients of personal information transmitted through the GOC use the data in accordance with all appropriate legislation. The GOC is also responsible coordinating with federal partners to which organization or group the personal information needs to be sent.

4.1.2 Mitigation Actions

- Do not use/transmit personal information unless it is absolutely required for an emergency response;
- If dissemination of information is required for the response activities:
 - a. Wherever possible limit dissemination of personal information within the GOC and with our limited number of partners based on their mandates;
 - b. Only Operations Centre is allowed to disseminate personal information to partners outside of the GOC;

- c. Whenever possible share emergency related information without personal identifiers or by using a summary of information rather than specific identifiers;
- d. Any dissemination of personal information must be recorded in the *Personal Information Collection, Dissemination and Disposal Tracking Sheet*. Please refer to Annex A (RDIMS #1288582).
- e. Selectively target groups or organizations to which the information is sent using Dissemination Levels or limited distribution lists;
- f. Attach the *Public Safety Canada Personal Information Caveat* to any dissemination of personal information. Please refer to Annex B (RDIMS# 1302770).

5.1 DISPOSAL PHASE

5.1.1 Risk

Any personal information received by the GOC is stored in the organization only on temporary basis. Once the emergency period is over (at the point of closing an event) all personal information must be destroyed. A follow up must be conducted with the organizations, if personal information was shared.

There is a risk that the information may not be promptly deleted and may reside longer than necessary on GOC systems

5.1.2 Mitigation Actions:

- Destruction:
 - a. Delete/destroy all copies of personal information from all GOC systems once the event is closed, including electronic and hard-copy formats. Once the information was deleted, record the action in the *Personal Information Collection, Dissemination and Disposal Template*. Please refer to Annex A (RDIMS #1288582).
 - b. Personal information that is stored electronically is destroyed appropriately according to its level of classification. At the classification "Protected B" and lower, all electronic copies of the information are deleted (including attachments to emails and saved versions), and then the computer's recycling bin is emptied. From "Protected C" up to and including Secret level, electronic information is deleted securely using an approved disk sanitization utility. IM/IT Security is contacted if assistance is required. For Top Secret systems, IM/IT Security is contacted for approved document disposal;
 - c. For paper copies at any level of classification, the approved paper shredding device is used to dispose of personal information. If there is a large quantity of paper to be shredded, classified information up to and including Secret level is packed into 1ft cubic boxes for disposal by the Records Office. A Classified Document Disposal Form (<http://infocentral/cnt/is/admn/fat-eng.aspx#fat-02>) is required, and pickup is

coordinated through the mailroom. More detailed can be found here:
<http://infocentral/cnt/is/admn/rcrds-ffc/dstrctn-eng.aspx>.

The GOC Privacy Protocol Aide-Memoire has been developed to facilitate the handling of personal information by GOC staff. Please refer to Annex C (RDIMS# 1307132).

More information on document disposal can be found at the following link for Transmission, Storage and Destruction of Designated and Classified Information:
<http://infocentrale/cnt/is/sec/fl/tsd-eng.pdf>.

Annex A:

The Personal Information Collection, Dissemination and Disposal Tracking Sheet

(RDIMS #1288582).

Annex B

Public Safety Canada Personal Information Caveat

(RDIMS# 1302770).

Personal information contained in the attached document(s) is provided in confidence by Public Safety Canada to the recipient solely for the purpose of (*enter purpose - i.e.: providing necessary health or social services*) as a result of the incident (*enter description of incident*).

In accordance with applicable freedom of information and/or privacy laws and policies of the recipient, all reasonable measures must be taken to safeguard personal information against improper or unauthorized, use, disclosure, retention or disposition. This includes handling the information in accordance with the security markings.

Access to personal information is to be limited to those employees of the recipient whose duties **require access** to the personal information. Limit access by administrative, technical and physical means to protect the personal information.

Recipients shall not disseminate personal information to third parties without the prior written consent of the individual to whom the information relates, except as authorized by law.

Personal information is to be destroyed or disposed of in accordance with the laws and policies applicable to the recipient.

Recipients are responsible for maintaining records relating to the receipt, transmission and disposal.

Annex C:

Watch Staff Aide-Memoire

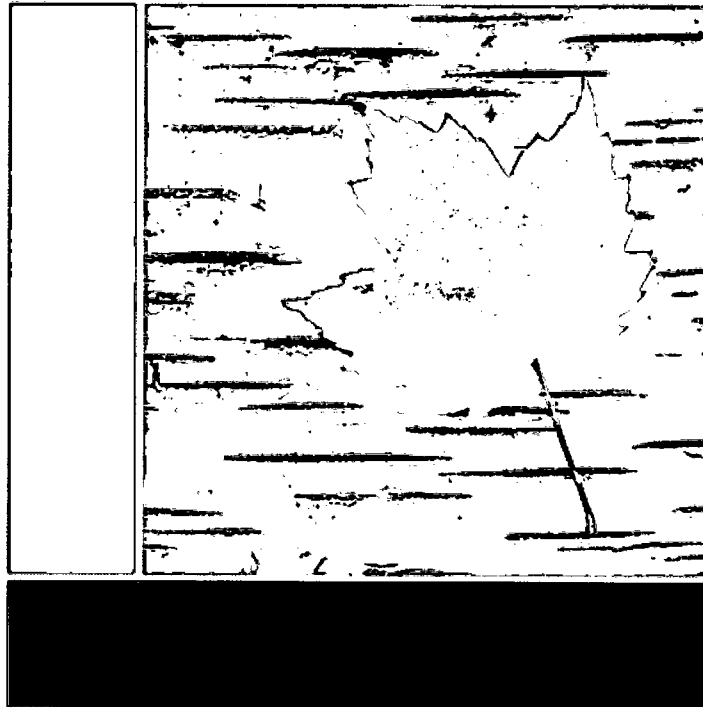
(RDIMS# 1307132)



Public Safety
Canada

Sécurité publique
Canada

BUILDING A **SAFE AND RESILIENT CANADA**



Government Operations Centre

Privacy Impact Assessment

April 2013

000110

Document Version

Version	Date	Change Made By	Change
1	Dec 2011	Sheila Gordon	
2	Feb 2012	Sheila Gordon	Initial comments from Jennifer Schofield and input from Richard Mungall
3	June 2012	Sheila Gordon	Comments from Richard Sarabura included
4	July 2012	Sheila Gordon	Comments from Jennifer Schofield included
5	Sept 2012	Sheila Gordon	Updated graphic and text edits.
6	Nov2012	Sheila Gordon	Updated with comments from PS legal
7	Jan 2013	Sheila Gordon	Final edits including MOU mitigation strategy. Added final comments from PS legal.
8	April 2013	Sheila Gordon	Added final comments from PS ATIP

Table of Contents

<i>SECTION I – Overview and PIA Initiation</i>	5
Government Institution: Public Safety Canada	5
Name of Program or Activity of the Government Institution:	5
Description of Program or Activity:	5
Description of the class of records associated with the program or activity:	6
Legal Authority for Program or Activity:	7
Summary of the project / initiative / change:	7
 <i>SECTION II – Risk Area Identification & Categorization</i>	 9
 <i>SECTION III – Analysis of Personal Information Elements</i>	 13
Personal Information Elements and Sub-elements	13
 <i>SECTION IV – Flow of Personal Information</i>	 14
Source of the personal information for the program or activity:	15
Internal use and disclosure	16
External Use and Disclosure	16
Retention / Storage	17
Access to Information	17
 <i>SECTION V – Privacy Compliance Analysis</i>	 19
Collection Authority	19
Direct Collection – Informed of Purpose	19
Retention	22
Accuracy	24
Use	24
Disclosure	25
Technology and Privacy	27
Privacy Considerations Related to Compliance Regulatory Investigation & Enforcement	28
Privacy Considerations Related to Search and Seizure	28

<i>SECTION VI - Summary of Analysis and Risk Mitigation</i>	29
Risks and Mitigation	29
Instructions for disposing of personal information:	31
 <i>SECTION VII – Supplementary Documents List</i>	 32
Federal Departments and Agencies - Dissemination Levels	32
 <i>SECTION VIII – Formal Approval</i>	 33
 <i>Appendix A - List of Acronyms</i>	 34

SECTION I – Overview and PIA Initiation

Government Institution: Public Safety Canada

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the <i>Privacy Act</i>
Director General, Government Operations Centre	Assistant Deputy Minister, Emergency Management and Regional Operations

Name of Program or Activity of the Government Institution:

Government Operations Centre – Collection of Personal Information

Description of Program or Activity:

1.4 Emergency Management

Without an all-hazards emergency management program, Canadians would be more vulnerable to a range of threats and disasters, and FPT governments would be unable to plan for, and respond to, emergencies in a coordinated and systemic manner. Public Safety Canada works to protect Canada and Canadians by providing national leadership and setting a clear direction for emergency management and critical infrastructure protection for the Government of Canada, as stipulated in the Emergency Management Act of 2007. This is achieved through emergency management policy and planning, provision of training and exercises, and research activities that support a unified emergency management system. The Department develops and maintains the federal government's capacity to manage emergencies; monitors and coordinates the federal response; and provides support to provinces and territories when federal assistance is needed. The Department also promotes public awareness of emergency management directly to Canadian citizens and businesses. Working closely with international counterparts, federal departments, provinces, territories, the first responder community and industry, to address all hazards (natural, technological and human induced), this program activity aims to foster a safe and resilient Canada through policy and program coordination across the four pillars of emergency management: prevention/mitigation, preparedness, response and recovery.

1.4.2 Emergency Response and Recovery

When provincial and territorial government resources are insufficient to respond to and/or recover from a large-scale natural or human-induced disaster, Public Safety Canada coordinates the federal response to the provincial or territorial government requesting assistance and may provide financial assistance. Our network of Regional Offices across Canada serve as the Department's primary link to provincial and territorial emergency management counterparts, as well as federal departments in the region to ensure a whole-of-government response. An integrated federal response to events of national significance is supported through 24/7 watch and early warning, national-level situational awareness, integrated risk assessment, response planning, whole-

of-government response management and support to senior officials' decision making. These services are provided to the Government of Canada and response organizations at the federal, provincial and territorial levels.

1.4.2.1 Emergency Management Coordination

This program delivers an all-hazard integrated federal emergency response to potential or actual disasters (natural or human-induced) that threaten the safety and security of Canadians across all regions, or the integrity of Canada's critical infrastructure. The program is delivered through the Government Operations Centre (GOC), a facility that provides strategic-level response coordination on behalf of the Government of Canada, in response to potential and occurring events affecting the national interest. This program continuously provides 24/7 watch and early warning for Government in support of partner mandates. The GOC provides definitive national-level situational awareness (e.g. Notifications, Situation Reports, intelligence products, briefings) to partners and senior decision makers, and to senior officials, provincial governments and/or the private sector. The GOC ensures whole-of-government response capability, plans for and coordinates the federal response to incidents, develops recommendations for the deployment and utilization of federal resources, and actions requests for emergency assistance from federal or provincial authorities. Working with the provinces and territories and international partners, the GOC is a key asset for DM and ADM communities, providing them with a mechanism for the implementation of their direction, keeping senior officials informed of evolving events, as well as identifying issues that need their engagement for resolution. The GOC improves the efficient use of Government of Canada strategic assets, and when offered, the resources of P/T governments. This program also aligns the work of regional offices with national efforts to support provincial and territorial partners in addressing emergencies.

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:

Emergency Management Operations

Description: Information on Government of Canada operational emergency response capabilities and programs including information pertaining to the Federal Emergency Response Plan, the National Emergency Response System, the Government Operations Centre (GOC) and the Canadian Cyber Incident Response Centre (CCIRC). Under this program, the GOC delivers an all-hazard integrated federal emergency response to events in the national interest. It provides 24/7 monitoring and reporting, national-level situational awareness, integrated risk assessments and warning products, as well as national-level planning and whole-of-government response management. In parallel and in collaboration with the GOC, CCIRC focuses on operational-level, cyber-only whole-of-government response.

Document Types: Memorandums, briefing notes and books, Question Period notes, reports, plans, presentations, evaluations, agreements, procedures, policies, maps, emails, lists, agendas, records of decision, letters, contracts and requests for proposals.

Class of Record Number: PS EMNS 050

- ☐ Proposal for a New Personal Information Bank
☐ Proposal to modify an existing personal information bank - PIB registration number and current description:

- ☐ New Class of Personal Information
☐ Proposed new Standard Personal Information Bank
☐ Proposal to Modify an Existing Personal Information Bank - Standard PIB number and current description:

Legal Authority for Program or Activity:

The Government Operations Centre's (GOC) legal authority is based on the:

- (1) *Department of Public Safety and Emergency Preparedness Act* (DPSEPA);
(2) *Emergency Management Act* (EMA);

Section 4 and 6 of the DPSEPA gives the Minister of Public Safety and Emergency Preparedness broad powers, duties and functions relating to public safety and emergency preparedness.

In addition, sections 3, 4 and 5 of the EMA set out the responsibilities of the Minister in relation to emergency management. These responsibilities, among others, include (1) monitoring potential or actual emergencies and advising ministers accordingly; (2) establishing policies and programs related to emergency management; (3) facilitating the authorized sharing of information in order to enhance emergency management; (4) coordinating the Government of Canada's response to an emergency; and (5) participating in international emergency management activities including developing joint plans with the United States.

When applying these authorities in an operational setting, the GOC, in some limited instances, receives personal information during the course of performing its mandated functions.

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

Summary of the project / initiative / change:

Under the authority of the EMA, the principal means by which the Minister of Public Safety exercises leadership for federal emergency management is through the Government Operations Centre (GOC). On behalf of the Government of Canada, the GOC ensures Canadians are better protected from major disasters, accidents and intentional acts by supporting response coordination of events affecting the national interest. The GOC provides 24/7 monitoring and reporting, national-level situational awareness, warning products and integrated risk assessments, national-level response protocols, and whole-of-government response management.

In fulfilling these EMA-mandated coordination responsibilities, the GOC works with all federal government institutions, provinces and territories, and, if required by the nature of the event, international partners. While

most events coordinated by the GOC do not require the collection of personal information, occasionally certain types of events such as large-scale evacuations or repatriation of Canadians and their families from disaster-stricken areas abroad, necessitate the collection of some personal information. Examples of this type of incidental collection are evacuee/repatriation manifest lists during the Lebanon evacuation of 2006 and the Haitian earthquake of 2010. Collection of personal information during these kinds of events by the federal government enables other government institutions (usually provinces/territories) to swiftly prepare appropriate emergency reception, medical care, housing, social services and resettlement arrangements for evacuees.

Note: Short description of the institutions business objectives, project objectives, project / initiative / change scope, product scope, stakeholders and assumptions.

SECTION II – Risk Area Identification & Categorization

Type of Program or Activity	Level of Risk to Privacy
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

Type of Personal Information Involved and Context	Level of risk to privacy
Only personal information provided by the individual – at the time of collection – relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities. The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.	☐ 1
Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.	☐ 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 For example: the personal information by association indirectly reveals information on the health, financial situation, religious or lifestyle choices 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. For example: the personal information by association indirectly reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and other individuals, such as relatives.	☐ 4

Program or Activity Partners and Private Sector Involvement	Level of risk to privacy
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

Duration of the Program or Activity	Level of risk to privacy
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

Program Population	Level of risk to privacy
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

Technology & Privacy	Risk to privacy
Does the new or modified program or activity involve the implementation of a <u>new electronic system</u> , 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
Does the new or modified program or activity require any modifications to <u>IT legacy systems</u> and / or services?	☐ YES ☒ NO
The new or modified program or activity involve the implementation of one or more of the following technologies:	

- 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). Identify the applicable category(ies): 	☐ YES ☒ NO
- 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... Identify the applicable category(ies): 	☐ YES ☒ NO
- Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the Directive on PIA, government institution 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 behavior. Identify the applicable category(ies): 	☐ YES ☒ NO
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.	

Personal Information Transmission	Level of risk to privacy
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

Risk Impact to the Institution	Level of risk to privacy
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. Decrease confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the <u>Government of Canada Outcome areas</u> .	☐ 4

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

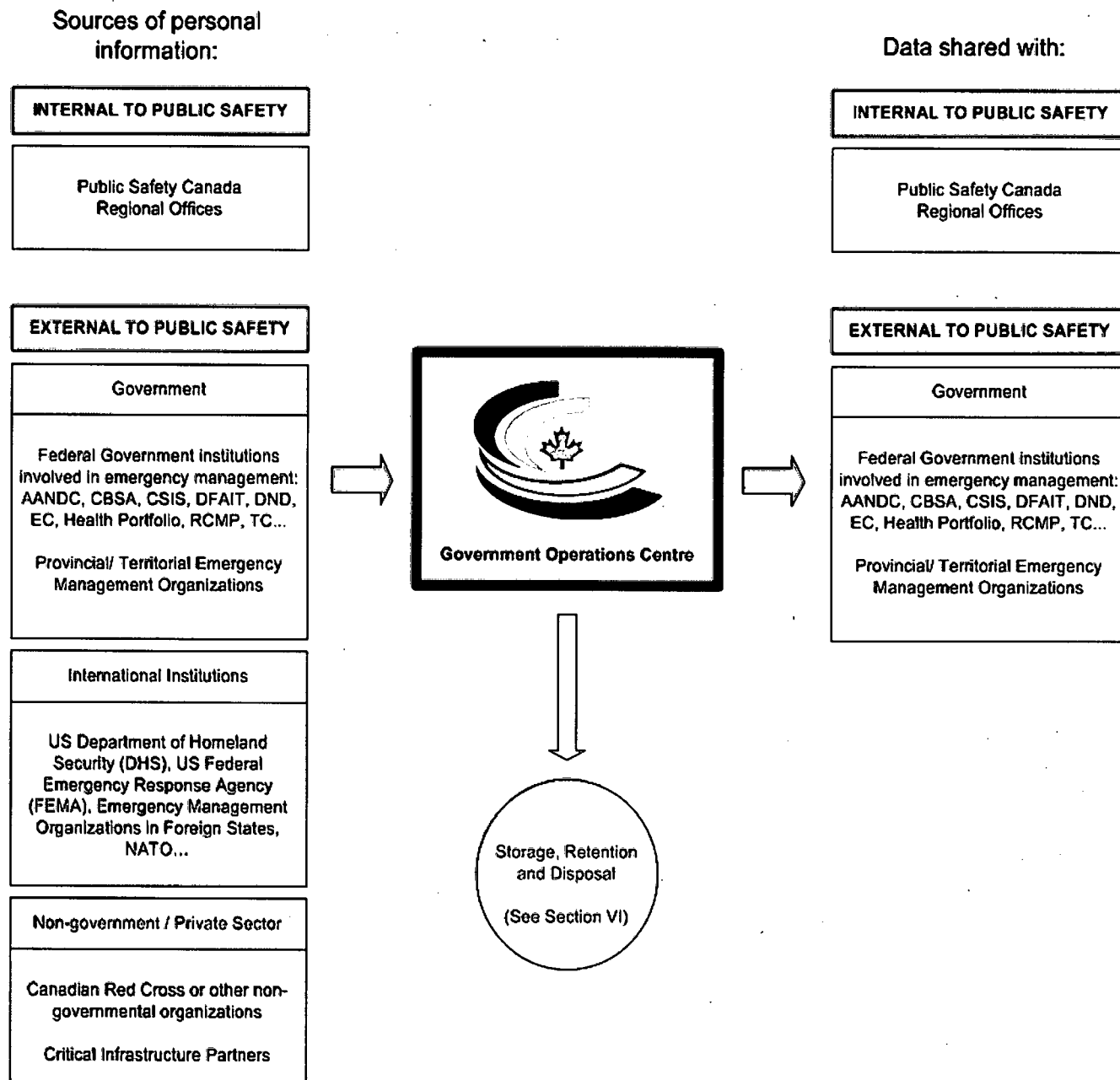
SECTION III – Analysis of Personal Information Elements

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 is identified as a potential privacy risk (level 2-3-4) in the Risk Area Identification and Categorization.

Define each element of personal information collected	Define sub-elements of personal information associated with the element identified in the first column	How is the personal information recorded?
1) Name 2) Nationality 3) Date of Birth 4) Address 5) Passport Number 6) Emergency Medical Conditions/ Injuries / Special Needs 7) Contact details 8) Health Insurance	1) First / middle / last name 2) Citizenship, Canadian or other 3) Day / month / year 4) Street address / city / province / postal code / country 5) Passport number / place of birth 6) Basic injuries, medical conditions, or special needs requiring immediate attention for persons being moved/evacuated from a disaster area 7) Phone numbers / email addresses 8) Health card number	☒ Paper ☒ Electronic ☒ Audio Recordings ☐ Visual Image Recordings ☐ Human Biological Samples ☐ Other (Specify)

SECTION IV – Flow of Personal Information



For an explanation of the acronyms above, please see **Appendix A – List of Acronyms**

Source of the personal information for the program or activity:

The source is the organization from which the personal information was collected. As there can be more than one source, all possible sources are identified.

SOURCE	DETAILS <i>(including Info Source Information)</i>
Federal Government - Internal to Public Safety	
Public Safety Canada Regional Offices (PS RO)	
Federal Government - External to Public Safety	
Aboriginal Affairs and Northern Development Canada (AANDC), formerly Indian and Northern Affairs Canada (INAC)	Emergency Management Assistance Program (INA DMO 090)
Canada Border Services Agency (CBSA)	National Risk Assessment Centre (NRAC) (CBSA PRO 001, CBSA IST 001, CBSA PPU 008)
Canadian Security and Intelligence Service (CSIS)	Passenger Protect Program, Security Screening (CSIS PPU 070, CSIS DDS 052)
Department of Foreign Affairs and International Trade (DFAIT)	Emergency Watch and Response Centre (DFAIT PPU 010, DFAIT CLD 917, DFAIT CED 908, DFAIT CLD 918)
National Defence (DND)	International Disaster Relief and Humanitarian Response Operations, Search and Rescue, Situational Awareness, CSE Foreign Intelligence Files (DND PPB 140, DND ADO 275, DND PPU 050, DND MIS 080, DND PPU 040)
Environment Canada (EC)	Environmental Emergencies (EC SMW 313)
Health Portfolio (HC and PHAC)	Health Portfolio Emergency Operations Centre (PHAC 010 0048)
Royal Canadian Mounted Police (RCMP)	National Operations Centre (NOC) (RCMP OPS 002, RCMP PPU 011)
Transport Canada (TC)	Transport Canada Situation Centre (TC ASA 001, TC ASE 001, TC HRM 002)
Non-federal Government	
Provincial/Territorial Government	Emergency Management Organizations

International	
Foreign State	U.S. Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security (DHS)
International Organization	NATO, United Nations
Private Sector	
Non-governmental Organization or Charity	Canadian Red Cross, St. John's Ambulance (information would usually be reported through the province/territory)

Internal use and disclosure

The location where the information will circulate within the federal organization, including related programs.

The personal information collected through the Government Operations Centre (GOC) may be sent to the Public Safety Canada Regional Offices (PS RO) to be further disseminated as needed to provincial/ territorial authorities. The PS ROs operate under the same framework of emergency management and for the purposes of using personal information, have the same mandate as the GOC to support response coordination of events affecting the national interest. Neither the GOC nor the PS ROs directly use the personal information collected.

Program	
Government Operations Centre	Emergency Management Operations (PS EMNS 050)

External Use and Disclosure

The organizations to which personal information could be disclosed under this program.

Federal Government - Internal to Public Safety	
Public Safety Canada Regional Offices (PS RO)	
Federal Government - External to Public Safety	
Aboriginal Affairs and Northern Development Canada (AANDC), formerly Indian and Northern Affairs Canada (INAC)	Emergency Management Assistance Program (INA DMO 090)
Canada Border Services Agency (CBSA)	National Risk Assessment Centre (NRAC) (CBSA PRO 001, CBSA IST 001, CBSA PPU 008)
Canadian Security and Intelligence Service (CSIS)	Passenger Protect Program, Security Screening (CSIS PPU 070, CSIS DDS 052)
Department of Foreign Affairs and International	Emergency Watch and Response Centre

Trade (DFAIT)	(DFAIT PPU 010, DFAIT CLD 917, DFAIT CED 908, DFAIT CLD 918)
National Defence (DND)	International Disaster Relief and Humanitarian Response Operations, Search and Rescue, Situational Awareness, CSE Foreign Intelligence Files (DND PPB 140, DND ADO 275, DND PPU 050, DND MIS 080, DND PPU 040)
Environment Canada (EC)	Environmental Emergencies (EC SMW 313)
Health Portfolio (HC and PHAC)	Health Portfolio Emergency Operations Centre (PHAC 010 0048)
Royal Canadian Mounted Police (RCMP)	National Operations Centre (NOC) (RCMP OPS 002, RCMP PPU 011)
Transport Canada (TC)	Transport Canada Situation Centre (TC ASA 001, TC ASE 001, TC HRM 002)
Non-federal Government	
Provincial/Territorial Government	Emergency Management Organizations

Retention / Storage

The organizations that will store the personal information including duplicates or backups of databases.

The GOC cannot confirm which, if any, organizations store the information beyond the termination of the incident or emergency event being managed. Because the GOC itself does not use the personal information for any administrative purpose, it is not retained after an incident is closed. The GOC expects that organizations receiving personal information will handle, store, and dispose of it in accordance with all applicable legislation. When necessary, the GOC also places restrictions on the distribution of information through the use of its dissemination levels system for other organizations (See Section VII – Dissemination Levels). Information distributed by the GOC will indicate to relevant organizations if and to what extent the information may be shared internally and externally.

Access to Information

The organizations that can access or handle personal information collected for the program or activity. Locations and approximate sizes of groups are given where available.

Federal government Institution responsible for program or activity:		
Groups, Areas, Divisions	Positions who have access to or use the personal information *	Geographical Location
Government Operations Centre (GOC)	Approximately 35 individuals	National Capital Region
Public Safety Canada's Regional Offices (PS RO)	Approximately 50-75 individuals	Vancouver, Winnipeg, Toronto, Montreal, Dartmouth

Other federal government Institution responsible for program or activity:		
Aboriginal Affairs and Northern Development Canada (AANDC), formerly Indian and Northern Affairs Canada (INAC)	Unknown	National Capital Region
Canada Border Services Agency (CBSA)	Unknown	National Capital Region
Canadian Security and Intelligence Service (CSIS)	Unknown	National Capital Region
Department of Foreign Affairs and International Trade (DFAIT)	Unknown	National Capital Region
National Defence (DND)	Unknown	National Capital Region
Environment Canada (EC)	Unknown	National Capital Region
Health Portfolio (HC and PHAC)	Unknown	National Capital Region
Royal Canadian Mounted Police (RCMP)	Unknown	National Capital Region
Transport Canada (TC)	Unknown	National Capital Region
Non-federal institution or private sector:		
Provincial/Territorial Government – Emergency Management Organization (EMO)	Unknown	Across Canada
Municipal Government	Unknown	Across Canada
Aboriginal Government/ Council	Unknown	Across Canada

* It is important to note that not all positions/groups listed in this column will have access to the personal information collected for a particular response. This is the number of people who potentially have access to information, depending on the nature of the incident or event.

SECTION V – Privacy Compliance Analysis

Collection Authority (Section 4 of the *Privacy Act*)

1. Has each element and sub-elements of personal information collected or to be collected been justified in terms of its necessity to the administration of the program or activity? <u>Note:</u> "Necessary" is a higher standard than merely being useful.	☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Review the proposed personal information elements and sub-elements outlined in the Personal information Analysis section to determine which pieces are "necessary" and not merely useful. Document any changes.
2. Is the Social insurance Number (SIN) being collected?	☐ YES ☒ NO	If YES Please state the legal and policy authority: Action Required to Support Legal & Policy Compliance in the absence of legal and policy authority to collect the SIN: ☐ Establish explicit legislative authority through legislative amendments. ☐ Establish legal and policy authority as outlined in the <i>Directive on SIN</i>.

Direct Collection – Informed of Purpose (Section 5 of the *Privacy Act*)

3. Is the information collected directly from the individual?	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Draft a detailed 'Privacy Notice' that integrates the required elements outlined below ☐ Integrate to the 'Privacy Notice', as appropriate, a request for consent for uses and disclosures that are not directly related to the purpose of the collection. The request for consent must include the required elements outlined in the <i>Directive on Privacy Practices</i>. The privacy notice must state all of the following: ☐ The purpose and authority for the collection; ☐ Any uses or disclosures that are consistent with
--	--	--

	the original purpose; ☐ Any uses or disclosures that are not related to the original purpose; ☐ Any legal or administrative consequences for refusing to provide the personal information; and ☐ The rights of access to, correction of and protection of personal information under the <i>Privacy Act</i>. *Adapting the privacy notice for either written or verbal communication at the time of collection. Written notices are to include a reference to the PIB described in Info Source. The Consent Form must state all of the following: ☐ The purpose of the consent and the specific personal information involved; ☐ The sources who will be asked to provide the information, in the case of indirect collections; ☐ Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought; ☐ Any consequences that may result from withholding consent; and ☐ Any alternatives to providing consent. Note: The above is supplementary to the information in the privacy notice. If NO ☒ Ensure that the requirements stated at Question 5 are met. <u>Policy requirement:</u> A detailed "Privacy Notice" is required where personal information is collected for an administrative purpose. <u>Legal Consideration:</u> Section 10 of the <i>Privacy Regulations</i> provides for the rights or actions under the act to be exercised or performed on behalf of a minor, an incompetent person, a deceased person or a person authorized by law to administer the affairs of that person.
--	---

4. Is the information collected from another source with informed consent of the individual?	☒ YES ☐ NO	If NO — or if YES and NO ☐ Ensure that the requirements stated at Question 3 are met. <u>Policy requirement:</u> Inform the individual of what information will be collected, how the information will be used and what source will be asked to provide the information. Individuals should also be informed of any alternatives or consequences that may result from their refusal to authorize any indirect collection. Written authorization from the individual to whom the personal information pertains is required. Collection of personal information from another source may be required in order to ensure that the personal information is accurate and up-to-date. See Question 8 regarding accuracy requirements.
5. Is the information collected from another source without notice to or consent from the individual? - Is the collection a result of a disclosure under subsection 8(2) of the Act? - Would direct notification of the individual result in the collection of inaccurate information? - Would direct notification of the individual defeat the purpose or prejudice the use for which the information is collected? - Is the information used for a non-administrative decision about the individual?	☒ YES ☐ NO ☐ YES ☒ NO ☐ YES ☒ NO ☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that the personal information bank's description adequately reflects the nature of such activities. ➤ Comment: The GOC is a non-administrative program, and as such, a personal information bank is not required. The GOC ensures that the Info Source accurately reflects the GOC's use of personal information by way of class of personal information. If NO Action Required to Support Legal & Policy Compliance: ☐ Direct collection must be adopted and the individual must be notified of the purpose of the collection. ☐ Ensure that the requirements stated at Question 3 are met. ➤ Comment: Direct collection and notification is not applicable. ➤ Information cannot be directly collected since the GOC has no direct contact with individuals affected by an emergency, disaster or security incident. The information is collected by authorities directly involved in responding to an incident at the "ground level."

		➤ In addition, it is not feasible to notify individuals about the purpose of collection due to the emergency nature of the situation. Events such as evacuations occur rapidly and often there is no possible way to establish contact. Moreover, the numbers of affected individuals would most likely overwhelm the resources of the GOC. Policy principle The exception to direct collection should be used sparingly. It is primarily intended for use by investigative bodies in those circumstances where direct collection would jeopardize the investigation.
6. Will the personal information collected only be used for: • The purpose for which it was collected or a purpose consistent with that purpose? • A purpose consistent with section 8(2) of the Act?	☒ YES ☐ NO ☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Identify all secondary purposes in the PIB description (i.e. other uses within the department or by another federal/provincial institution that has authority to collect the information). ☐ Integrate in the 'Privacy Notice', as appropriate, a listing for uses and disclosures that are not directly related to the purpose of the collection or consistent with that purpose. ☐ Ensure that the requirements stated at Questions 4 or 5 are met. Policy requirement Inform the individual at the time of collection of any intended uses or disclosures that are not directly related to the program or activity for which the information is being collected. (This would be considered an indirect collection by other programs.) Policy Requirement Ensuring that individuals are notified in advance of follow-up activities including all means of communication to be expected by the government institution. The individuals will be in a position to recognize legitimate requests for personal information. This will help minimize the risk of individuals providing their personal information under a false pretext.
Retention (Section 6 of the Privacy Act)		
7. Is the personal information being used to make a decision or as part of a process to make a decision that directly affects an identifiable individual? This	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Prepare and obtain approval for a retention

includes use for verification/ authentication purposes.	schedule based on your legal requirements and operational needs; AND ☐ Retain records for a minimum of 2 years as required by the <i>Privacy Regulations</i>; OR ☐ Obtain consent of the individual to dispose of the personal information earlier than the minimum 2 year retention period; AND ☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. If NO Action Required to Support Legal & Policy Compliance: ☐ Ensure that the policy requirements for Non- Administrative Privacy Protocol, outlined in the <i>Policy on Privacy Protection</i> are followed. ➤ Public Safety Canada's Non-Administrative Privacy Protocol is in the approval stages. In the meantime, information is retrieved and treated in accordance with the <i>Privacy Act</i>. ☐ Prepare and obtain approval for a retention schedule based on your legal requirements and operational needs. ➤ Since the personal information collected is transitory in nature, the GOC does not retain it beyond the termination of an incident. ☐ Obtain a Record Disposition Authority from the Librarian and Archivist of Canada. ➤ Since the personal information collected is transitory in nature, the GOC is not required to obtain a disposition authority. The GOC is responsible for determining appropriate retention time and subsequently disposing of the information in accordance with departmental standards. This time may vary based on the type of incident being responded to. <u>Policy requirement</u> Retain personal information for a minimum of two years, as detailed in section 4 of the <i>Privacy Regulations</i>. In accordance with the <i>Library and Archives of Canada Act</i>, only the Librarian and Archivist of Canada may authorize the disposition of government records by issuing Records
--	--

		Disposition Authorities (RDA).
--	--	--------------------------------

Accuracy – (Section 6 (2) of the <i>Privacy Act</i>)		
8. What measures will be taken to ensure that the personal information used in administrative decisions is accurate, up-to-date and complete? (More than one option may apply) - Direct collection or validation with the individual. - Technological means to identify keystroke errors and discrepancies. - Personal information matching program to verify personal information integrity against a "reliable source" where authorized or where consent was obtained. - In cases where direct collection or consent is not feasible, obtain information from trusted sources (either public or private) and verify accuracy against existing personal information before use. If Other – please define below:	☐ YES ☐ YES ☐ YES ☐ YES ☐ YES ☐ YES	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that, if applicable, your institution's PIB mentions the use of periodic personal information matching as a consistent use. If NO Please provide details as to why reasonable steps cannot be used. ➤ Not applicable <u>Legal and Policy Requirements</u> Subsection 6(2) of the <i>Privacy Act</i> requires government institutions to take <i>all reasonable steps</i> to ensure that personal information that they use for an administrative purpose is as accurate, up-to-date and complete as possible. Decisions that directly affect individuals must be made on the basis of accurate, up-to-date and complete information as possible. If periodic personal information matching occurs for the purposes of ensuring accuracy of information, institutions must reflect this under the "consistent use" section of the relevant PIB.

Use (Section 7 of the <i>Privacy Act</i>)		
9. Is there an activity log attached to the personal information record to record uses not described in the Personal Information Bank (Info Source)?	☒ YES ☐ NO	If YES Action Required to Support Legal & Policy Compliance: ☒ An activity log is attached to personal information records when used for consistent but unreported use. ➤ The GOC maintains a detailed duty and information log that details how information is used and exactly where and

		when it is disclosed. Should use of personal information outside the scope of the PIA occurs, it is reported to the departmental ATIP Coordinator. The ATIP Coordinator ensures that the Privacy Commissioner and TBS are advised and, if necessary, updates the GOC's description of information use on Info Source. ☒ The Privacy Commissioner is advised of this consistent use. ☒ The PIB description is amended, in time for the next edition of Info Source, to include the unreported use. If NO Action Required to Support Legal & Policy Compliance: ☐ Institutions must put in place a means to record and identify uses that were not described in the Personal Information Bank. Legal Requirements: Section 9(4) of the <i>Privacy Act</i> requires a government institution to report to the Privacy Commissioner any consistent use of personal information that has not been included in the Index, and to ensure that the use is included in the next statement of consistent uses set forth in the next edition of the Index. Policy Requirement If personal information used for a consistent purpose that is not identified in a personal information bank – the head of the institution or delegate must notify the Privacy Commissioner
Disclosure (Section 8 of the <i>Privacy Act</i>)		
10. Are processes in place to ensure that personal information will only be disclosed to individuals within and without the government institution who have a "need to know" and that there are adequate privacy practices to ensure the confidentiality and integrity of the personal information? This includes procedures to prevent against loss or theft. This covers the entire lifecycle of the	☒ YES ☐ NO	If NO Action Required to Support Legal & Policy Compliance: ☐ Ensure that the requirements stated at Question 11 are met by the receiving institution. Policy requirement Government institutions are to ensure that adequate safeguards are in place when disclosing information. This includes having an action plan for privacy breaches (unauthorized disclosures) and measures (physical, logical, administrative) to ensure that only the people that "need to know" have access to the personal information.

personal information: • Collection • Use • Retention • Disposition. This includes disclosures to other government institutions, other levels of government, other jurisdictions, foreign governments, international organizations or private sector organizations		See Directive on Privacy Practices ➤ The GOC uses the appropriate document classification levels to ensure information is protected when disclosing to other organizations. ➤ The GOC also uses a system of dissemination levels when releasing information; this system tells the recipient group the extent to which they are allowed to share that information internally and externally to their organization. ➤ Non-federal organizations are subject to both (1) the <i>Personal Information Protection and Electronic Documents Act</i> (PIPEDA); and in some cases (2) provincial/municipal privacy legislations/regulations. As such, the GOC expects these organizations to be in compliance with these legislations/regulations and store/handle personal information accordingly. ➤ Federal organizations are subject to the <i>Privacy Act</i>, and the GOC expects these organizations to be in compliance with this legislation and handle personal information accordingly.
11. Is the disclosure of the personal information governed by: A Memorandum of understanding? ☐ YES An accord? ☐ YES An arrangement? ☐ YES A contract? ☐ YES If Other – please define below: ➤ The GOC is in the process of drafting an MOU that would govern the disclosure of personal information between the		If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure the PIB description identifies this use. ☐ Ensure that the notification or consent notice mentions this use. ☐ Ensure contractual clauses are included to protect personal information. Contracts that are established with private sector entities outline measures and provisions to address the following: ☐ Control over the personal information; ☐ Limitations on collection and handling as well

GOC and some of our regional partners who are most often the recipients of personal information from the GOC. See section VI on Risk Mitigation for further details.		as any prohibitions regarding the personal information for the purposes of the contract; ☐ Disposition of the personal information, where relevant; ☐ Administrative, technical and physical safeguards; and ☐ Obligations of other parties acting on behalf of the government institution. If NO Action Required to Support Legal & Policy Compliance: ☐ Prepare a written statement describing the nature of the information sharing and have it approved by the relevant parties. Policy on Privacy Protection Measures are to be established, when personal information is involved, to ensure that the government institution meets the requirements of the <u>Privacy Act</u> when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations. Ensure that appropriate privacy protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information. If any portion of the project (administration, service delivery, system maintenance or personal information storage) involves the use of a third-party contractor, care must be taken to ensure that institutions continue to fulfill their privacy obligations.
Technology and Privacy		
12. Will the system/software /program application employ cookies or other tracking methods to collect personal information about users and their transactions? If so, for what purposes will the collected information be used and how long will the information be retained? Please define purpose and retention period below:	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Collection and use of personal information through these means must be reflected both in the PIB description and the Privacy Notice. ☐ Technology staff who have access to personal information collected through these methods must be aware of privacy and security policy requirements.

13. Does the new or modified program or activity result in an increased ability for surveillance or monitoring of a given target population?	☐ YES ☒ NO	If YES Action Required to Support Legal & Policy Compliance: ☐ Ensure that the requirements in regards to awareness stated at Question 12 are met.
---	--	--

Privacy Considerations Related to Compliance Regulatory Investigation & Enforcement		
14. Is the legal authority for conducting compliance / regulatory investigation and enforcement the same as the legislative authority for the program or activity?	☐ YES ☐ NO ☒ N/A	If NO Action Required to Support Legal & Policy Compliance: Identify legislative authority: ☐ Ensure that the requirements stated at Questions 3 and 6 are met. ☐ Ensure the activities are listed in the PIB's description. If YES Action Required to Support Legal & Policy compliance: ☐ The activities are listed in the Privacy Notice; ☐ The activities are listed in the PIB's description. ➤ Not applicable - the GOC does not conduct investigations.

Privacy Considerations Related to Search and Seizure
15. What is the specific legal authority for conducting regulatory or criminal enforcement, surveillance or intelligence gathering? Not applicable – the GOC does not conduct investigations. Action Required to Support Legal & Policy Compliance: ☐ Request legal advice from your Legal Services Unit about compliance with section 8 of the <u>Charter of Rights and Freedoms</u>, the <u>Privacy Act</u> and other applicable acts

SECTION VI - Summary of Analysis and Risk Mitigation

Risks and Mitigation

The Government Operations Centre's (GOC) use of personal information is inherently low-risk for three reasons. First, personal information is rarely collected at the GOC. Only for exceptional and often large-scale events involving, for example, an evacuation or repatriation is personal information sometimes involved. Secondly, the GOC's use of personal information is limited solely to transmission to the appropriate partner; no analysis of personal data is necessary within the GOC. Lastly, no personal information is retained by the GOC beyond the termination of the event, because the data is not relevant to any decision making, administration, strategic objective or reporting.

Nevertheless, risks do exist for the use of personal information at the GOC in three phases: collection, storage and disclosure. These risks and the GOC's proposed mitigation strategies for each are outlined in the table below. In general, the GOC reduces risk by strengthening processes already in place, continual training, evaluation, and the implementation of lessons learned.

Collection Phase	RISK: While the GOC does not directly collect personal information, it is responsible for the acceptance of data from a trusted partner. This risk is two-fold. First, the GOC must assume that the personal information collected was done so in accordance with appropriate legislation. Secondly, there is a risk of the GOC accepting personal information that is unnecessary for operations and may have been sent by a partner either in error or with a misunderstanding of the GOC's mandate and information requirements.
	MITIGATION: To address the risk of collecting unnecessary personal information, the GOC returns to sender any personal data that may be inadvertently or mistakenly sent to the GOC. This may include, but is not limited to, replying to the email and informing the sender that the GOC does not require or want such information. Follow-ups with the organization(s) responsible may be required and are conducted when necessary. Any personal information contained in the original message is then deleted from all GOC systems, including electronic and hard-copy formats. More regular training for GOC staff on how to identify unnecessary personal information and return it to the sender is planned to increase consistency across different watch teams and ensure a standardized GOC response on this type of occurrence. In addition, an administrative note on this subject will be added to the reference tool used by watch teams. <i>Timeline for improving training on GOC's use of personal information: <u>September 2013</u></i> Dissemination levels (DL) are another means by which the GOC and its federal partners can appropriately limit the sharing of information, thus helping to reduce the risk associated with the collection of personal information. A specific DL is assigned to information by the originator and corresponds to an agreed-upon group or level for distribution. In this way, the originator has a degree of control over the spread of the information. More information on DLs can be found in Section VII.

Storage Phase	RISK: For the duration of the event, any personal information that is received by the GOC and deemed to be necessary to emergency management operations is <u>temporarily stored</u> within the GOC. This may include electronic records or hard copies. The risk in the storage phase is to the confidentiality of the personal information. Anyone with access to the operations centre or the GOC servers could theoretically view personal information. There is also a risk that the information may not be promptly deleted and may reside longer than necessary on GOC systems. MITIGATION: The risk associated with storing the personal information during an event is best mitigated if the transfer, copying, circulation, saving and printing of personal information is minimized wherever possible. While some people may need to know that certain personal data has arrived at the GOC, few, if any, GOC staff actually need to view the information itself. Emails, conversations and reports should therefore refer to but not contain the personal data. Best practice is to keep a copy of the personal information only in the format in which it was received, and transfer it to the relevant partner/organization using the same means. This mitigation strategy of keeping personal information on only one system limits access and helps reduce unnecessary diffusion. To effectively implement these practices, further training is planned for all GOC staff on handling personal information. This will take the form of a privacy briefing delivered at an all-staff meeting, followed by detailed written instructions containing the GOC's policies on personal information. As a part of this training, staff will be instructed to delete all personal information once an incident is closed. This policy will be included in the GOC staff training materials/handbook (under development), and the deletion of personal information will become a regular and required step on the checklist of closing an incident. <i>Timeline for delivering training on GOC's use of personal information: <u>September 2013</u></i> <i>Timeline for adapting the process of incident closure: <u>September 2013</u></i>
Disclosure Phase	RISK: The final risk identified for the GOC's use of personal information is the disclosure to partners for emergency management purposes. Similar to risk associated with data collection, the GOC must assume that recipients of personal information transmitted through the GOC use the data in accordance with all appropriate legislation. The GOC is also responsible for deciding to which organization or group the personal information needs to be sent. This decision carries the risk of human error or poor judgement. MITIGATION: The risk associated with the disclosure of personal information by the GOC is largely mitigated by selective targeting of groups or organizations to which the information is sent. Generally, the GOC shares its information with a large number of partners to facilitate a whole-of-government response

	and to ensure all organizations are kept informed of events. With personal information, however, it is important for watch teams to be selective in their disclosure in order to keep distribution on a need-to-know basis. As with the first two mitigation strategies, staff training on this issue will reduce risk. In addition to the careful and targeted selection of recipients of personal information, the GOC also plans to draft a Memorandum of Understanding (MOU) on the sharing of personal information to further mitigate the disclosure risk. This MOU would be signed by the GOC and by our regional partners with whom personal information is most often shared. It will contain guidelines for the use of personal information including the type of personal information that can be shared, the specific purpose for the sharing of such information, and the procedures for information transmission. Most importantly, it will clearly outline the expectation that both parties use the information in accordance with applicable federal/provincial/territorial privacy legislation. <i>Timeline for improving training on GOC's use of personal information: <u>September 2013</u></i> <i>Timeline for drafting MOUs on use of personal information: <u>December 2013</u></i> As mentioned above in the Collection Phase mitigation section, Dissemination Levels (DLs) can be used by the originator of the information to appropriately limit its sharing and distribution. This is another tool that can be used to mitigate the risk associated with information disclosure. More information on DLs can be found below in Section VII.
--	--

Policy on disposing of personal information:

Personal information that is stored electronically is destroyed appropriately according to its level of classification. At the classification "Protected B" and lower, all electronic copies of the information are deleted (including attachments to emails and saved versions), and then the computer's recycling bin is emptied. From "Protected C" up to and including Secret level, electronic information is deleted securely using an approved disk sanitization utility. IM/IT Security is contacted if assistance is required. For Top Secret systems, IM/IT Security is contacted for approved document disposal.

For paper copies at any level of classification, the approved paper shredding device is used to dispose of personal information. If there is a large quantity of paper to be shredded, classified information up to and including Secret level is packed into 1ft cubic boxes for disposal by the Records Office. A Classified Document Disposal Form (<http://infocentral/cnt/is/admn/fat-eng.aspx#fat-02>) is required, and pickup is coordinated through the mailroom. More detailed can be found here: <http://infocentral/cnt/is/admn/rcrds-ffc/dstrctn-eng.aspx>.

Photocopying of personal information, even where classification levels allow, is avoided except when absolutely necessary, to limit the diffusion of the information.

More information on document disposal can be found at the following link for Transmission, Storage and Destruction of Designated and Classified Information: <http://infocentrale/cnt/is/sec/fl/tsd-eng.pdf>.

SECTION VII – Supplementary Documents List

Federal Departments and Agencies - Dissemination Levels

Guidelines for Information Sharing and Reporting Among Federal Operations Centre

Federal Operations Centres Working Group

Date of Issue: 09 Dec 2011

Version 1.0

(Excerpt)

USE OF DISSEMINATION LEVELS

The Primary Department/originator should inform the GOC and other supporting Departments of any limitations on the further dissemination of any correspondence. There are five dissemination levels:

- a. DL – 1 - *Releasable to Critical Infrastructure Partners and the Public. This level would apply to information that is suitable for release CI Partners and the public. Level 1 assumes that distribution may still be limited and will be tailored for private partners and the public.*
- b. DL – 2 - *Releasable to All Federal Departments and Agencies. This level would apply to information that is suitable for release to all Federal Departments/Agencies and supporting organizations;*
- c. DL – 3 - *Releasable to Authorized Organizations and Key Decision-Makers. This level would apply to information that is required by authorized organizations/GOC and key decision-makers at all levels to determine the appropriate preventative and/or protective measures to mitigate against known threats. Level 3 assumes that distribution is limited;*
- d. DL – 4 - *Releasable to Authorized Federal Organizations. This level would apply to information that is suitable for release to specific federal organizations and the GOC (see note below). Level 4 assumes that distribution is authorized for select key partners with the necessary need to know; and*
- e. DL – 5 - *No Further Dissemination Authorized. This level is designated for information releasable internally within the department/agency. Level 5 is the most restrictive level and would be applied to the most sensitive information. Level 5 assumes that only limited distribution is authorized based on strict need to know.*

All departments/agencies must follow the directions in any report containing a dissemination level. If the GOC or another department/agency feels that there are additional government departments that need to be informed, then the department holding the information must seek approval from the originator prior to disseminating any further. Any changes to a dissemination level should be communicated as soon as possible so that the information flows as efficiently as possible.

SECTION VIII – 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 core PIA as they relate to the administration of the identified program or activity.



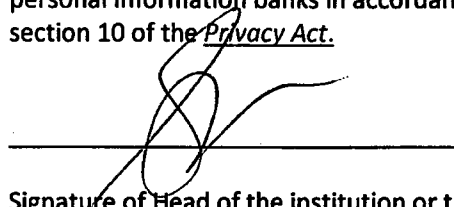
Signature of PIA lead for program or activity (DG or senior official with functional authority for program)

MAY 01 2013

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.



Signature of Head of the institution or the delegate responsible for Section 10 under the Privacy Act (ADM or other delegated authority)

MAY 02 2013

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

Appendix A - List of Acronyms

Acronym	English	Français	Acronyme
	Definition	Définition	
AAFC	Agriculture and Agri-Foods Canada	Agriculture et Agroalimentaire Canada	AAC
AANDC	Aboriginal Affairs and Northern Development Canada	Affaires autochtones et Développement du Nord Canada	AADNC
ADM	Assistant Deputy Minister	Sous-ministre adjoint/e	SMA
ATIP	Access to Information and Privacy	Accès à l'information et protection des renseignements personnels	AIPRP
CBSA	Canada Border Services Agency	Agence des services frontaliers du Canada	ASFC
CCG	Canadian Coast Guard	Garde côtière canadienne	GCC
CCIRC	Canadian Cyber Incident Response Centre (@PS)	Centre Canadien de réponse aux incidents cybernétiques (@SP)	CCRIC
CFIA	Canadian Food Inspection Agency	Agence canadienne d'inspection des aliments	ACIA
CHC	Canadian Hurricane Centre	Centre canadien de prévision d'ouragan	CCPO
CIC	Citizenship and Immigration Canada	Citoyenneté et Immigration Canada	CIC
CIDA	Canadian International Development Agency	Agence canadienne de développement international	ACDI
CNSC	Canadian Nuclear Safety Commission	Commission canadienne de sûreté nucléaire	CCSN
CRA	Canada Revenue Agency	Agence du revenu du Canada	ARC
CRC	Canadian Red Cross	Croix-Rouge canadienne	CRC
CSC	Correctional Service of Canada	Service correctionnel du Canada	SCC
CSE	Communications Security Establishment	Centre de la sécurité des télécommunications	CST
CSIS	Canadian Security Intelligence Service	Service canadien du renseignement de sécurité	SCRS
DFAIT	Department of Foreign Affairs and International Trade	Ministère des Affaires étrangères et du Commerce international	MAECI
DFO	Fisheries and Oceans Canada	Pêches et Océans Canada	MPO

English		Français	
Acronym	Definition	Définition	Acronyme
DG	Director General	Directeur général / Directrice générale	DG
DL	Dissemination Level	Niveau de diffusion	ND
DM	Deputy Minister	Sous-ministre	SM
DND	Department of National Defence	Ministère de la Défense nationale	MDN
DoJ	Department of Justice	Ministère de la Justice	MJ
EC	Environment Canada	Environnement Canada	EC
EM	Emergency Management	Gestion des urgences	GU
EMA	<i>Emergency Management Act</i>	Loi sur la gestion des urgences	LGU
EMRO	Emergency Management and Regional Operations (@PS)	Gestion des mesures d'urgence et opérations régionales (@SP)	GMUOR
FERP	Federal Emergency Response Plan	Plan fédéral d'intervention d'urgence	PFIU
GC	Government of Canada	Gouvernement du Canada	GC
GOC	Government Operation Centre	Centre des opérations du gouvernement	COG
HC	Health Canada	Santé Canada	SC
HP	Health Portfolio (HC, PHAC, & Emergency Operations centre @HC)	Portefeuille de la Santé (SC, ASPC, et COU @SC)	
IM	Information Management	Gestion de l'information	GI
MOA	Memorandum of Agreement	Protocole d'entente	PE
MOU	Memorandum of Understanding	Protocole d'entente	PE
NERS	National Emergency Response System	Système national d'intervention d'urgence	SNIU
NGO	Non-Governmental Organization	Organisation non gouvernementale	ONG
NPB	National Parole Board	Commission des libérations conditionnelles du Canada	CLCC

Acronym	English	Français	Acronyme
	Definition	Définition	
NRC	National Research Council of Canada	Conseil national de recherches Canada	CNRC
NRCan	Natural Resources Canada	Ressources naturelles Canada	RNCan
NSERC	Natural Sciences and Engineering Research Council	Conseil de recherches en sciences naturelles et en génie	CRSNG
OGD	Other government department	Autres ministères du gouvernement	AMG
Opscen	Operations Centre	Centre des opérations	Opscen
PCO	Privy Council Office	Bureau du Conseil privé	BCP
PHAC	Public Health Agency of Canada	Agence de la santé publique du Canada	ASPC
PMO	Prime Minister's Office	Cabinet du Premier ministre	CPM
PS	Public Safety Canada	Sécurité publique Canada	SP
PSEPC	Public Safety and Emergency Preparedness Canada (former name for PS)	Sécurité publique et Protection civile Canada (ancien nom de SP)	SPPCC
PWGSC	Public Works and Government Services Canada	Travaux publics et Services gouvernementaux Canada	TPSGC
RCMP	Royal Canadian Mounted Police	Gendarmerie royale du Canada	GRC
RO	Regional Office	Bureau régional	BR
TBS	Treasury Board of Canada Secretariat	Secrétariat du Conseil du Trésor	SCT
TC	Transport Canada	Transports Canada	TC

Page 146

**is withheld pursuant to section
est retenue en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 147

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 148

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 149 to / à 150
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

Page 151

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 152 to / à 153
are withheld pursuant to section
sont retenues en vertu de l'article

of the Access to Information
de la Loi sur l'accès à l'information

Page 154

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 155 to / à 156
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

Pages 157 to / à 159
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

Pages 160 to / à 161
are withheld pursuant to section
sont retenues en vertu de l'article

of the Access to Information
de la Loi sur l'accès à l'information

Pages 162 to / à 163
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

Page 164

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 165

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 166 to / à 167
are withheld pursuant to section
sont retenues en vertu de l'article

of the Access to Information
de la Loi sur l'accès à l'information

**Pages 168 to / à 169
are withheld pursuant to sections
sont retenues en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 170 to / à 174
are withheld pursuant to section
sont retenues en vertu de l'article

of the Access to Information
de la Loi sur l'accès à l'information

Page 175

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 176

**is withheld pursuant to section
est retenue en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 177

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 178

**is withheld pursuant to section
est retenue en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 179

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 180 to / à 188
are withheld pursuant to section
sont retenues en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Page 189

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 190 to / à 192
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

Page 193

**is withheld pursuant to sections
est retenue en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 194 to / à 199
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

**Pages 200 to / à 209
are withheld pursuant to sections
sont retenues en vertu des articles**

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 210 to / à 212
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information

Pages 213 to / à 234
are withheld pursuant to sections
sont retenues en vertu des articles

of the Access to Information
de la Loi sur l'accès à l'information