PURPOSE

The *Education Statute Law Amendment Act* (Student Performance Bill 78), *2006, received Royal Assent on June 1, 2006. Introduced in March 2006, the act contains several limited but substantive amendments to the Education Act and the Ontario College of Teachers Act*, 1996, *to support improved student performance and cooperation between education service providers based on respect and openness to the public for the purpose of improved student performance.*

MISA (Managing Information for Student Achievement) is a provincial initiative designed to build local and provincial capacity to collect, manage, and access information to support evidence-informed decision making to improve student learning. In accordance with this initiative, school boards/authorities are developing systems for managing and accessing a wide range of data, enhancing the technology available for reporting and analysis, and providing increased access to data and information related to student achievement.

The Privacy and Information Management (PIM) taskforce was established in September 2006 as an OASBO (Ontario Association of School Business Officials) and MISA joint project committed to helping school boards comply with provincial and federal access and privacy legislation. The PIM taskforce also supports efforts to meet the expectations of parents, students, and teachers with respect to information security and protection of personal information, thereby strengthening public trust and confidence.

What is a Privacy Impact Assessment (PIA)?

A PIA is an assessment framework used to identify the actual or potential risks that a proposed or existing information system, technology, or program may have on an individual's privacy. Examples of such systems and programs include data warehousing, centralized electronic student information systems, and information sharing with other school boards/authorities, education providers, or sectors.

Completing a PIA will help school boards/authorities determine if there are privacy-related concerns and risks that can be mitigated. It can also assist in identifying:

- options for managing, minimizing, and/or removing privacy impacts;
- unsatisfactory levels of accountability and/or oversight; and
- identification of when personal information is unnecessary to meet objectives.

A PIA can be separated into two stages.

Stage 1: The completion of a **privacy compliance checklist,** which analyzes what personal information is being collected. If the privacy compliance checklist leads to a determination that personal information is being collected, then the next stage must be undertaken.

Stage 2: The completion of a **comprehensive assessment** is only required if the privacy compliance checklist determines that personal information is being collected. If no personal information is involved, the second stage need not be undertaken.

The purpose of a PIA is to ensure that personal information is managed safely, securely and responsibly in accordance with legislative requirements. Its purpose is not to prevent information from being appropriately collected, used, retained and disclosed, but rather to ensure that appropriate operational practices are applied throughout the information lifecycle.

Why should a school board/authority do a PIA?

School board officials should consider conducting a PIA when they plan a new system or administrative practice or major changes to an existing system or practice that will collect, use and/or disclose personal information.

The PIA process is a due diligence exercise in which school boards can identify and address potential privacy risks that may occur in the course of their everyday operations.

A PIA is a valuable tool to provide review and feedback before a school board/authority implements proposed administrative practices and information systems relating to the collection, use, or disclosure of data/information identifying individuals.

A PIA may also be conducted when reviewing existing systems and practices for privacy compliance.

It is advisable for school boards to conduct a PIA in order to:

- confirm legal authority to collect, use, and disclose personal information;
- ensure fair information practices;
- identify and manage potential privacy risks through appropriate documentation (e.g., policies and procedures);
- communicate key messages and update notifications and privacy statements;
- save time and money (to avoid redesign or retrofit late in the development stage of an initiative or project);
- mitigate the risk of a privacy breach; and
- assure senior management that privacy policy and legislative compliance have been fulfilled.

A PIA is more than just a privacy compliance tool; it is an information management tool.

What are the major benefits for school boards/authorities of conducting a PIA?

- **Ensuring that individual privacy is protected**
  A PIA helps a school board determine if there are privacy risks associated with a particular program or service.
- **Promoting an awareness and understanding of privacy issues**
  A PIA puts privacy at the forefront of any new initiative.
- **Reducing the risk of non-compliance**
  A PIA helps school boards/authorities reduce the risk of non-compliance with privacy legislation and policies. This helps avoid costly redesigns of programs and services and assures student and employee stakeholders that their privacy is safeguarded.
- **Assisting school board officials to make better decisions**
  A PIA provides information to school board/authorities officials about privacy risks inherent in a new or redesigned program or service. Having this information helps these officials make better decisions.
- **Promoting trust and confidence**
  Public trust and confidence in the operations of a school board/authorities is increased by the knowledge that the PIA process is in regular and consistent use within the board.

A PIA has other benefits, including:

- identifying the potential for particular privacy impacts, such as additional uses of personal information that may evolve from the original stated uses and expectations or those that may arise from new legislation or technology;
- improving the project's consultation process, including public consultation (where necessary), so that privacy issues are more comprehensively identified and stakeholders are better informed;
- demonstrating to others that the handling of personal information in the project has been critically analyzed with privacy in mind; and
- playing a broader educational role about privacy, that can benefit not only the project, but also the board as a whole.

The information gathered in a PIA can also be used as part of the school board's/authority's broader project management processes for identifying risks to privacy.

A PIA helps to avoid costly and/or embarrassing privacy mistakes because it can:

- be used at the design stage to identify what needs to be done to ensure a project's compliance with privacy legislation and other board-specific or board-related legislative requirements-any necessary adjustments can be made during a project's development so that it will comply with all relevant laws that relate to the handling of personal information;
- include a list of applicable privacy laws and show the data-handling practices of the project, as well as the organizational rules to carry out these practices (e.g., policy and procedures), to comply with the specific provisions of the identified laws;

- provide an opportunity to consider community values (e.g., trust, respect, individual autonomy and accountability) and to reflect those values in the project by meeting the community's privacy protection expectations; and
- be used as a resource to broaden the school board's/authority's risk management processes in general.

A PIA can be a valuable tool to help identify what needs to be done to ensure a project's compliance with privacy legislation and/or other governing legislation.

What are the risks for school boards/authorities of not doing a PIA?

The risks associated with failing to appropriately address privacy issues can have an impact on the success of an initiative or project. These risks include:

- breach of an individual's personal privacy;
- failure to comply with relevant privacy legislation (i.e., breach of privacy);
- loss of credibility and trust of the community because of failure to meet expectations with regard to the protection of personal information (negative publicity); and
- systems redesign or retrofit late in the development stage (often at considerable expense).

How does an effective PIA work?

A PIA works most effectively when it is an integral stage/step of a project's design and development. By undertaking a PIA as an integral part of new projects, the school board/authority is able to:

- describe fully and systematically the way personal information "flows" in the project;
- analyze how these information flows will have an impact on privacy;
- identify the project's potential for further privacy risks;
- consider alternative privacy practices during project development rather than retrospectively; and
- make informed choices and recommendations about how the project will proceed.

A PIA is important in the development of a project involving personal information and should be an evolving or "living document." As the project develops and issues are identified, the PIA document can be updated and supplemented, resulting in the completion of a more comprehensive and useful PIA. A PIA should also be considered for existing projects.

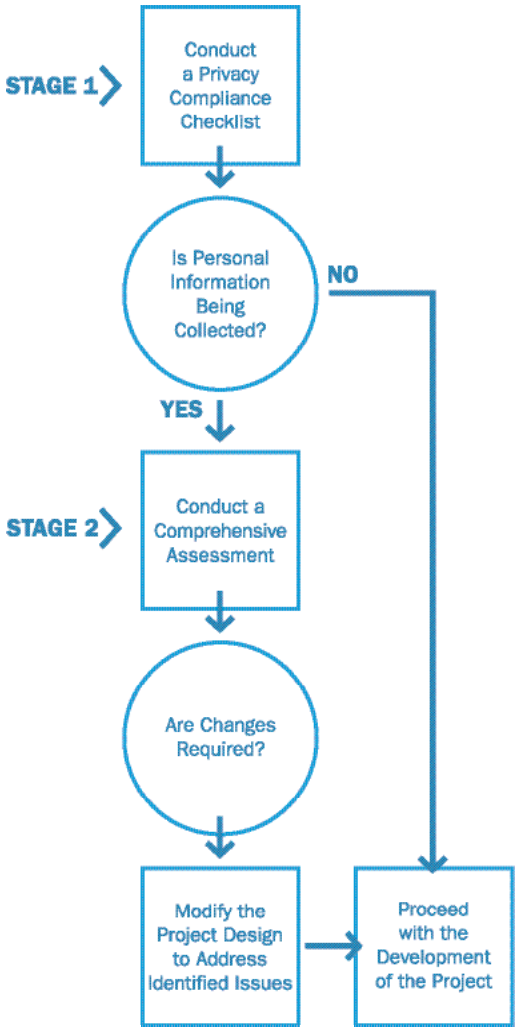
A PIA works best when it forms part of a project's evolution.

The stages of Privacy Impact Assessment

A PIA is comprised of two stages:

Stage 1: Privacy Compliance Checklist

Stage 2: Comprehensive Assessment



Privacy Compliance Checklist

A privacy compliance checklist (see Appendix C) is an important and useful first step in the PIA process. It should be completed for all new or redesigned projects, programs, technologies, initiatives, applications, and organizational practices. The checklist is a preliminary assessment of a project to identify the nature and sensitivity of any personal information that may be collected, used, or disclosed by the project, as well as the legal authority for the project/program.

Comprehensive Assessment

The comprehensive assessment (see Appendix D) is generally required for any project that:

- directly collects, uses or discloses personal information;
- indirectly collects personal information from any source;
- uses or expands the uses of common personal identifiers (e.g., OEN, MEN, SIN);
- introduces a new program or substantial system redesign of an existing program or system that collects, uses, or discloses personal information; or
- contracts with a third party to collect, use, or disclose personal information.

Once it is determined that personal information is involved in the project, the fundamental premise behind a comprehensive assessment is the mitigation of a potential privacy breach.

Understanding the purposes and function of a PIA will assist in deciding whether or not to implement a PIA for any given project. The primary driver is a substantial change in the collection, use, disclosure, or retention of personal information.

Planning the Comprehensive Assessment

Once the school board/authority has determined that a comprehensive assessment is necessary, the next consideration is the most appropriate design and approach based on the completed privacy compliance checklist.

Planning the most appropriate process will be influenced by the nature of the project. The design can be determined by looking at the project's:

Stage of development	Is it at the early or conceptual stages of development, or at a more advanced or detailed stage of development?
Scope	Is it limited or broad in scope?
Type	Is it a new program or system, or an alteration or "incremental" change to an existing program or system?
Personal information	Does it involve a limited or significant amount of personal information? What is the quantity and sensitivity of the personal information being handled?
Public impact	Does the project involve the handling of significant amounts of personal information about each individual, or the handling of personal information about a significant number of individuals? What is the public's perception of and expectation for the security of this personal information?
Interaction	What is the degree of interaction between personal information in more than one database (e.g., sharing or data-matching across the system, or across jurisdictions, or between the public and private sectors)?
Outsource	Will personal information handling be outsourced?

In general, the key components of a comprehensive assessment include the following:

Project description	Broadly describe the project, including the project's aims and whether any personal information will be handled.
Mapping the information flows	Describe and map the flows of personal information in the project.
Privacy impact analysis	Identify and analyze how the project impacts upon privacy.
Privacy management	Consider alternative options, particularly those that improve privacy outcomes while still achieving the project's goals.
Report and recommendations	Produce a final PIA report that includes the above information and recommendations.

Each of the above components should be addressed to some extent in every comprehensive assessment, with the level of detail being determined by the nature and stage of the project.

Who is involved in conducting a PIA?

Generally, a PIA uses a team approach and makes use of the various in-house experts available within the school board/authority, including staff responsible for access and privacy. It may consist of different stages and personnel as the project evolves. It is important to identify an individual or group of individuals who will be responsible for the completion of the PIA. The PIA leadership should have a clear mandate to review the project design decisions against the criteria of the PIA and provide the necessary advice and feedback to the senior project management team.

Some projects have considerably more privacy impact than others. In those cases, an independent PIA conducted by external privacy consultants or law firms may be preferable. Representation from school councils may also be advisable in some cases to provide input on the community's values and privacy protection expectations.

An individual staff member working in isolation would not undertake a PIA; it may consist of different stages and personnel as the project evolves. This "team" approach should be decided by assigned school board/authority individuals based on the scope of the project.

The following chart indicates who could be involved in a PIA and the types of skills they can provide:

PIA Leadership Role	PIA Leadership Skills
Project manager / team members	• Drive the process. • Build privacy component into the project plan. • Plan PIA activities in accordance with established project management principles.
Senior administration rep. (Superintendent)	• Support and advocate privacy commitment to approved project.
FOI Coordinator / privacy contact officer / records management	• Provide privacy expertise regarding standards, legislation, technologies and privacy developments. • Provide procedural and legal skills related to privacy and protection of recorded information.
Information technology	• Provide technology and systems expertise relating to the design and operation of the system/project application, networking products, Internet tools, system security, and front-end interface systems accessing the information.
Communications	• Document and publish essential notifications and information updates.
Other identified partners and stakeholders (e.g., students, parents, employees, ethics considerations) Σ	• Contribute to operational knowledge and understanding of the function of the project and the uses of the information. • Become familiar with the policies and procedures associated with the project, operational and business design skills related to the project.
Legal counsel/external consultants	• Provide legal and specialized expertise with regard to specific areas of the PIA or project, as required. This will be dependent upon the complexity of the personal information being assessed.

These roles are fundamental to ensuring that the PIA component of a project will be successful. Some individuals may play multiple roles, but it is important to assign the roles to specific individuals.

Why are consultation and transparency important to the PIA process?

Consultation, communication, and transparency are key to the success of any project that involves partners and/or significant stakeholders. A PIA is not just based on information technology. Business partners have to articulate the purpose. Privacy partners have to articulate the legislative and policy requirements. IT partners have to provide the technology context. Each contribution informs the assessment. Consultation with key stakeholders helps to ensure that key issues are noted, addressed, and communicated.

Similarly, wherever possible, publishing the contents and findings of a PIA can add value to the PIA and to the project. Publishing helps to demonstrate to stakeholders and the community that the project has been critically analyzed with privacy in mind. Publishing also represents good practice by contributing to the transparency of the project.

Where warranted, a PIA that incorporates public consultation can also help to garner broad community awareness and confidence in the project.

The PIA process is designed to ensure that privacy is considered throughout the business redesign or project development cycle, and particularly at the conceptual stage, the final design approval and funding stage, the implementation and communications stage, and the post-implementation audit or review stage.

DOING THE PIA

Overview of the Process

The PIA process requires a thorough analysis of potential impacts on privacy and a consideration of measures to mitigate or eliminate any such impacts. The privacy impact assessment is a due diligence exercise in which the organization identifies and addresses potential privacy risks that may occur in the course of its operations.

While PIA's are focused on specific projects, the process should include an examination of organization-wide practices that could have an impact on privacy. The school board's/authority's privacy policy and procedures, or the lack of them, can be a significant factor in the ability of the school board/authority to ensure that privacy protection measures are available for specific projects.

The onus always remains on the Board to ensure adequate levels of privacy protection, as required in applicable legislation MFIPPA or PHIPA, and if challenged in this regard, the Privacy Commissioner's Office will look for proof that the Board has made reasonable efforts to protect privacy. A PIA cannot be used to obtain a waiver of, or release from, any requirement of the relevant legislation.

A PIA is a process that helps to determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements. It also measures both technical compliance with privacy legislation, such as the MFIPPA and PHIPA, and the broader privacy implications of a given proposal. The PIA is also intended to help policy writers and decision-makers manage potential privacy risks.

As noted in sections 1.1 and 2.0, the two stages of the PIA process are:

1. **Conduct a Privacy Compliance Checklist**
   i. If it is determined that no personal information is being collected, the project may proceed.
   ii. If it is determined that personal information is being collected, proceed to Stage 2.
2. **Complete a Comprehensive Assessment**
   i. If it is deemed that changes are required with regard to the way personal information is collected, used, disclosed or secured for compliance with the *Ontario School Board Privacy Standard*, the project design must be modified to address these issues before it can proceed.

The end result of the PIA process is documented assurance that all privacy issues have been appropriately identified and adequately addressed or, in the case of outstanding issues, brought forward to senior management for further direction.

Privacy Impact Analysis – Privacy Compliance Checklist

In order to provide assurances that all relevant factors and potential privacy issues have been addressed, the following four key areas must be considered in the process:

1. *People* are important for two reasons: first, they handle personal information and must be aware of how that information is collected, used, retained and disclosed; second, as part of the privacy compliance environment, they must create and monitor the effectiveness of policies and processes. Privacy policies set boundaries and establish the privacy rights and obligations of parties.

   Consider: Ongoing management, privacy training programs, general organizational awareness of privacy and security issues, the level of knowledge required to perform specific functions, and the availability of manuals and other forms of guidance and/or mechanisms for communicating privacy and security policies and procedures.

2. *Processes* are necessary to implement the policies and procedures and are designed to ensure that a consistent message is communicated throughout the organization.

   Consider: What information is collected, why and how it is collected, how privacy and security are ensured operationally, and what mechanisms are in place to provide individual access to information.

3. *Systems* provide a means of protecting personal information through a variety of physical and electronic controls and other security measures.

   Consider: System design characteristics, data security and integrity measures, authority, access controls, and audit trails.

4. *Records management practices* establish a framework within which personal information is managed.

   Consider: The physical space where information is stored, physical security measures, the availability of secure document disposal facilities, and processes for secure disposal of old information technology, encryption technology, password protection, levels of authority (e.g., personal computers, legacy servers, etc.) which may hold personal information.

The PIA investigates how the flow of information in a project affects the choices individuals have regarding how personal information is handled, the intrusiveness into the private lives of individuals, the compliance with privacy law, and how the project fits into community expectations.

The Privacy Impact Analysis should consider:

- *which privacy impacts are serious and which are less so;*
- *whether the privacy impacts are necessary or avoidable; and*
- *how the privacy impacts may affect the broad goals of the project.*

Key questions to be answered through the privacy impact analysis phase of a PIA can be determined by conducting a Privacy Compliance Checklist (see Appendix A). This questionnaire investigates whether the personal information aspects of the project comply with applicable privacy laws.

Ontario School Board Privacy Standard – Comprehensive Assessment

The *Ontario School Board Privacy Standard* is a commitment we are applying in the collection, use and disclosure of personal information/data and addressing issues of privacy, security and confidentiality. These privacy commitments are based on the *Model Code for the Protection of Personal Information* that was developed by the Canadian Standards Association and was recognized as a national standard in 1996.

The Ontario School Board Privacy Standard can also be used for discussion purposes to complete a Comprehensive PIA (see Appendix B).

The ten commitments, with explanatory notes, are as follows:

1. **Accountability and Responsibility:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles

Start by identifying internally who will be your privacy officer(s). Such individuals must be designated by the school board/authority. As personal Information may be collected and processed by different departments within your organization, you should also consider whether a team of individuals would be necessary to ensure the whole board is compliant with the Act.

2. **Specified Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Conduct a "privacy audit" to determine what personal information you collect and for what purpose. Check your forms and publications and/or websites to ensure privacy statements that identify purpose for collection of personal information are present and visible where necessary. It is also important to ensure the availability of other information that may be required by law (i.e., legal authority for collection, and the title, business address, and telephone number of a person who can respond to questions about collection). Contact information for your privacy officer(s) should also be easily accessible.

3. **Consent:** The knowledge or consent of the individual is required for the collection, use, or disclosure of personal information, except when not required by law.

Consent is generally not necessary under MFIPPA, except in limited cases where information is being collected indirectly. However, this does not mean that consent cannot form part of the collection process. As part of your audit, consider how you collect information. As varying types of consent are possible, consider which is most appropriate to the nature, including sensitivity, of the information you collect.

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

This means that an organization must limit the type of information collected to correspond with the stated purpose. Section 28(2) of MFIPPA provides that "no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity." Sections 29(1) and (2) of MFIPPA outline the manner of collection and notice requirements to the individual regarding the collection of personal information, including the principal purpose or purposes for which the personal information is intended to be used.

5. **Limiting Use, Retention, and Disclosure:**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 law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes, or as required by law.

Your privacy policy must include guidelines that govern the handling of personal information while your organization is using it, including minimum and maximum times for retaining it. Information used to make a decision about an individual should also be kept long enough to allow the individual to have access to it.Section 30(1) and (4) of MFIPPA ensures that personal information must be collected, used, disclosed, retained and disposed of in accordance with the regulations. (O.Reg. 823/90) Note: MFIPPA contains minimum but not maximum retention periods.

6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used.

Under sections 30(2) and 30(3) of MFIPPA, institutions must take reasonable steps to ensure that personal information within the records of the institution is not used unless it is accurate and up-to-date, with the exception of personal information that is prohibited by legislation for routine updating if it is not necessary to fulfill the purpose given for the initial collection, e.g., law enforcement purposes.

7. **Security Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

As part of your procedures identify methods of secure storage and disposal. Such procedures can include physical and technical measures as needed, as well as staff education and awareness.

8. **Openness and Transparency:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Specific information about personal information policies and practices must be readily available in an understandable form. This must include the name or title and address of the privacy officer and a description of the type of personal information the school board/authority collects, uses, and retains. Under sections 25 and 34 of MFIPPA, institutions must make available a Directory of General Records and Personal Information Banks for inspection by the general public or for clarification by a requester seeking access to records and information under the care, custody, and control of the institution and is required to document specific information about such banks.

9. **Access and Correction:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Under sections 36 and 37 of MFIPPA, every individual has a right of access to personal information that is in the custody or under control of an institution, with specific exemptions as noted under section 38 of MFIPPA. In addition, every individual who is given access to his/her personal information is entitled to ensure that the information is accurate and complete and, if it is not, to request that it be corrected, or to have a statement of disagreement attached to the personal information that was not corrected as requested.

10. **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 organization's privacy compliance.

The school board/authority must be ready to respond to privacy complaints, including amending policies and practices if necessary. School boards/authorities must also be ready for compliance audits and appeals relative to the access to and/or release of personal information, should there be reasonable grounds to believe that the organization has acted in contravention of the Act(s). The Office of the Information and Privacy Commissioner/Ontario will investigate these matters.

In practice, organizations (including school boards/authorities of education) can use the ten commitments of the Privacy Standard in developing a privacy policy.

The Privacy Standard can also be used to develop a comprehensive PIA.

Report and Recommendations (see Appendix C: Privacy Impact Assessment Report)

The Assessment Has Been Done... What's Next?

The PIA report with its findings and recommendations is a valuable resource, assisting the project team, senior management, and other stakeholders. The PIA can be used to further inform and educate those involved in, or affected by, the project.

For example:

- The PIA should feed into further planning about the project's next steps. This may include resource allocation; stakeholder management; advising the senior management and governing body (the board) about risks; staffing; designing; piloting; testing; consultation; public education; and evaluation;
- Generally, PIA findings should be published at the appropriate stage, in particular to ensure that key stakeholders have a copy; and
- PIA findings may need to be revisited at different phases or for different aspects of the project as it progresses.

Documentation of the PIA investigation, analysis, assessment, and findings forms an ongoing, useful decision-making tool for the organization. Providing a PIA report also enables the success of any PIA recommendations implemented to be reviewed as part of the post-implementation review of the project.

Organizations are encouraged to include the PIA findings during any subsequent public consultation on the project. Organizations are also encouraged to make the PIA findings available to the public as part of the project's implementation.

Privacy and project goals can both be achieved.

Acknowledgements and References

Government of Ontario (June 2001). Privacy Impact Assessment: A User's Guide. Information and Privacy Office; I & IT Strategy; Policy, Planning and Management Branch. Officer of the Corporate Chief Strategist, Management Board Secretariat.

Information Privacy Commissioner (October 2005). *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act.*

Office of the Information and Privacy Commissioner (January 2001). *Privacy Impact Assessment: Instructions and Annotated Questionnaire.* Alberta, Canada.

Office of the Privacy Commissioner (August 2006). *Privacy Impact Assessment Guide: Australian Government.*

Related Links

Ontario Ministry of Government Services, Privacy Impact Assessment Guidelines
http://www.accessandprivacy.gov.on.ca/english/pia/pia.html