Office of the
Privacy Commissioner
of Canada

A GUIDE FOR SUBMITTING PRIVACY IMPACT ASSESSMENTS TO THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

Expectations

TABLE OF CONTENTS

1. THE PIA PROCESS

A Privacy Impact Assessment (PIA) is a process that helps determine whether initiatives involving the use of personal information raise privacy risks, measures, describes and quantifies these risks, and proposes solutions to eliminate or mitigate privacy risks to an acceptable level. The Canadian government has been an international pioneer in the use of PIAs as a tool to ensure privacy is considered in the development of programs and initiatives. In 2002, the government of Canada's *Privacy Impact Assessment Policy* came into effect, requiring most federal government institutions to develop and maintain PIAs to evaluate whether program and service delivery initiatives involving the collection, use or disclosure of personal information were in compliance with privacy legislation, policies, guidelines, and best practices. More recently, as part the overall TBS Policy Suite Renewal process, and in an effort to help government institutions streamline their PIA processes, the PIA *Policy* has been replaced with a *Directive on Privacy Impact Assessment*. As did the *Policy* before it, the Directive applies to 250 government institutions listed in the schedule to the *Privacy Act*, including parent Crown corporations and any wholly owned subsidiary of these corporations. It specifically exempts the Bank of Canada.

The Directive took effect on April 1, 2010, and it is to be implemented in stages until April 1, 2011. It requires Deputy Heads to establish a PIA development and approval process, and outlines requirements for the establishment or modification of Personal Information Banks (PIBs)[1] and the completion of core PIAs for new or substantially modified programs and activities involving personal information. The core PIA includes a general description of the program or activity and its legislative authority, as well as a standardized risk assessment scale which indicates the type of personal information involved and the category of use and disclosure contemplated. It sets minimum requirements for

[1] A Personal Information Bank (PIB) is a listing of all personal information held by a government institution that has been used, is being used, or is available for use for an administrative purpose or is retrievable by a person's name, identifying number, symbol, or other individual identifier. The *Privacy Act* requires that government institutions report to the public on how this personal information is handled by publishing PIB descriptions in Info Source, which is released annually by TBS; individuals use Info Source to find out how and where their personal information is used and retained, so that they may exercise their rights of access and correction.

The intent of this document is to illuminate our process for analysing the privacy risks of government initiatives, and set out our expectations of government institutions in regard to the type and depth of information we would like to see provided for our consideration in Privacy Impact Assessment (PIA) reports. As there is no mandatory format for PIAs required by the April 2010 Treasury Board Secretariat (TBS) Directive on Privacy Impact Assessment (there is mandatory content as described in Appendix C of the Directive), institutions are free to tailor, or customize, their PIA processes and reports to allow optimal analysis of privacy risks, and to best meet obligations for privacy protections and transparency of process to Canadians. Our suggestions are intended to help institutions in this regard.

the information that must be reported to TBS in order to fulfil privacy risk management obligations. The *Directive* indicates, however, that the core PIA is only the starting point; departmental officials are also responsible for determining if further analysis, including a more comprehensive PIA, is needed.

The OPC was an early proponent of the use of PIAs as a preventative measure and fully supports their use as an important privacy risk reduction exercise and planning tool for government institutions. The OPC worked with TBS during the development of the original PIA *Policy*, and has also consulted with TBS on the new *Directive*. PIAs can reveal privacy risks and identify measures to help ensure compliance with the Act, make certain that privacy issues of public concern are resolved or mitigated, ensure accountability for the use of personal information, and provide transparency to Canadians about how their personal information is treated when in the hands of government.

PIAs give managers and decision makers the information they need to make prudent policy, program and system design choices, substantially reducing the risks of having to end or modify programs or services after implementation in order to comply with privacy requirements. Following the privacy practices outlined in the PIA process results in better managed and more effective operations, and enables Canadians to understand how government handles their personal information and to trust that this will be done responsibly.

Under the new TBS PIA *Directive*, institutions must undertake PIAs for programs and activities when:

- Personal information is used or intended to be used in a decision-making process directly affecting individuals;
- Substantial modifications are made to existing programs or activities where personal information is used or intended to be used for an administrative purpose;
- Contracting out or transferring programs or activities to another level of government or to the private sector results in substantial modifications to the program or activities.

Under these circumstances, institutions are obliged to undertake, at minimum, a core PIA, and may decide to further investigate and document privacy risks in a more in-depth assessment if institutional officials feel it is warranted. According to the *Directive*, a final copy of the approved core PIA is to be submitted to OPC at the same time that it is provided to TBS. The Directive states that TBS officials will review the core PIA only to ensure that it includes the required documentation. TBS will also review and approve the attached Personal Information Bank (PIB) descriptions to meet its obligations under the *Privacy Act*. The Directive states that TBS will not provide further comment or advice on PIAs, and will not review any documents or material that is surplus to the core PIA. However, our office will undertake comprehensive reviews of PIAs and all associated documents, and we will offer institutions our advice, comments, consultation and recommendations.

The *Directive* gives institutional officials the responsibility of determining whether the privacy risks of an initiative are serious enough to warrant supplementary documentation, deeper analysis, or greater risk mitigation strategies. It is understood that not all initiatives will require more than a core PIA in order to properly assess and mitigate privacy risks, and for these, it would not be necessary for institutions to go beyond the requirements of the core PIA. Indeed, the OPC does not itself undertake in-depth reviews of all the PIAs we receive for government initiatives using personal information. We focus our resources on initiatives that in our view, pose the greatest risks. In order to undertake our reviews of these more complex and/or intrusive initiatives, we will generally require supplementary information. The *Directive* reflects this situation, instructing institutions to provide OPC with any additional documentation that we may request. This will help us better understand the personal information risks and privacy implications of the initiative. During our review of the initiative, OPC staff may consult with institutions by telephone or via email, and may arrange meetings to ask questions and discuss our concerns. Our comments and advice are transmitted to departments in the form of letters of recommendation, to which we ask for a response.

We recognize that since the introduction of the PIA Policy in 2002, government institutions have been provided with a variety of tools and guidance documents by TBS in an effort to help them in the drafting of PIAs. These included the PIA *Guidelines*, which were based on the PIA *Policy*. The *Guidelines* gave institutions detailed advice on how to determine whether a PIA was required and included a section on how to organize PIA reports. TBS also provided a PIA e-Learning Tool, also based on the old *Policy*, for the use of federal government institutions.[2] PIAs are also meant to be informed by the *Regulations* under the *Privacy Act*, and by other privacy related TBS policies, directives and guidelines, such as the *Policy on Privacy Protection* and the *Directive on the Social Insurance Number*. It is our understanding that a user guide to help institutions with the requirements of the new *Directive* is under development by TBS. We hope that our guidance document will complement the TBS materials, while at the same time help government institutions to understand our need for additional information and our distinct role in the PIA review process. Our mandate as the guardian of the privacy rights of Canadians requires that we take a broad view of privacy risks and that we question the justification for privacy invasive programs, projects or initiatives that use Canadians' personal information. This broader scrutiny may require us to ask for a greater depth of information and analysis from institutions.

[2] See Annex B for a list of PIA tools and resources

2. OPC REVIEW OF PRIVACY IMPACT ASSESSMENTS

Since we started our PIA review function, in conjunction with the introduction of the TBS PIA Policy in 2002, OPC has analysed PIAs against the *Privacy Act* and the universal privacy and fair information practice principles of the Canadian Standards Association *Model Code for the Protection of Personal Information (the Model Code)*. These principles were also reflected in the first TBS PIA Guidelines, and formed the basis of the Policy's Privacy Analysis Questionnaire which departments were encouraged to use to guide their examination of risks. Our office will continue to refer to the principles of the *Model Code* to review PIAs received under the more streamlined *Directive*, which does not include use of the Questionnaire. While we recognize that adherence to the ten principles is not mandatory for government institutions, we promote their voluntary adoption. The principles are widely accepted and internationally recognized and provide a logical and coherent framework for privacy analysis. Our review also takes into account numerous other TBS policies and directives, as well as widely recognized best practice guidelines such as the Public Sector Chief Information Officer Council's (PSCIOC) *Personal Information sharing Agreement Guidelines* and the *Generally Accepted Privacy Principles* of the Canadian Institute of Chartered Accountants. We will first take into account, however, the necessity, proportionality and effectiveness of those government initiatives, which, in our view, pose the greatest potential risks to Canadians' privacy rights.

2.1 Using the Four-Part Test of R. v. Oakes for Necessity and Proportionality

Highly visible and controversial government programs have recently underlined the importance of ensuring that the broader privacy risks and societal implications of some initiatives are carefully evaluated at the outset. The risks of certain government programs and initiatives should be measured and assessed in the context of their potential impact on our democratic society, our civil liberties, and our fundamental human right to privacy as recognized in Canadian law, including the *Privacy Act*, the *Canadian Charter of Rights and Freedoms*, and the case law interpreting them. The *Privacy Act* sets out fundamental rights of Canadians in their interactions with the federal state. The Supreme Court of Canada has recognized on numerous occasions that privacy interests are worthy of protection under the *Charter* and has further stated that the *Privacy Act* has quasi-constitutional status.[3]

We expect federal entities undertaking PIAs for particularly intrusive or privacy invasive initiatives or technologies to first demonstrate that the activity or program is necessary to achieve a specific and legitimate purpose, that it is likely to be effective in achieving that purpose, that the intrusion

[3] *Dagg v. Canada (Minister of Finance)* [1997] 2 S.C.R. 403 *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)* [2003] 1 S.C.R. 66 *Lavigne v Canada (Office of the Commissioner of Official Languages)* [2002] 2 S.C.R. 773, and *H.J. Heinz Co. of Canada v. Canada (Attorney General)* [2006] 1 S.C.R. 441

on privacy is proportional to the benefit to be derived and that no other less privacy intrusive alternative would achieve the same purpose. To guide this analysis, we will ask government departments to answer the following four questions, which are based on the test used in *R. v. Oakes*[4] to weigh reasonable limitations on rights and freedoms in a free and democratic society:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the need?
- Is there a less privacy-invasive way of achieving the same end?

In applying this test to PIAs, we ask federal entities to establish that programs and initiatives that impinge on privacy are rationally connected to a public goal that is pressing and substantial. This should be articulated clearly and specifically, and should not be a simple reiteration of the institutional mandate, for example, "law enforcement", or "border control".

We also ask for a description of how, specifically, the proposed collection or use of personal information will meet the need as described. This entails empirical evidence in support of the initiative and precludes the collection of personal information for "just in case" scenarios or the retention of information that might be useful for yet to be determined future purposes.

Then, we ask institutions to show us how they will ensure that the collection, use and disclosure of personal information is undertaken in the least privacy invasive manner possible. This analysis should discourage the over-collection or over-sharing of information. Finally, we ask that entities consider using other, less privacy-intrusive methods, and/or other information to meet their goals, such as using anonymous or aggregate data and undertaking physical security screening in lieu of identity-based screening which requires the collection of large amounts of personal information, or using privacy protective technologies.

2.2 Using the Model Code for the Protection of Personal Information

Once the initial questions of the four-part test have been answered, and the proposed collection and use of personal information have been justified, the security of the information in the hands of government must also be demonstrated. This is where an analysis of the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association *Model Code for the Protection of Personal Information* is useful. As discussed previously, it is our view that these principles provide an accessible and logical framework for completing the privacy analysis. The OPC expects the submitted PIA to contain

[4] *R. v. Oakes* [1986] 1 S.C.R. 103

complete and accurate descriptions of how each of these principles is taken into account in the development of federal initiatives involving personal information.

The ten principles, slightly amended for pertinence to public sector, are listed below, with examples of what OPC might expect to see reflected in a PIA following each principle in italics. These examples are not exhaustive but are meant to give an indication of the type of information we are seeking as we review PIAs. A checklist for the preferred PIA format and the associated documents we generally require can be found at Annex C.

2.2.1 Accountability

A government institution is responsible for personal information under its control and shall designate an individual or individuals who are accountable for compliance with the following principles. This is also in keeping with the requirements of section 6 of the Directive on Privacy Impact Assessment, and includes responsibility for establishing a PIA development and approval process, and for establishing and modifying Personal Information Banks (PIBs) as appropriate.

A government institution is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The institution should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. This is reflected in section 6.2.10 of the TBS *Policy on Privacy Protection*, and includes the need to ensure that appropriate privacy protection clauses are included in contracts with private sector organizations, other government departments or public sector partners, and when inter-jurisdictional or transborder flows of personal information are involved.

Government institutions should implement policies and practices to give effect to the principles. This includes implementing specific procedures to protect personal information, mechanisms for complaints, for inquiries, and for recourse, training staff, and developing communications materials to explain the institution's policies and procedures in a publicly transparent manner.

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

2.2.2 Identifying Purposes

The purposes for which personal information is collected shall be identified and documented by the institution at or before the time the information is collected. Institutions must determine that the information they propose to collect is reasonable and necessary for the program or activity. This is in keeping with the *Privacy Act*, is related to the Limiting Collection principle, and is in keeping with section 5 of the TBS *Directive on Privacy Practices*.

These purposes should be specified publicly through Info Source and other reporting mechanisms, and/or directly to the individual from whom the personal information is collected. This is in keeping with section 4 of the *Privacy Act* and is referenced in the risk assessment scale of the TBS *PIA Directive*. Information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used except for the purpose for which the information was obtained or for a use that is consistent with the purpose of the original collection.

OPC believes that the definition of consistent use should be interpreted narrowly, and that a "reasonable and direct connection" test should be applied. This principle is linked closely to the Limiting Collection principle, and the Limiting Use, Disclosure, and Retention principle. Information may also be used for purposes for which it could be disclosed to the institution under subsection 8(2) of the *Privacy Act*. This gives an institution greater certainty that it is allowed to use personal information for the purpose for which it was disclosed (to the institution) as described under 8(2). This might include using the information for collecting a debt owed to the Crown, for example, or when the greater public interest in using the information would clearly outweigh any invasion of privacy.

The Privacy Act restricts federal government institutions to the collection of personal information that relates directly to an operating program or activity of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose for the collection or on-line notices of use; a copy of an up to date Personal Information Bank (PIB) description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable and directly connected to the original collection – this may include an analysis of how an individual to whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

2.2.3 Consent

Fair information practices generally indicate that knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except in certain circumstances where it would be inappropriate. However, individual consent plays a relatively minor role in public sector data protection laws, including the *Privacy Act*. A large amount of personal information is collected by federal institutions without individual consent because the government has legislative authority to do so. Personal information may also be collected, used, or disclosed without the knowledge and consent of the individual when seeking such consent might defeat the purpose of collecting the information – when it is being collected for law enforcement purposes, for example, or for the detection and prevention of fraud.

It should be noted that even when consent is obtained where it is appropriate to do so, this does not remove the necessity for an institution to have lawful authority for the collection of the information, or the necessity that the information be directly related to the program or activity. Where consent is not required, the purposes for collection must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

This notice of purpose can be given in many ways. For example: an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses where appropriate, and acknowledging that the information can or will be shared under statutory authority or under certain provisions of the *Privacy Act*.

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of the notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the Privacy Act; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

2.2.4 Limiting Collection

The collection of personal information shall be limited to that which is necessary for the identified purposes. As indicated by section 4 of the *Privacy Act*, institutions are not to collect personal information indiscriminately, and may not collect information unless it relates directly to an operating program or activity. Institutions should ensure that both the amount and the type of information collected are strictly necessary to fulfil the stated need. This principle is linked closely to the Identifying Purposes principle and the Consent principle.

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the Privacy Act that no personal information is to be collected by a government institution unless it relates directly to an operating program or activity of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

2.2.5 Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by or provided for by legislation. Personal information shall be retained only as long as is necessary to fulfil those purposes. The *Privacy Act* states that personal information may be used or disclosed without the consent of the individual in certain circumstances, and these are listed in Section 8 of the *Act*. As noted in the discussion under the Identifying Purposes principle, information may also be used for the purposes for which it could be disclosed to the institution under subsection 8(2) of the *Act*. Institutions contemplating using personal information for a new purpose must ensure either that consent is obtained, or that the proposed new use qualifies as a "consistent use".

For a use or disclosure to be consistent, it must have a reasonable and direct connection to the original purpose for which it was obtained or compiled. Institutions should develop guidelines and procedures with respect to the retention of personal information, and these retention schedules should indicate minimum and maximum retention periods in keeping with the *Privacy Act* and Privacy Regulations. Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. This principle is closely linked to the Consent principle, the Identifying Purposes principle, and the Individual Access principle.

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the Privacy Act and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

2.2.6 Accuracy

This principle states that personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. The *Privacy Act* directs government institutions to take "all reasonable steps to ensure that personal information is as accurate, up-to-date and complete as possible". In considering how to apply this principle, the interests of the individual must be taken into account – information should be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information might be used to make a decision about the individual.

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

2.2.7 Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Institutions must protect personal information regardless of the format in which it is held. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The methods of protection should include physical measures, for example, locked filing cabinets and restricted access to offices; institutional measures such as appropriate employee security clearance levels and limiting access to a "need-to-know" basis; and technological measures, such as the use of passwords and encryption. Institutions shall make their employees aware of the importance of maintaining the confidentiality of personal information. Particular care shall be used in the disposal or destruction of personal information.

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information; strong electronic access control, including controls on remote access, and the use of mobile devices; policies for the use of portable storage devices such as flash drives; a description of role-based access controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

2.2.8 Openness

Institutions shall make readily available to individuals specific information about policies and practices relating to the management of personal information. Institutions shall be open about their policies and practices with respect to the management of personal information, and this information shall be made available in a form that is generally understandable. The information made available shall include the name/title and address of the person who is accountable for the personal information policies and practices and to whom complaints or inquiries or requests for recourse can be forwarded; the means of gaining access to personal information; a description of the type of personal information held including an account of its use; and a copy of any brochures or other information that explain the policies and procedures surrounding the use of personal information.

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the Privacy Act; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

2.2.9 Individual Access

The *Privacy Act* protects the privacy of all Canadian citizens and permanent residents regarding personal information held by a government institution. It also gives individuals, including individuals in Canada who are not permanent residents or citizens, the right to access their own personal information in the hands of government, and to request that corrections be made. The federal government publication Info Source provides individuals with an index of personal information held by government institutions subject to the *Privacy Act*. Descriptions of information contained in personal information banks (PIBs) should be clear and comprehensive, as this is the tool that is meant to ensure transparency for the public, and is intended to be used as a reference for individuals making requests for access to institutional holdings of personal information under the *Act*. While not all personal information can be released when a request is made, exemptions and exclusions should be interpreted as narrowly as possible.

Under this principle, OPC would expect a PIA to include a description of the institution's formal ATIP process; a description of any informal process it may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

2.2.10 Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the institution's compliance. Institutions must have procedures in place to receive and respond to complaints or inquiries about policies and practices relating to the handling of personal information. The complaint process should be easily accessible and simple to use. If a complaint about the use of personal information is found to be justified, steps should be taken to amend policies and practices in order to ensure systemic problems are noted and remedied.

OPC would expect to see a PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the Privacy Act; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

2.3 Using an action plan to keep the PIA relevant

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

PIAs are meant to be evergreen documents and thus should be revisited and updated regularly as the project or initiative progresses, changes, evolves, or winds down. The Action Plan can be an excellent tool in this regard. It should include a schedule for regular updates, revisions or addenda to the PIA, a timetable for refreshing the TRA for the project or initiative's IT system, and a plan for auditing and reporting on compliance with the privacy protection provisions of any MOUs or information sharing agreements that have been undertaken with third parties. The Action Plan should also include details of the retention schedule and forward planning for the ultimate disposition, safe storage, or destruction of the personal information involved. The PIA Action Plan is an integral component of the organization's overall Privacy Management Framework (PMF).

2.4 Multi-Institutional PIAs

Given the increase in horizontal initiatives and the current federal government emphasis on client centered services, we are receiving a corresponding increase in the number of multi-institutional and multi-jurisdictional PIAs. For each cluster of PIAs, it is important that one department or agency takes a strong policy leadership role for privacy. This helps ensure coherent communications with our office and the effective identification of privacy risks among all participating institutions. It also helps ensure the implementation of mitigation strategies across linked programs and initiatives. The intent is to have an overarching PIA that would—among other things—articulate a business case justifying the need for, say, increased information sharing; outline a common communications strategy to inform Canadians of the increased sharing of their information across government departments; and provide a solid foundation of expected privacy practices as guidance for all the departments and agencies participating in the initiative.

ANNEX A
PIA RESOURCES, TEMPLATES AND GUIDELINES

TBS Directive on Privacy Impact Assessment
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text#cha8

TBS Policy on Privacy Protection
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

TBS Directive on Social Insurance Number
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342

TBS Privacy Impact Assessment Policy
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450

TBS Privacy Impact Assessment Guidelines
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12451

PIA e-Learning Tool
http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-eng.asp

Institute for Citizen-Centred Service (ICCS) – Personal Information Sharing Agreement Guidelines
http://www.iccs-isac.org/en/practice/privacy.htm

Canadian Institute of Chartered Accountants – Generally Accepted Privacy Principles
http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/index.aspx

Canadian Standards Association – Model Code for the Protection of Personal Information
http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code

Organization for Economic Co-operation and Development – Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Office of the Privacy Commissioner of Canada – PIA Resources
http://www.priv.gc.ca/pia-efvp/index_e.cfm

TBS Chief Information Officer Branch – Report on Best Practices Identified During Implementation of the Privacy Impact Assessment Policy and Guidelines
http://www.tbs-sct.gc.ca/pgol-pged/pia-best/pia-best00-eng.asp

TBS Policy on Privacy Protection
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do-PR-eng.asp?printable=True

29th International Conference of Data Protection and Privacy Commissioners (2007) PIA Workshop
http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook12_bil.pdf

ANNEX B
CHECKLIST FOR PIA FORMAT AND ASSOCIATED DOCUMENTS

PIA Format

Ideally, PIAs should include the following sections to ensure thorough, complete assessments are conducted and that OPC PIA Review staff can proceed with an analysis without having to request more information from the submitting institution:

- A cover letter signed at the appropriate level of delegated authority.
- A detailed project overview including objectives, rationale, clients, approach, programs and/or partners involved.
- A list of all stakeholders and their roles and responsibilities.
- A list of all data elements that involve personal information and a related description of the data flow.
- A list of relevant legislation and policies that govern the project to demonstrate legal authority for the collection of personal information.
- A privacy analysis identifying privacy risks associated with the project. At minimum, the universal privacy principles should be addressed.
- A detailed risk mitigation plan outlining mitigating measures that will be adopted to address privacy risks identified in the PIA. Include any residual or outstanding risks that cannot be addressed, with an explanation of why.
- An outline of a privacy-oriented communications strategy, if the implementation of such a strategy is considered appropriate.
- Details on internal procedures relating to: incident response to privacy breaches, access and correction requests, and complaints.

Associated Documentation

Certain documents are integral to OPC conducting an in-depth analysis of projects that raise privacy risks. Without these key documents, there is a chance that serious privacy risks might go unidentified, potentially compromising the privacy rights of Canadians. Be sure to include the following documents with your PIA submission to OPC to assist us in identifying privacy risks and to ensure as expeditious a review as possible:

- Project-specific privacy policies and procedures.
- A summary of privacy risks identified in any Threat and Risk Assessment pertaining to the initiative, and an account of action taken to address these risks.
- A copy of any legal instrument, agreement or Memorandum of Understanding that was used to define the rights and responsibilities pertaining to information sharing among parties to the initiative.
- Data matching assessment.
- Copies of third party contracts pertaining to information sharing.
- Copies of any forms that are used to collect personal information, including associated notice of use and privacy statements.
- Copies of any public education materials that have been created which deal with personal information management.
- PIB description(s).
- A copy of the PIA summary to be posted on the institutional website.

Office of the
Privacy Commissioner
of Canada

For more information

For general inquiries please visit our website at **www.priv.gc.ca** or call us

Toll-free: 1 (800) 282-1376
Tel: (613) 995-8210
TTY/TDD: (613) 992-9190
Fax: (613) 947-6850

Cat. No.: IP54-36/2011E-PDF
ISBN: 978-1-100-18204-9