Australian Government

Office of the Privacy Commissioner

Privacy Impact Assessment Guide

August 2006

Table of Contents

About This Guide

1 How to use

The aim of this Guide is to give Australian Government and ACT Government agencies (agencies) an introduction to Privacy Impact Assessments (PIA). The Guide consists of the following sections and a series of practical modules.

- **Overview of Privacy Impact Assessment** provides a broad introduction to PIA, including an explanation of what a PIA is, its purpose, when it will be appropriate to conduct a PIA, and its benefits.
- **Is a PIA Necessary?** discusses making the important threshold assessment as to whether a particular project will require a PIA.
- **Approaching the PIA** introduces the key stages which will be at the core of most PIAs. The Guide does not impose a particular form of PIA on agencies, but instead recognises the importance of flexibility in any PIA. This section also provides some tips for planning the most appropriate PIA process for a particular project.
- **Doing the PIA** explains how to do a PIA in more practical detail, including a deeper explanation of the key stages of the process.
- **Acknowledgements and Resources** provides some useful national and international resources in relation to PIAs.
- **Modules A-F** are some useful, practical tools which are designed to be used at specific stages of a PIA. The main body of the Guide explains when and how these can be used.

The Guide is designed to be of use to both management and officer level audiences. Generally, the *Overview of Privacy Impact Assessment* section provides the more general, big picture information about PIAs, and can play the role of an Executive Summary for senior management about PIAs. The other sections, in conjunction with the modules, are designed to extend upon this material, and be of more specific, practical benefit to any staff actually involved in carrying out the PIA.

2 Meaning of certain concepts

Personal information / information privacy - In Australia, federal privacy legislation primarily concerns itself with information privacy, that is, it is designed to regulate the manner in which individuals' personal information is handled. Information privacy is therefore the main regulatory focus of the Office of the Privacy Commissioner (the Office) and this Guide.

The *Privacy Act 1988* (Cth) (www.privacy.gov.au/act/privacyact/index.html) defines "personal information" as:

> *"…information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded*

in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

Personal information does not always need to include an individual's name. It includes information that can be linked to or can identify a specific individual through association or inference.

It is important to note however that, whilst information privacy is the regulatory focus of the Office and this Guide, it is only one aspect of privacy more broadly. For example, there are other types of privacy (such as bodily privacy; territorial privacy; communications privacy).[1] Whilst this Guide is primarily designed to address information privacy issues through the PIA process, other types of privacy can also be considered, particularly where such privacy issues may pose risks to the overall success of the project.

Project - The term "project" is used throughout the Guide to describe the activity or function the agency is assessing. A PIA can be applied to any project that handles personal information. The project may be any proposal, review, system, database, program, application, service or agency initiative that includes the handling of personal information.

 **-** This symbol appears at certain places in the Guide.

This symbol simply aims to highlight certain key privacy messages as they appear throughout the Guide, and is designed to act as a pointer to useful summaries of key material.

[1] For a summary of different types of privacy see Banisar D, 2000, *Privacy and Human Rights: an international survey of privacy laws and developments*, Electronic Privacy Information Centre, Washington: www.privacyinternational.org/survey.

Overview of Privacy Impact Assessment

3 What is a PIA?

A PIA "tells the story" of a project or policy initiative from a privacy perspective and helps to manage privacy impacts.

A PIA is an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals – it "tells the story" of the project from a privacy perspective.[2] The purpose of doing a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts.

A PIA can help to identify and assess the privacy impacts a project may have, for example, by assisting an agency to identify when the collection of particular personal information is unnecessary to a project, or whether the project lacks appropriate accountability or oversight processes.

A PIA can assist agencies to manage privacy impacts by providing a thorough analysis of the effect of the project on individual privacy and helping to find potential solutions. In many cases, a PIA can help to make a significant difference to the privacy impact of the project whilst still achieving the project's goals. The elements that make up a PIA (including identification, analysis and management of privacy impacts) help agencies to drive good privacy practice and underpin good public policy in their projects.

4 Why do a PIA?

The PIA pay off: helping to ensure the success of the project.

The Privacy Act does not refer to PIAs nor does it require agencies to undertake a PIA. However, the success of an agency's project will depend in part on it complying with legislative privacy requirements and how well it meets broader community expectations about privacy.[3] Failure to appropriately address privacy issues can have an impact on the trust of the community and can pose risks to the success of the project.

[2] Professor David Flaherty, Professor Emeritus, University of Western Ontario.

[3] It is acknowledged that the task of making an assessment of the community's broader expectations about privacy can be a difficult one. For further information in relation to the Office's research into privacy attitudes in Australia, see the OPC website at www.privacy.gov.au/business/research.

The risks associated with failing to consider the privacy implications of a project can take many forms, and may include, for example:[4]

- **Failure to comply** with either the letter or the spirit of relevant privacy legislation, resulting in a breach of the law and/or negative publicity;
- **Stimulating public concern or loss of credibility** as a result of a perceived loss of privacy or a failure to meet expectations with regard to the protection of personal information; or
- **A need for systems to be redesigned** or retrofitted late in the development stage at considerable expense.

A project which underestimates privacy impacts, and as a result makes privacy mistakes or simply gets privacy wrong, can place its overall success at risk by not meeting the test of trust and acceptance by the community, or by breaching privacy legislation. It is therefore in an agency's interests to do a PIA for any projects which involve the handling of personal information.

5 Benefits of a PIA

A PIA helps to avoid costly or embarrassing privacy mistakes.

The over-arching benefit of a PIA is that it allows agencies to identify and analyse privacy impacts during a project's design phase, which in turn assists agencies to determine the appropriate management of any negative privacy impacts and thereby avoid costly or embarrassing privacy mistakes. Dealing with privacy impacts can be challenging for agencies. By conducting a PIA, agencies will be in a much better position to meet those challenges.

Some more specific benefits of conducting a PIA are discussed below.

Compliance with privacy law

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 other agency-specific or cross-portfolio legislative requirements.

The Privacy Act, through the Information Privacy Principles (www.privacy.gov.au/act/ipps/index.html) (IPPs),[5] provides a minimum level of privacy protection to personal information handled by agencies. Many agencies are also subject to agency-specific legislative requirements that add

[4] For a further discussion of the risks associated with failing to consider the privacy implications of a project see *Privacy Impact Assessment: A User's Guide* on the Government of Ontario's Access and Privacy Office website at www.accessandprivacy.gov.on.ca/english/pia/index.html.

[5] For the full text of the Information Privacy Principles see the OPC website at www.privacy.gov.au/act/ipps/index.html.

further privacy protections (such as secrecy provisions), as well as legislative requirements which apply more generally across government.

A PIA helps agencies to identify and make any necessary adjustments during a project's development, so that it will comply with all relevant laws that relate to the handling of personal information. A PIA can include a list of applicable privacy laws and an account of how the data-handling practices of the project, as well as the business rules to carry out those practices, will comply with the specific provisions of these laws.

Further guidance for agencies on compliance with the Privacy Act can be found at www.privacy.gov.au.

Reflecting community values

Compliance with relevant privacy law is fundamental to assessing and managing privacy impacts. Compliance underpins the PIA, but it is not the whole story. Projects can have adverse impacts on the privacy of individuals in many ways, and considerations other than compliance with privacy law may also need to be taken into account when assessing the impact of a project.

As a community and as individuals we value our privacy.[6] We try hard to strike a balance between meeting our personal needs and goals, and appreciating what others need or want to know about us. Privacy is valued, not only because it underpins our human dignity, but also because it gives us a measure of control in our everyday interactions as to how our personal information is handled in the wider world.

Conducting a PIA provides agencies with the opportunity to consider the values the community places on privacy – trust, respect, individual autonomy and accountability – and to reflect those values in the project by meeting the community's privacy protection expectations. In determining how to achieve the right balance in a project, agencies should consider the interests of the agency, the broader community and the interests of the individual, and consider taking steps to ensure that the privacy impacts identified do not outweigh the public benefit to be gained in the project.

Project risk management

The information gathered in a PIA can also be used as part of an agency's broader project risk management processes.

The *Australian/New Zealand Risk Management Standard* (AS/NZS 4360:2004) and the companion handbook *Risk Management Guidelines* (HB 436:2004) are used in government to assist in the process of assessing and managing project risks.

By feeding PIA information into their risk management processes, agencies will be in a better position to assess the level of risk which privacy impacts

[6] OPC Research into Community Attitudes Towards Privacy in Australia 2004 www.privacy.gov.au/business/research/index.html#1a

represent to the project, and decide on the most appropriate avoidance, mitigation or management strategies.

Other benefits

A PIA has other important benefits including:

- helping to find privacy solutions which also help to progress the project's goals;
- identifying the potential for particular privacy impacts such as:
    - function creep (i.e. additional uses of a system, and/or the personal information it involves, which 'creep' away from the original stated uses and potentially from the original expectations of the individuals involved); or
    - those that may arise from new legislation or technology;
- improving the project's consultation process, including public consultation, so that privacy issues are more comprehensively identified and stakeholders are better informed regarding the project's privacy and information handling aspects;
- demonstrating to others that the handling of personal information in the project has been critically analysed with privacy in mind; and
- playing a broader educational role about privacy, which can benefit not only the project but the agency as a whole.

6 How does a PIA work?

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

A PIA works most effectively when it forms part of a project's development, so that it helps to shape the evolution of the project. This ensures that privacy is 'built in' rather than 'bolted on'.

By undertaking a PIA as an integral part of the project from the beginning, agencies are able to:

- describe fully and systematically the way personal information "flows" in the project;
- analyse how these information flows will impact on privacy;
- identify early, a project's potential for further privacy erosion, for example, through function creep;
- consider alternative, less privacy-intrusive practices during project development rather than retrospectively; and

- make informed choices and recommendations about how the project will proceed.

Given the importance of a PIA in the evolution of a project involving personal information, the PIA document itself will also usually tend to be an evolving or living document. As the project develops and the issues become clearer, a PIA document can be updated and supplemented, leading to the completion of a more comprehensive and useful PIA. Projects which are more significant in scope may even require more than one PIA throughout their development.

7 Indicators that a PIA will be important

Significance of the project, and the extent to which personal information is handled.

Generally, it is the significance or scope of a project, and the extent to which a project involves the collection, use or disclosure of personal information, which will indicate the importance of doing a PIA, and the level of detail that may be required.

The greater a project's size, complexity or scope (looking, for example, at indicators such as the proportion of the community upon which the project impacts, and the effects the project is likely to have on relevant individuals), the more likely it will be that a comprehensive PIA will assist in determining and managing the privacy impacts the project may pose. A project which, for example, involves significant amounts of personal information, or information that is generally regarded as sensitive, is likely to benefit from a PIA.

Not every project will need a PIA. Agencies will be in the best position to assess whether a PIA is necessary or desirable, and the level of detail that may be required. However, this Guide provides some assistance to agencies in making this assessment.

8 Who does the PIA?

Generally, the agency undertaking the project will be responsible for deciding if a PIA is necessary or desirable and then ensuring it is carried out.

Usually, a PIA would not be undertaken by an individual staff member working in isolation; it may consist of different stages and personnel as the project evolves. Generally, a PIA uses a team approach and makes use of the various 'in-house experts' available in the agency, including the agency's Privacy Contact Officer, as well as calling on outside expertise as necessary. In many cases, a set of 'fresh eyes' looking over a project can identify privacy impacts not previously recognised.

Some projects will have markedly more privacy impact than others. In those instances, a robust and independent PIA conducted by external assessors

may be preferable as it may help to develop community trust in the findings of the PIA and the intent of the project.[7]

9 Consultation and transparency

In assessing privacy impacts, it will often be appropriate to consult widely. Consultation with key stakeholders is intrinsic to the PIA process as it helps to ensure that key issues are noted, addressed and communicated.

As a PIA also involves consideration of community attitudes and expectations in relation to privacy, and because potentially affected individuals are likely to be key stakeholders, public consultation will also often be important, particularly where large quantities of personal information are being handled or where information of particular sensitivity is involved. A PIA which incorporates public consultation can help to engender broad community awareness and confidence in the project.

Whilst the extent and timing of the consultation may vary depending on the project (for example, projects may be at a preliminary, sensitive or confidential stage), consultation will generally add significant value to a PIA and potentially increase stakeholder and community confidence in the initiative.

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

[7] There are a growing number of privacy consultancies and law firms that offer PIAs as a service. Whilst the OPC cannot endorse or recommend a particular organisation to conduct a PIA, the OPC website hosts a page of privacy service providers which includes some PIA providers. Visit http://www.privacy.gov.au/links/service/index.html

Is a PIA Necessary?

10 Threshold Assessment

Will personal information be collected, used or disclosed in the project?

Not every project will need a PIA. The first critical question in assessing whether a PIA is needed is whether any personal information will be collected, used or disclosed in the project. If personal information is not involved in the project at any stage, the project may have a negligible impact on information privacy, and a PIA may not be necessary.

Making this important threshold assessment provides the opportunity for projects with no or minimal information privacy implications to be identified relatively easily and quickly.

Such a threshold assessment will essentially require an agency to broadly describe the project, including the project's aims, and analyse whether any personal information will be handled. ***Module A*** (developed by the Attorney-General's Department) is an example of a tool which may be used within agencies to assist officers in making this threshold assessment.

Approaching the PIA

11 Key stages of a PIA

Once an agency has determined that a PIA is necessary for a particular project, the next question is likely to be what kind of approach to the PIA will be most appropriate in the circumstances.

A number of PIA models have been developed internationally which may be helpful (see *Acknowledgements and Resources*). While some of these models are focused on compliance with a particular jurisdiction's privacy legislation, they all aim to provide some means of measuring the privacy impacts posed by a project.

Whilst there is no one-size-fits-all PIA model, there are a few broad stages which could be considered key to undertaking such a process.

Generally, the key stages of a PIA include:

1. **Project description:** broadly describe the project, including the project's aims and whether any personal information will be handled.

2. **Mapping the information flows:** describe and map the flows of personal information in the project.

3. **Privacy impact analysis:** identify and analyse how the project impacts upon privacy.

4. **Privacy management:** consider alternative options, particularly those which will improve privacy outcomes whilst still achieving the project's goals.

5. **Recommendations:** produce a final PIA Report, which includes the above information and recommendations

The material which follows suggests that each of the above stages be addressed to some extent in every PIA, with the level of detail being determined by the nature of the project.

12 Planning the PIA

The nature of the project will determine the PIA process.

Planning the most appropriate PIA process for a particular project will be influenced to a significant extent by the nature of the project and the stage of development the project has reached. For example, a particular project might:

- be at the early or conceptual stages of thinking, or at a more advanced or detailed stage of thinking;
- be an alteration to a well-established existing program or system (an "incremental" project), or a significant new program or system;
- be either limited or broader in scope; or
- involve a limited or more significant amount of personal information.

It is also possible for a project to feature more than one of these characteristics. For example, an incremental project might still be broad in its scope and privacy implications.

Agencies will be in the best position to consider these matters and to decide upon the most appropriate PIA process. To assist agencies in this regard, ***Module B*** provides some guidance and examples which are designed to help demonstrate how the PIA process can differ for different types of projects or projects at various stages.

Doing the PIA

The following sections provide some more detailed assistance about considerations which may be helpful at each of the key stages of the PIA process.

13 Project description

Describe the big picture.

The aim of this first stage of a PIA is to draft a broad, 'big picture' description of the project, including an explanation of:

- the project's overall aims (including how they fit within the agency's broader objectives);
- the drivers for or reasons behind the project;
- the scope and extent of the project;
- any links with existing programs or projects;
- whether any personal information will be handled; and
- some of the key privacy elements (for example, what sort of information will be collected; for what general purposes will it be used and disclosed; etc.).

This information helps to provide a broad explanation of the nature of the project, and can provide important context for the rest of the PIA. Any description of the project which has been done as part of the Threshold Assessment (see *10. Threshold Assessment* above) is likely to be useful at this stage of the PIA.

14 Mapping the information flows

Understand how the information flows in the project.

Once a broad description of the nature and scope of the project has been completed, the next stage in a PIA is to describe and map the flows of personal information in the project. This could include:

- what personal information is to be handled in the project;
- how the personal information is to be collected;
- how it will be used;
- internal flows;
- disclosures;
- security measures; and
- any privacy, secrecy and other relevant legislation applying to those flows.

In order to effectively map the information flows, communicating with all relevant sections of the agency will be important. Attempting to complete this stage in isolation runs the risk that valuable information about how the project will work, and how any personal information will be handled, may not be taken into account. This could lead to difficulties as the project develops.

This stage of the PIA should also describe the environment that currently exists, and how the project will affect this environment. For example, where a project involves new uses for personal information already held by an agency, this description could identify the nature of such personal information and the context in which it was initially collected (including the purpose of collection). Illustrating the data flows using diagrams or maps can give a clearer picture.

It may also be possible at this stage for an agency to start making some preliminary assessments, based on the above information, of possible areas where privacy impacts or compliance issues might potentially arise, as well as developing some early thoughts on possible alternatives.

The elements of the project that are likely to be relevant to the information privacy impact include: the ***collection*** of personal information; its ***use*** and ***disclosure***; the ability individuals have to ***access*** information about them, and to ***correct*** that information if need be; the applicable ***security*** safeguards; the processes for ensuring ***data quality***; and whether an ***identity management*** system is involved.

Module C contains a series of questions which address each of these areas. It is designed to assist in producing a clear picture of the project's information flows, and in doing so should also begin to draw out some possible areas where information privacy issues might arise in the project.

15 Privacy impact analysis

Privacy impacts affect individual choice.

Once the description and mapping of the information flows has been completed to the level of detail possible considering the nature and status of the project, the next stage in a PIA is to identify and critically analyse, based on that information, how the project impacts upon privacy (both positively and negatively).

A project has a privacy impact if, for example, it affects an individual's choices about who has access to particular information about them. Identifying and then making an assessment of the privacy impacts of a project means the agency must take a critical look at the degree to which the project might compromise individual autonomy in relation to personal information.

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.

This analysis will require a thorough and frank assessment of whether the project will provide acceptable privacy outcomes, or whether it will generate unacceptable impacts upon privacy. Some consideration as to the availability of alternatives which may improve privacy outcomes may also be possible at this stage. The results of any stakeholder or public consultation are likely to provide important information to assist this analysis.

A number of factors can influence this analysis, such as the context in which the information is collected or the content of the information. Sometimes, simply handling a name and address might involve a privacy impact in the wrong circumstances, for example when an individual is under threat of harassment or violence, and the intention is to put the information onto a public register. Some types of personal information are generally more sensitive than others, such as genetic and general health information or information about criminal convictions.

Module D is designed to be used as a starting point for agencies conducting such an analysis. It provides a series of questions which should assist in drawing out how the project impacts upon privacy.

An important component of this analysis for Australian and ACT Government agencies will be to assess whether the project is consistent with the Information Privacy Principles (IPPs) in the Privacy Act, with which all such agencies must comply. ***Module E*** (developed by the Attorney-General's Department) contains a series of questions which specifically address IPP compliance issues. Reference to the description and mapping of the

information flows previously documented should assist agencies in responding to these questions.

16 Privacy management

Privacy and project goals can both be achieved.

Using the findings of the privacy impact analysis, the next stage of the PIA will be to identify and consider any possible options which may help to eradicate or mitigate the negative privacy impacts identified.

The process of considering such alternatives does not necessarily need to involve compromising a project's goals. If such consideration is done well, an agency may find that it has options available to it which will make a significant difference to the privacy impact of the project whilst still achieving the project's goals. For example, the use of privacy enhancing technologies (PETs)[8] may help to ensure that only the minimum necessary amount of personal information is collected, whilst still enabling the project's functions to be achieved.

Module F should be used as a starting point for this critical stage of the PIA. It lists some matters which agencies should consider when deciding upon appropriate responses or actions in relation to any negative privacy impacts identified. This stage of the PIA can also feed into an agency's broader project risk management processes (see *5. Benefits of a PIA — Project risk management* above).

17 Recommendations

The final stage of the PIA will be to finalise the documentation of the above information, including recommendations for the future of the project based on the assessment. The PIA story will most usefully be told in the form of a report. For some examples of PIA reports which may be helpful, see *Acknowledgements and Resources*.

A PIA, critically focused on the elements of the project, can produce a variety of recommendations; not all of which will match the agency's expectations. For example, a recommendation may suggest further fine-tuning is needed in a particular area of the project, such as collection practices.

The PIA report should identify avoidable impacts or risks and suggest measures to remove them or reduce them to an appropriate level.

[8] For an introductory discussion of the concepts of Privacy Enhancing Technologies (PETs) and Privacy Intrusive Technologies (PITs), see the Office's speech *Under the Gaze, Privacy Identity & New Technology* on the OPC website at www.privacy.gov.au/news/speeches/sp104notes.pdf.

The recommendations should indicate the best way forward to manage the privacy impacts identified in the project, which may include:

- changes that need to be made in order to achieve a more appropriate balance between the goals of the project, the interests of the agency and the interests of the individuals affected by the project;
- whether further consultation is required; and
- whether, if the privacy impacts are too significant, the project should proceed.

18 The assessment has been done … what then?

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 instance:

- the PIA should feed into further planning about the project's next steps. This may include resource allocation, stakeholder management, advising Ministers and government (including about risks), staffing, designing, trialling, 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 (for agencies, the OPC is likely to be a key stakeholder); 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 agency. 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.

The Privacy Commissioner encourages agencies to include the PIA findings during any subsequent public consultation on the project. The Commissioner also encourages agencies to make the PIA findings available to the public as part of the project's implementation.

19 Role of the Office

There is no formal role for the Office of the Privacy Commissioner in the development, endorsement or approval of PIAs. However, it may be able to assist agencies with advice on privacy issues arising throughout the PIA process.

Acknowledgements and Resources

Acknowledgements

Assessing the privacy impact of a project is still a relatively recent development, particularly in Australia. A number of different models have been developed nationally and internationally for conducting a PIA. In some overseas jurisdictions, a PIA is required by law in certain circumstances and the PIA format is prescribed.

The Office acknowledges the ground-breaking and informative work undertaken by The Office of the Privacy Commissioner of New Zealand (www.privacy.org.nz/home.php), The Office of the Privacy Commissioner of Canada (www.privcom.gc.ca/pia-efvp/index_e.asp) and Professor David Flaherty among others, in the area of privacy impact assessment information and guidance. This Guide builds on that work, particularly the guidance material from the New Zealand Privacy Commissioner.

The Office would also like to thank the New Zealand Privacy Commissioner's Office for providing a number of the PIA references and resources below, which agencies may find helpful.

Privacy Victoria has also produced a guide to PIAs directed at Victorian Government agencies, which was useful during the preparation of this Guide.

PIA Resources

Australian Government Information Management Office (AGIMO)

AGIMO has produced some guidance on how to conduct consultative impact assessments: http://www.agimo.gov.au/infrastructure/authentication/agaf/impguidegovt/volume3/part5/appendix_a_-_sample_privacy_law_compliance_checklist.

Canada

The Treasury Board of Canada Secretariat has produced a useful PIA e-learning tool: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp.

New Zealand

Office of the Privacy Commissioner (New Zealand), *Privacy Impact Assessment Handbook*: http://www.privacy.org.nz/library/privacy-impact-assessment-handbook.

For a collection of online resources from around the world, collated by the New Zealand Privacy Commissioner's Office, see: http://www.foi.gov.uk/sharing/toolkit/pia_online_res.pdf.

United States of America

The Privacy Office of the Department of Homeland Security has released official guidance for use in drafting PIAs: www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.

Victoria (Australia)

Office of the Victorian Privacy Commissioner, Privacy Impact Assessments – a guide: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf.

PIA Reports (or summaries)

The following is a small sample of reports or summaries of findings and recommendations published by a number of national and international government agencies and organisations that have undertaken a PIA. The Office does not specifically endorse any of these resources, nor does it encourage any specific format for PIA reports. They are provided to give agencies some idea of the different approaches to PIA reporting that are open to them.

Australia

Australian Bureau of Statistics – PIA for a Proposal for Enhancing the Population Census (2005): www.abs.gov.au/websitedbs/D3110124.NSF/f5c7b8fb229cf017ca256973001fecec/fa7fd3e58e5cb46bca2571ee00190475!OpenDocument

Australian Government Information Management Office (AGIMO) – Privacy Management Strategy for the Identity Management for Australian Government Employees Framework (IMAGE) (2006): http://www.agimo.gov.au/__data/assets/pdf_file/51358/IMAGE_Privacy_Management_Strategy_1_0__2_.pdf.

Canada

The Treasury Board of Canada Secretariat's PIA e-learning tool (referred to above) includes some useful suggestions for what elements might comprise a PIA Report: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course2/mod3/mod3-2d_e.asp.

Summary of Foreign Affairs Canada's PIA for the Facial Recognition Project: http://www.ppt.gc.ca/publications/facial_recognition_e.aspx.

Alberta Screening Directive (2003): http://www.pao.gov.ab.ca/directives/staffing/privacy-impact-assessment.pdf.

Canadian Institute of Health Information NHEX (2002): http://secure.cihi.ca/cihiweb/en/downloads/spend_nhex_e_PIANHEX.pdf.

Alberta Information and Privacy Commissioner Registry: http://www.oipc.ab.ca/pia/registry.cfm.

New Zealand

State Service Commission series of PIAs in relation to the All-of-Government Authentication Project:

2003: http://www.e.govt.nz/services/authentication/authent-pia-200312.

2004: http://www.e.govt.nz/services/authentication/pia-200404.

2005: http://www.e.govt.nz/services/authentication/gls-pia.

Statistics New Zealand PIA in relation to the Injury Statistics Pilot Project (2004): http://www.stats.govt.nz/NR/rdonlyres/1AD12FED-E5D2-4AA1-AAA2-219F8C837940/0/PilotPrivacyImpactAssessment.pdf.

NZ Health Information Service PIA for the Mental Health Information Project (1999): http://www.nzhis.govt.nz/documentation/mhinc/mhprivacy.html.

United States of America

The PIA guidance material of the Privacy Office of the Department of Homeland Security (referred to above) also contains examples of official PIA Reports of significant initiatives within the U.S. Department of Homeland Security: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0511.xml.

Other Privacy Management Resources

Office of the Privacy Commissioner (Australia): www.privacy.gov.au

Building privacy into a system is discussed further in “Management and Integrity of Electronic Information in the Commonwealth 2003”, the Office Submission to the Joint Committee of Public Accounts and Audit: http://www.privacy.gov.au/publications/jcpaasubs.doc.

Strategies for, and approaches to, good identity management practices are discussed in “Proof of ID Required? Getting Identity Management Right”: Speech delivered by the Privacy Commissioner to the Australian IT Security Forum, Sydney, 2004: http://www.privacy.gov.au/news/speeches/sp1_04p.pdf.

There are a growing number of privacy consultancies and law firms that offer PIAs as a service. Whilst the OPC cannot endorse or recommend a particular organisation to conduct a PIA, the OPC website hosts a page of Privacy Service Providers which includes some PIA providers: http://www.privacy.gov.au/links/service/index.html.

MODULE A Threshold Assessment

Background

1. This Threshold Assessment module was developed to assist employees of agencies to determine, early in the developmental stages of a proposed project, whether that project is likely to require a PIA. It could be deployed as a template on desktops, portable computers or internal websites (provided they are secure) for use by any employee proposing change.
2. If an agency[9] is developing a program, system, legislation or other initiative that involves personal information, the provisions of the *Privacy Act 1988* (the Act) apply. Each agency is responsible and accountable for the personal information it collects, even when the personal information is in the custody of external service providers or contractors operating either in Australia or overseas.

How the Threshold Assessment works

3. The Threshold Assessment basically aims to draw out whether the proposed project involves the collection, use or disclosure of "personal information". The discussion as to what constitutes personal information (below) should be useful in making this assessment.
4. Generally speaking, if personal information is not involved in the project, the project is unlikely to have the degree of impact on information privacy which would necessitate the completion of a PIA. However, a lack of personal information will not necessarily guarantee that there will be no information privacy impact. For example, a project may not involve personal information now, but may present issues if personal information was to become involved down the track. Furthermore, the fact that personal information is not involved in a project does not guarantee that other types of privacy (such as bodily; territorial; communications privacy) are not relevant.[10]
5. As such, whilst the Threshold Assessment is designed to help employees determine whether a PIA is necessary, there is no hard-and-

[9] Most Australian Government and ACT Government agencies are bound by the *Privacy Act 1988*: see sec 6(1) (definition of "agency").

[10] Whilst this Guide deals with information privacy, other types of privacy can also be considered in a project's PIA, especially where such issues may pose risks to the overall success of the project. For a summary of different types of privacy see Banisar D, 2000, *Privacy and Human Rights: an international survey of privacy laws and developments*, Electronic Privacy Information Centre, Washington: www.privacyinternational.org/survey.

fast rule about when to do a PIA. Each project needs to be considered within its own broader context.

What is personal information?

6. A range of factors can be relevant when considering whether "personal information" is involved in a project. The Act defines "personal information" as:

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

7. The Act also defines "sensitive information" as:

   "(a) *information or an opinion about an individual's:*

   I. racial or ethnic origin; or

   II. political opinion; or

   III. membership of a political association; or

   IV. religious beliefs or affiliations; or

   V. philosophical beliefs; or

   VI. membership of a professional or trade association; or

   VII. membership of a trade union; or

   VIII. sexual preference or practice; or

   IX. criminal record;

   that is also personal information; or

   (b) health information about an individual."

8. Personal information does not always need to include an individual's name to be regulated by the Act. It may include information that can be linked to or can identify a specific individual through association or inference.

9. The Act's definitions are culturally neutral. It is therefore important to consider the cultural context in which the personal information will become available. It should not be assumed that the stakeholders or clients operate under the same cultural framework as the record-keeper. So if a record-keeper operates under one cultural/institutional framework and the information becomes available to a particular group in our society, what appears deidentified or unidentifiable to the record-keeper may identify an individual, when placed in the hands of that group.

   For example, generic information such as ethnic origin may not by itself seem to identify an individual. However, if an ethnic identifier is disclosed along with other information and relates to an individual in a small town where there are only a limited number of people of that ethnic

origin, it could identify an individual and therefore become personal information under the Act.

10. Note also that personal information may be collected directly from an individual or indirectly from another source. It would therefore be prudent to consider the concept of "collection" broadly, encompassing for example personal information that flows through the agency as well as real-time online verifications and information from shared databases.
11. The following is a suggested Threshold Assessment template.

Suggested Threshold Assessment Template

1. Agency name.

2. Contact details of the employee responsible for completing this Threshold Assessment.

3. Brief description of the project being proposed.

Section 13 of the Guide (*Project description*) suggests some matters that might be useful for inclusion in this kind of broad project description, e.g.

- the project's overall aims (including how it ties in with the agency's functions or activities);
- the drivers for or reasons behind the project;
- the scope or extent of the project; and
- any links with existing programs.

If the project being proposed involves modifications to an existing program, first describe the current program and then the proposed changes. In these circumstances, it will also be relevant to provide details (if any) of any prior PIAs undertaken in relation to the existing program. If no PIA was undertaken, it may be appropriate to consider whether one should be undertaken now.

4. Does the project being proposed involve the collection, use or disclosure of personal information?

In answering this question, consider whether the project involves the handling of any "personal information" (see *What is personal information?* above). Briefly describe (if any) the elements of personal information that will be collected, used or disclosed (e.g. name, address, date of birth). If so, also explain some of the key privacy elements (e.g. the general purposes for which it will be collected, used and disclosed; any authority under which it is collected; the nature and sensitivity of the personal information; etc).

If the project being proposed involves modifications to an existing program, describe the changes to the handling of any personal information (if any) that would be involved, should the proposal be implemented.

Yes ❑ No ❑

If you have answered YES to question 4 then (subject to paragraphs 4 and 5 above) some form of PIA will probably be necessary. See Section 11 of the Guide (Key stages of a PIA) to continue.

Note: *if you have come to the conclusion that a* ***PIA is necessary****, please ensure that you retain the description of the project compiled at question 3 above. It will be necessary for inclusion in the PIA. Sign off below and retain this Threshold Assessment for your records.*

If you have answered NO to question 4 then (subject to paragraphs 4 and 5 above) a PIA may not be necessary.

Note: *if you have come to the conclusion that a* ***PIA is not necessary****, you should record that you have reviewed the proposal and reached this conclusion by signing off below and retaining this Threshold Assessment for your records.*

_____ _____

(Proponent) (Proponent's manager)

Date: _____ Date: _____

MODULE B Nature of the Project

A broad assessment of the nature of a project will help an agency to decide on the most appropriate PIA process for that project. Such an assessment will generally include looking at the project's:

- **scope:** is it limited or broad?
- **type:** is it a new program, or an alteration to a well-established existing program (an "incremental" project)?
- **stage of development:** is it at a conceptual or a more advanced stage of thinking?

Scope of the project

A project's **scope** can be assessed by looking at the extent to which the project demonstrates certain key attributes, such as the:

- **quantity** of the personal information handled;
- **sensitivity** of the personal information involved, for example information that has biometric or genetic components;
- **significance** of the project, e.g. its size or complexity;
- degree of cross-agency or cross-sector **interaction** which will be required, e.g. sharing or data-matching across agencies, or across jurisdictions, or between the public and private sectors; and
- significance of the **public impact** of the project, for example, through the handling of significant amounts of personal information about each individual, or the handling of personal information about a significant number of individuals.

A project's scope can also broaden, in privacy terms, where it includes features which may tend to increase the risk of adverse privacy impacts. For example, consider whether:

- personal information-handling will be or has been **outsourced**;
- **new legislation or new technology** will be required in relation to the handling of the personal information;
- the aggregation of personal information in **databases** will be involved;
- entirely **new collections** of personal information are planned e.g. as a result of an agency acquiring new functions; and
- a **new method** of using or disclosing personal information is being introduced.

Generally, the greater the scope of the project, the more likely it will be that a PIA will assist in determining and managing the privacy impacts posed by that project, and the more detailed that the PIA is likely to be.

Type of project and stage of development

An agency will also find it useful to consider the **type** of project (e.g. new or incremental?), including the **stage of development** it has reached (e.g. conceptual or more advanced?).

Generally, an incremental project is one which proposes to add or make changes to an existing program or system, rather than implement a new program or system. If a project is incremental, this Guide should generally be read so as to apply to the new personal information flows, unless the agency is of the view that the existing program or system may also benefit from a PIA. Like all projects, incremental projects can range from being limited in scope through to being quite significant in their scope and privacy implications. If it appears that an incremental project is more significant in scope, a more comprehensive PIA may be required.

It is beyond the scope of this Guide to attempt to recommend an appropriate PIA process for all the various types of projects that might be undertaken. However, a few examples of different project types are provided below, to demonstrate how the PIA process can differ for different project types or projects at various stages. These examples are not intended to be exhaustive.

Example A: Incremental projects of limited scope

Where a project is incremental and appears to be relatively limited in scope, a shorter PIA might be all that is required. For example, a project might be considered to be of limited scope if it proposes a relatively minor adjustment to a well-established existing program, or if it involves the collection and use of a very limited amount of personal information (that is not sensitive information) in a secure environment.

Even for projects where a shorter PIA might be found to be appropriate, the PIA process should preferably still address all the key stages (see *11. Key stages of a PIA* above). However, in such circumstances it may, for example, eventuate that:

- the degree of mapping of information flows required is quite small;
- the amount of questions that require answers is relatively low;
- the analysis of the privacy impacts is relatively uncontroversial;
- the privacy impacts are minimal;
- the recommendations might be few; and/or
- the final report might be relatively brief.

Provided such an outcome is warranted by the nature of the project, this will constitute an adequate PIA in the circumstances.

Example B: Projects at conceptual stage of development

For projects at the earlier or conceptual stages of development, it might only be possible for the key stages of a PIA (see *11. Key stages of a PIA* above) to be initially addressed in a preliminary manner. For example, the information flows might only be able to be mapped to the extent of the detail available at the time. This may also mean that only a preliminary analysis of privacy impacts and possible management strategies might be possible.

In these circumstances, the preliminary PIA should be viewed as part of an evolving process. Initially, the PIA can be progressed and documented. As the project develops and the issues become clearer, the PIA can be updated and supplemented, leading to a more comprehensive PIA being completed. In some circumstances (e.g. significant projects), preliminary reports and interim recommendations will be important to ensuring that privacy is built in.

Example C: Significant projects at advanced stages of development

For projects which are at relatively advanced stages of development and which are broad in scope, it is likely that a comprehensive PIA (or, in some circumstances, more than one comprehensive PIA) will be appropriate. A comprehensive PIA will also undertake the key stages of a PIA (see *11. Key stages of a PIA* above), but in a more detailed and thorough fashion.

MODULE C Mapping the Information Flows

The purpose of this stage of the PIA is to describe and map the flows of personal information in the project. The information compiled during this stage will form the basis for the forthcoming analysis of privacy impacts.

The elements of the project that are most likely to be relevant to information privacy impact include:

- the ***collection*** of personal information;
- its ***use*** and ***disclosure***;
- the ability individuals have to ***access*** information about them;
- the ability individuals have to ***correct*** information about them if need be;
- the applicable ***security*** safeguards;
- the processes for ensuring ***data quality***; and
- whether an ***identity management*** system is involved.

The series of questions which appear below is designed to assist agencies in describing how their project deals with each of these areas. In doing so, the questions should also help draw agencies' attention to possible points where information privacy issues might arise.

In this regard, a "***Privacy Risk***" box indicates circumstances where a project may present a risk to individual privacy. This could be by altering an individual's choices about who knows what about them, or by otherwise compromising an individual's autonomy in relation to their personal information.

Any responses to the following questions should be documented for use at the privacy impact analysis stage. The responses will also be useful for any forthcoming PIA reporting documents.

1 Collection

Good collection practices underpin good privacy.

When considering collection, describe:

- how the collection relates to the agency's functions or activities;
- what public interest justifies the collection;
- why the personal information, including the particular data items and kinds of data, is necessary for the project;
- whether the information can be collected in a de-identified or anonymous manner; and
- whether individuals can choose not to provide some or all of the personal information sought.

How will the information be collected? Might some individuals feel that the method of collection is unreasonably intrusive? Examples of unreasonably intrusive collection practices may include requiring individuals to divulge intimate or sensitive information in a public area where others can overhear or collecting video footage of individuals' private activities without their knowledge.

Privacy Risk	Collecting unnecessary or irrelevant personal information, or intrusive collection.

1.1 Scope of collection

Detail the collection process.

Describe:

- the personal information, including the data items to be collected (e.g. name, address, occupation, identification numbers);
- where the information is to be collected from (e.g. from the individual directly, from other individuals, from other agencies or organisations, from publicly available sources);
- whether the information will be paid for or exchanged for something else of value;
- how the circumstances of the individuals involved will be taken into account when the personal information is being collected, e.g. cultural diversity, hearing impairment, languages other than English;
- why each element of the information is being collected (e.g. identify whether some data items are collected for some purposes and other data items for different purposes);
- whether the information to be collected is of a sensitive nature (including, for example, financial information, political or religious beliefs, health, sexual practices, biometric or genetic information);
- any statute, authority or requirement the agency is relying upon to collect the information; and
- alternatives to collection that have been considered and rejected (e.g. using de-identified data).

Where an individual's consent will be sought to the collection of their personal information, outline what other matters may depend on that consent. For example, is a particular service or benefit only available if the individual consents to the collection of some or all of the requested personal information?

Privacy Risk	Bulk collection of personal information, some of which is unnecessary or irrelevant.

1.2 Notice

What do individuals know about the collection?

Personal information should be handled in a transparent way so there are no surprises for the individual. Identify and describe what information is given to the individual about the collection, and how it is given, including:

(a) **Purpose and authority**

- the purpose for which the personal information is being collected;
- whether the collection is authorised or required by law (and, if so, which law?);

(b) **Use and disclosure**

- uses or disclosures that the agency considers consistent with the purpose for collection;
- the people, bodies or agencies to which the collecting agency usually or sometimes discloses personal information (and any further uses and disclosures by those people, bodies or agencies);
- proposed uses or disclosures for purposes other than the purpose of collection; and

(c) **Choice**

- do individuals know they have a choice about the handling of their personal information where these choices exist? Has the agency told them?

Privacy Risk Individuals unaware of collection or its purpose.

1.3 Method of collection

Identify and describe:

- how often the personal information is to be collected (e.g. only on one occasion or ongoing);
- any potentially sensitive or intrusive methods of collection (including photographs, fingerprinting, iris scanning, drug testing and the collection of genetic information, for example, through buccal swabs);
- any covert methods of collection, such as surveillance, and why they are necessary and appropriate (e.g. some website cookies and surveillance devices including electronic listening devices and cameras); and
- whether the technology is privacy enhancing or privacy invasive, and why.

Privacy Risk	Covert collection is generally highly privacy invasive, and should only occur under prescribed circumstances.

2 Use

No surprises! Use personal information in ways that are expected by the individual.

Generally speaking, "use" refers to what happens to personal information in the hands of the collector.

2.1 Use

Identify and describe:

- all the uses of the personal information (including ones which may be expected but uncommon);
- how all these uses relate to the purpose for which the personal information was collected;
- any changes to the purpose for using the information after the information is collected; and
- measures in place to prevent use for secondary purposes.

2.2 Secondary purposes

If the information collected may be used for an additional or secondary purpose, identify and describe:

- whether consent is required for the secondary use;
- if the use is directly related to the purpose of collection;
- whether an individual can decline the secondary use and still be involved in the project; and
- if new, unplanned purposes for handling personal information arise in the life of the project, the extent to which individuals will be involved in decisions about these new purposes.

Privacy Risk Using personal information for unplanned secondary purposes.

2.3 Data linkage / matching

Aggregation or the bringing together of diverse groups of personal information collected for different purposes, either in the agency or by another agency or organisation, has privacy risks. For example, it may reveal personal information not previously available, or it may reveal information not necessary for the purpose at hand.

Identify and describe:

- any intention or potential for the personal information to be linked, matched or cross-referenced to other information held in different databases (held by the agency or by other agencies or organisations);[11]
- how this linkage, matching or cross-referencing might be done;
- any decisions affecting the individual that are to be made on the basis of such datamatching, linking or cross-referencing;
- what safeguards will be in place to limit inappropriate access, use and disclosures of the resulting information;
- what mechanisms will be in place to ensure audit trails and appropriate back-ups; and
- what protections are in place to ensure the accuracy of the data linkage and that individuals will not be adversely affected by erroneous data matching; for example, have individuals been informed of the data linkage?

Privacy Risk	Unnecessary or unplanned data linkage.

[11] Also see the OPC's *Guidelines for the Use of Data-Matching in Commonwealth Administration* at www.privacy.gov.au/publications/p6_4_23.doc.

3 Disclosure

No surprises! Tell the individual about disclosures.

Generally speaking, “disclosure” refers to the process of releasing personal information outside the control of an agency.

Identify and describe:

- to whom and under what circumstances the personal information will be disclosed and why;
- whether the personal information disclosed to others outside the agency will be protected from privacy risks in the same way as information held by the agency (e.g. covered by the Privacy Act, or by a similar privacy law);
- if the information is to be published, or disclosed to a register, e.g. a public register;
- whether the individual has been told about the disclosure and what choices they have (including about the publication or suppression of their information); and
- whether the disclosure is authorised or required by law, specifying the relevant provisions.

Privacy Risk Disclosures not originally planned can lead to privacy complaints.

4 Access and correction

Getting access to personal information should be clear and straightforward.

Identify and describe:

- how an individual can access their personal information (including any costs incurred by the individual); and
- how the individual can have the information about them corrected, or annotations made, if necessary.

Privacy Risk Inaccurate information can cause problems for agencies and individuals.

5 Security

Logical (IT) and physical security measures.

Describe:

- what security measures will be taken to protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse, including how data is transferred between sites;
- what security measures will be taken to protect personal information where its handling will be or has been outsourced to external agencies or organisations;
- who will have access to the information, and who authorises those access rights;
- the systems in place to prevent and detect misuse of, or inappropriate access to, the personal information; and
- what action will be taken if there is a security breach (e.g. informing individuals of the breach).

Assess the project against agency IT plans and physical security, e.g. use of lap-tops, encrypted media for disks, access to sites and systems.

Privacy Risk Unauthorised internal and external access and use.

5.1 Retention and destruction

Identify and describe the retention and destruction practices to be employed in the project, including:

- when personal information is to be de-identified or destroyed;
- how this is to be done and whether it will be done securely;
- whether a data retention policy and destruction schedule is in place; and
- how compliance with the data retention policy and any relevant legislation relating to record destruction will be measured.

Privacy Risk	Retaining personal information unnecessarily.

6 Data quality

Identify and describe:

- the consequences for individuals if the personal information is not accurate or up-to-date (e.g. the kinds of decisions made on the basis of the information; the risks to the agency and the individual posed by inaccurate information);
- how information will be kept up-to-date;
- the processes to ensure that the data is only used or disclosed when it is relevant, up-to-date and complete; and
- the updates and modifications to personal information which will be disseminated to others outside the agency to whom personal information has been disclosed.

Privacy Risk	Making decisions based on poor quality data.

7 Identity management

Don't authenticate identity unless necessary.

Agencies handling personal information may require identity management systems and processes robust enough to identify, to an appropriate level of confidence, the individuals whose personal information they are dealing with.[12]

Identify and describe:

- to what extent the project can proceed through the handling of anonymous or de-identified information;
- whether it is necessary to authenticate identity, and to what degree of confidence (e.g. taking into account a consideration of the value of the transaction);
- how evidence of identity is to be authenticated;
- whether the project involves the issuing of a new identification number to individuals, and its purpose;
    - this includes whether the new identification number could potentially be used for other purposes or adopted by other agencies or private sector organisations, and, if so, what protections could be put in place to address this;
- any expected uses and disclosures of this or other identification numbers (by any agency or organisation); and
- individual attributes, other than identity, that need to be authenticated (e.g. that an individual has a certain qualification).

[12] See also "*Proof of ID Required? Getting Identity Management Right.*" www.privacy.gov.au/publications/index/html#S.

MODULE D Privacy Impact Analysis

The privacy impact analysis stage of a PIA investigates how the information flows in a project affect the choices individuals have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law, and how the project fits into community expectations.

Key questions to be answered through the privacy impact analysis phase of a PIA include the following:

- Does the project comply with privacy legislation (see ***Module E***) and agency-specific legislative requirements?
- Do individuals have to give up control of information about themselves to any degree?
- Will it require, or is it likely to result in, individuals changing their behaviour (e.g. having to present identification in more circumstances), or incurring costs?
    - Will the project impact disproportionately on individuals or groups without identity documentation?
- Will decisions that have consequences for individuals be made on the basis of the personal information handled in the project (e.g. decisions about services or benefits)?
    - Does the project deliver the right amount of accurate and relevant information to adequately inform these decisions?
- Is there provision for complaint-handling mechanisms, in the event that privacy breaches eventuate?
- Have emergency procedures been devised in the event that the system fails?
- Is there provision for audit and oversight mechanisms, including emergency procedures in the event that the system fails?
- Does the project include the potential for function creep (e.g. might there be an interest in using the personal information collected for the project, for other purposes) or other unplanned consequences?
- Assess the value of the information to unauthorised users (e.g. is it information that others would pay money or expend effort to gain access to)?
- Is any intrusion (physical or on property) or surveillance (whether covert or overt) fully justified and proportional to the outcome?
    - Is it the only way of achieving the aims of the project?
    - Is it done in the least intrusive manner?

    - Is it subject to legislative or judicial authority?
- How consistent is the project with community values about privacy (e.g. does it involve new ways of identifying individuals, the creation of significant databases or the use of genetic material or information)?
- How has privacy been factored in the project's cost-benefit analysis, and the analysis of the project's return on investment?

MODULE E IPP Compliance Checklist

This IPP Compliance Checklist aims to assist employees proposing change to investigate whether the personal information aspects of their project comply principally with the IPPs in section 14 of the Privacy Act.

Module E has been designed to be deployed as a template on desktops, portable computers (provided they are secure) or internal websites for use by any employee proposing change. Where so adopted by agencies, the module may need to be modified to add agency-specific details. For example, some agencies have processes that need to be completed where changes to computer software and/or hardware are contemplated. It would be more user-friendly if the PIA and such agency-specific processes were linked electronically. It would also usually assist the PIA process if a summary or copy of the documentation for those linked processes were attached to the PIA documentation, where relevant.

It should be noted that many terms used in the IPPs and NPPs have specific meanings, and it would be prudent to refer to the Privacy Act's definition for those terms. Another useful source for guidance in this regard is the Privacy Commissioner's IPP/NPP Guidelines (published on the Privacy Commissioner's website at www.privacy.gov.au). This module provides web addresses for the relevant Guidelines at the foot of the boxed text that summarises each IPP/NPP. Users are encouraged to refer to the Guidelines before responding to the questions asked in this module, and if necessary to seek further guidance from sources such as the agency's Privacy Contact Officer, legal unit or external guidance.

A) Information Privacy Principles (IPPs)

1) IPP 1 – Manner and purpose of collection

Personal information shall not be collected for inclusion in a record, or in a generally available publication, unless:

- for a lawful "purpose" directly related to a "function" or "activity" of the collector AND
- necessary for or directly related to that purpose.

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

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_14.4.pdf.)

1) Is the information to be collected for a lawful purpose directly related to a function or activity of the collector?

Yes ❑ No ❑

(If yes, please specify the "purpose" of collection and the relevant "function" or "activity" to which it is directly related. In particular, if the collection is "authorised" or "required" by, or under, a specific Act, regulation or determination, please specify details of the nature of this authority (n.b. this information will also be relevant to Question 3 under IPP 2 below). If no, please indicate what alternatives are proposed.)

2) Will the information collected be "necessary for" or "directly related to" that purpose?

Yes ❑ No ❑

(If yes, please indicate how it is "necessary for" or "directly related" to the relevant purpose. If no, please indicate what alternatives are proposed.)

3) Will the information be collected by "lawful" and "fair" means?

Yes ❑ No ❑

(If yes, please specify the "lawful" and "fair" means proposed. If no, please indicate what alternatives are proposed.)

If you answered "No" to any of the questions above, your agency may not have authority under the Privacy Act to collect the personal information in question. You may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

2) IPP 2 – Solicitation of personal information from the individual concerned

Where a collector collects personal information for inclusion in a record or in a generally available publication, and the information is solicited by the collector from the individual concerned, the collector shall take such steps (if any) as are, in the circumstances, "reasonable" to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware:

- of the purpose for which the information is being collected;
- if the collection of the information is "authorised or required by or under law" – the fact that the collection of the information is so "authorised" or "required"; and
- any person to whom, or any body or agency to which, it is the collector's "usual" practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_14.4.pdf.)

1) Is the personal information to be solicited by the collector from the individual concerned?

Yes ❑ No ❑

(If yes, please detail how the information is to be solicited. If no, please detail why it will not be collected from the individual concerned, including the authority for not doing so, if relevant.)

If information is not to be solicited from the individual concerned, you may not need to address all of the following three questions. It is however prudent to err on the side of caution and answer them in any case, as there may be privacy risks, including potential inaccuracy, when personal information is not collected directly from the individual (see *1. Collection* in ***Module C***).

2) Will “reasonable steps” be taken to inform the individual of the purpose of the collection?

Yes ❑ No ❑

(If yes, please specify what “reasonable steps” will be taken. If no, please indicate why not.)

3) If the collection is to be “authorised” or “required” by law, will the individual be so advised?

Yes ❑ No ❑

(If yes, please specify which law and how the individual will be advised. If not, please indicate why not.)

4) Will the individual be advised about the “usual disclosures”?

Yes ❑ No ❑

(If yes, please list the proposed “usual” disclosures and specify how the individual will be advised. If no, please indicate why not.)

If you have answered “No” to questions 2, 3 or 4 above, your agency may not be able to collect, use or disclose the personal information in question. You may need to seek further advice (e.g. from your agency’s Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

3) IPP 3 – Nature and method of personal information solicited

Agencies must take "reasonable steps" to ensure that solicited personal information collected is relevant to the purpose of collection, up to date and complete, and is not collected in an "unreasonably intrusive way".

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_14.4.pdf)

1) Will "reasonable steps" be taken to ensure that any solicited personal information collected is "relevant", "up to date" and "complete"?

Yes ❑ No ❑

(If yes, please specify what the steps will be. If no, please indicate why not.)

2) Will reasonable steps be taken to ensure that the information will be collected in a way that does not "unreasonably intrude" on the individual?

Yes ❑ No ❑

(If yes, please specify what the steps will be. If no, please indicate why not.)

If you have answered "No" to either of the questions above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

4) IPP 4 – Storage and security of personal information

A record-keeper who has possession or control of a record shall ensure:

- that, by "reasonable" security safeguards, the record is protected against loss, unauthorised access, use, modification or disclosure, and against other misuse; and
- if given to a person in connection with the provision of service to the record-keeper, that everything is "reasonably" done to prevent "unauthorised" use or disclosure of information in the record.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf.)

If your proposed changes involve modifications to information or computer technology, you may have to complete other agency-specific processes. If so, it may be useful to attach a summary or a copy of the documentation from that process to this PIA as relevant, and particularly where information flows are to be modified.

Note: For assessments related to new or existing Information or Computer Technology (ICT) systems, this section should be completed by the unit in the agency responsible for systems maintenance and security and signed off by the unit's manager.

a) Security safeguards[13]

1) Will there be "reasonable technical security" in place to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse?

Yes ❑ No ❑

(If yes, please specify what they will be and how they will prevent loss, unauthorised access, use, modification or disclosure, or other misuse. If no, please indicate why not.)

2) Will there be "reasonable physical security" in place to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse?

Yes ❑ No ❑

(If yes, please specify what they will be and how they will prevent loss, unauthorised access, use, modification or disclosure, or other misuse. If no, please indicate why not.)

3) Will there be work unit policies and procedures in place for the security of personal information during the handling (routine and ad hoc) of the information?

Yes ❑ No ❑

(If yes, please specify what those policies and procedures will be and how they will protect information during handling. If no, please indicate why not.)

[13] Acknowledgment is given to the British Columbia Office of the Information and Privacy Commissioner's *Privacy Impact Assessment Template* (see www.oipcbc.org/sector_public/resources/pia.htm).

4) Will controls and procedures be created for the authority to add, change or delete personal information?

Yes ❑ No ❑

(If yes, please specify what they will be. If no, please indicate why not.)

5) Will your system security include an ongoing audit process that can track use of the system, including for back-up materials (e.g. when and who accessed, and if those processes collect personal information will they themselves have privacy protections built in)?

Yes ❑ No ❑

(If yes, please specify what the process will be and how they will protect privacy. If no, please indicate why not.)

6) Will audit mechanisms identify inappropriate accesses to the system?

Yes ❑ No ❑

(If yes, please specify how and what the consequences will be. If no, please indicate why not.)

b) Safeguarding information provided to external parties

An agency must do everything it "reasonably" can to prevent unauthorised use or disclosure of information it provides to external parties providing a service to the agency, whether private sector contractors or overseas agencies or organisations.

1) Will the contractual obligation imposed by the agency on the external party comply with section 95B of the Privacy Act?[14]

Yes ❑ No ❑

(If yes, please specify the relevant provisions in the proposed contract. If no, please indicate why not.)

2) Will the contract include requirements inconsistent with NPPs 7-10?

Yes ❑ No ❑

(If yes, please specify the proposed inconsistencies and the reasons for them.)

[14] In relation to section 95B, see the Privacy Commissioner's Information Sheet 14 – "Privacy Obligations for Commonwealth Contracts" (www.privacy.gov.au/publications/IS14_01.html); the Australian Government Solicitor's Legal Briefing No 63 – "Outsourcing: Agency Obligations under the Privacy Act" (www.privacy.gov.au/publications/LB.pdf) and also IPP 11.3.

3) Will the agreement with a State/Territory government or agency/body or the arrangement with a foreign government, agency, body or organisation include explicit undertakings that the recipient will afford the same privacy restrictions and protections as the information receives in the hands of the Commonwealth agency, including against different third party uses and disclosures?

(N.B. It may be helpful to also consider IPP 11.3 obligations (see below) at this point.)

Yes ❑ No ❑

(If yes, please specify the proposed undertakings; indicate which Privacy Act protections they exclude, if any; and how adherence will be monitored. If no, please indicate why not.)

If you have answered "No" to any of the questions above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

5) IPP 5 – Information related to records

A "record-keeper" in "possession" or "control" of personal information shall:

- unless "authorised by law" to refuse to do so, take such steps as are "reasonable" to enable any person to ascertain:
  - whether the "record-keeper" has possession or control of personal information,
  - the nature of that information,
  - the purposes for which that information is used, and
  - the steps which need to be taken if the person wishes to gain access to their records;
- maintain a record setting out the:
  - nature of records kept,
  - purpose of each type of record,
  - classes of individual about whom records are kept,
  - period for which each type of record is kept,
  - persons entitled to, and the conditions under which they may have, access to the records, and
  - steps to be taken by an individual wishing to access their records; and
- ensure that:
  - the record maintained above is made available for public inspection, and
  - a copy of this record is given to the Privacy Commissioner in June each year.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf.)

1) Will the “record-keeper” be “authorised by law” to refuse to inform any person of the records in the record-keeper’s possession or control?

Yes ❑ No ❑

(If yes, please indicate which law will be relied upon and how the discretion will be exercised.)

2) Will processes be put in place to satisfy the above requirements?

Yes ❑ No ❑

(If yes, please specify how each of these criteria will be satisfied. If no, please indicate why not.)

If you have answered "No" to question 2 above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

6) IPP 6 – Access

Individuals shall be entitled to have "access to records", except to the extent the record-keeper is "required" or "authorised" to refuse access under any law of the Commonwealth that provides access by persons to documents.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. The qualification in this IPP effectively grants access to information on the basis of the rights available under the *Freedom of Information Act 1982.* For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf.)

1) Will processes be put in place to provide access to records under the relevant Commonwealth law (e.g. *Freedom of Information Act 1982; Archives Act 1901)*?

Yes ❑ No ❑

(If yes, please specify the proposed processes. If no, please indicate why not.)

If you have answered "No" to the question above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

7) IPP 7 – Alteration of records

A "record-keeper" shall take "reasonable steps", subject to any Commonwealth law that provides a right to require correction or amendment of documents, to ensure that the record is accurate and, having regard to the purpose of collection or use, that the record is relevant, up to date, complete and not misleading.

Where the "record-keeper" is unwilling to amend a record in accordance with a request by the individual concerned and no decision or recommendation to the effect that the record should be amended is made under the provisions of a law of the Commonwealth, the "record-keeper" shall on request attach any statement by the individual concerned correcting, deleting or adding to the record.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf.)

1) Will reasonable steps be taken to ensure accuracy, relevance, currency, completeness of records and that they are not misleading?

Yes ❑ No ❑

(If yes, please describe the reasonable steps. If no, please indicate why not.)

2) Will provision be made for attaching corrections?

Yes ❑ No ❑

(If yes, please specify the provisions. If no, please indicate why not.)

8) IPP 8 – Record-keeper's obligation to check accuracy etc

"Record-keepers" shall not use personal information without taking "reasonable steps" to ensure the accuracy, currency and completeness of the information.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/ipp8_11.pdf.)

1) Will processes be put in place to ensure accuracy, currency and completeness before information is used?

Yes ❑ No ❑

(If yes, please specify the proposed processes. If no, please indicate why not.)

If you have answered "No" to the question above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

9) IPP 9 – Use only for relevant purposes

A "record-keeper" shall not use information except for a purpose to which the information is relevant.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/ipp8_11.pdf.)

1) Will relevance be tested before use?

Yes ❑ No ❑

(If yes, please specify how it is proposed that relevance will be tested. If no, please indicate why not.)

If you have answered "No" to the question above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

10) IPP 10 – Limits on use for other purposes

1) A "record-keeper" shall not "use" information obtained for a particular purpose for any other purpose unless:

a) the individual has consented to use for that other purpose; or

b) on reasonable grounds, use for that other purpose is "necessary" "to prevent or lessen a serious and imminent threat to life or health"; or

c) use for that other purpose is "authorised or required by or under law"; or

d) use for that other purpose is "reasonably necessary" for "enforcement of criminal law" or a "law imposing a pecuniary penalty", or to "protect public revenue"; or

e) use for that other purpose is "directly related" to the purpose for which the information was obtained.

2) Where used for d) above, the record-keeper shall record that use in the record of the information concerned.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/ipp8_11.pdf.)

"**Use**" in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication.

By way of guidance, "use" refers to what may happen to the personal information in the hands of the collector/record-keeper. "Disclosure" refers to the process of releasing personal information from the control of the record-keeper.

"**Consent**" means express consent or implied consent.

1A) Will the individual the personal information is about be asked to consent to the proposed use for other purpose(s)?

Yes ❑ No ❑

(If yes, please specify how consent will be sought and describe the other purpose(s). If no, please indicate why consent will not be relied upon and describe the other purposes.)

1B) Will a record be kept of whether the consent was “express” or “implied”?

Yes ❑ No ❑

(This is not strictly an IPP requirement, but it is nonetheless an important matter to consider. If no record will be kept, please indicate why. If proposing to rely upon implied consent, please specify basis for so doing.)

2) Will there be processes or guidance in place to assist the record-keeper determine what constitutes “necessary to prevent or lessen a serious and imminent threat to the life or health” of a person, before invoking this exemption?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance. If no, please indicate why not.)

3) Will there be processes or guidance in place to assist the record-keeper determine whether a proposed other purpose is either “required” or “authorised” by or under law, before invoking this exemption?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance. If no, please indicate why there will be no processes or guidance.)

4) Will there be processes or guidance in place to assist the record-keeper determine what is “reasonably necessary” for enforcement of a “criminal law”, “pecuniary penalty” or “protection of the public revenue”, before invoking this exemption?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance related to satisfying the “reasonably necessary” test, and determining the law(s) that will be relied upon. If no, please indicate how the record-keeper will satisfy the “reasonably necessary” test and determine the relevant law(s).)

5) Will there be processes or guidance in place to assist the record-keeper determine what “directly related purposes” are?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance related to satisfying the “directly related purpose” test. If no, please indicate how the record-keeper will satisfy the “directly related purpose” test.)

6) Will there be processes in place to allow the record-keeper to record that a use under IPP 10(d) has occurred?

Yes ❑ No ❑

(If yes, please specify the proposed processes. If no, please indicate why not.)

If you have answered “No” to any of the questions above, you may need to seek further advice (e.g. from your agency’s Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

11) IPP 11 – Disclosure

1) A "record-keeper" shall not "disclose" information to a person, body or agency (other than the individual concerned) unless:

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

b) the individual has "consented" to the disclosure; or

c) the record-keeper believes on "reasonable grounds" that the disclosure is "necessary" to "prevent or lessen a serious and imminent threat to life or health"; or

d) disclosure is "required or authorised by or under law"; or

e) disclosure is "reasonably necessary" for "enforcement of criminal law" or a "law imposing a pecuniary penalty", or to "protect public revenue".

2) Where disclosed for e) above the "record-keeper" shall record that use in the record of the information concerned.

3) A person, body or agency to whom such personal information is disclosed shall not use or disclose the information for a purpose other than the purpose for which it was disclosed to it.

(NB This is a summary of the IPP only. Please refer to section 14 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this IPP see www.privacy.gov.au/publications/ipp8_11.pdf.)

1) Will processes be put in place to make individuals aware of the usual disclosures and to assist the record-keeper determine whether the individual was "reasonably likely to have been aware" of such disclosures?

(NB The responses to the IPP 2 questions will be relevant.)

Yes ❑ No ❑

(If yes, please specify the proposed processes. If no, please indicate why not.)

2A) Will the individual whose personal information is to be disclosed have consented to the disclosure(s)?

Yes ❑ No ❑

(If yes, please specify how consent will be sought and describe the proposed disclosure(s). If no, please indicate why consent will not be relied upon and describe the proposed disclosure(s).)

2B) Will a record be kept of whether the consent was "express" or "implied"?

Yes ❑ No ❑

(This is not strictly an IPP requirement, but it is nonetheless an important matter to consider. If no record will be kept, please indicate why. If proposing to rely upon implied consent, please specify basis for so doing.)

3) Will there be processes or guidance in place to assist the record-keeper determine what constitutes "necessary to prevent or lessen a serious **and** imminent threat to the life or health" of a person, before invoking this exemption?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance. If no, please indicate why not.)

4) Will there be processes or guidance put in place to assist the record-keeper determine whether a proposed disclosure is either “required” or “authorised” by or under law, before invoking this exemption?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance. If no, please indicate why there will be no processes or guidance.)

5) Will there be processes or guidance in place to assist the record-keeper determine what is “reasonably necessary” for enforcement of a “criminal law”, “pecuniary penalty” or “protection of the public revenue”, before invoking this exemption?

Yes ❑ No ❑

(If yes, please specify the proposed processes or guidance related to satisfying the “reasonably necessary” test, and determining the relevant law(s) that will be relied upon. If no, please indicate how the record-keeper will satisfy the “reasonably necessary” test and determine the relevant law(s).)

6) Will there be processes put in place to allow the record-keeper to record that disclosure under IPP 11(e) has occurred?

Yes ❑ No ❑

(If yes, please specify the proposed processes. If no, please indicate why not.)

7) Will there be processes put in place to ensure that the person, body or agency to whom disclosure has been made will only use or disclose such information for the purposes for which the disclosure was made to that person, body or agency?

(N.B. The responses to some of the IPP 4 questions will be relevant.)

Yes ❑ No ❑

(If yes, please specify the proposed processes and how compliance will be monitored. If no, please specify why processes will not be put in place and how this requirement will be satisfied.)

If you have answered "No" to any of the questions above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this IPP.

B) Commonwealth Contracts

Under section 95B of the Act, agencies are required to ensure that a "contracted service provider" under a Commonwealth contract does not do any act that would breach the IPPs. "Contracted service providers" are also required to comply with the NPPs, unless the contract provides otherwise. There are four NPPs which have no IPP equivalents, and these are listed below. Agencies should include provisions relating to these when contracting services.

Agencies should also ensure, pursuant to section 16F of the Act, that any personal information collected under a Commonwealth contract is not used or disclosed for direct marketing unless the contract so requires.

"Contracted service provider", for a government contract, is defined as: *"...an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or a subcontractor for the government contract".*

1) NPP 7 – Identifiers

An "organisation", other than a prescribed organisation, must not adopt as its own "identifier" of an individual an identifier assigned by an agency, and must not use or disclose an identifier assigned by an agency unless necessary to fulfil an agency obligation, or for "law enforcement and similar purposes".

(NB This is a summary of the NPP only. Please refer to Schedule 3 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this NPP see www.privacy.gov.au/publications/nppgl_01.pdf.)

"Identifier" is defined as including: "...*a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an identifier*."

"Organisation" means:

(a) an individual; or
(b) a body corporate; or
(c) a partnership; of
(d) any other unincorporated association; or
(e) a trust;

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory."

1) Is the organisation a "prescribed organisation" for the purposes of NPP 7?

Yes ❑ No ❑

(If yes, please specify the prescribing instrument and its relevance to any proposed disclosures. If no, please answer questions 2 to 4 below.)

2) Will the agency disclose any "assigned identifiers" to an organisation for any purpose?

Yes ❑ No ❑

(If yes, please specify any intended organisations and purposes. If no, please proceed to NPP 8 questions below.)

3) Will steps be taken to ensure that the organisation does not adopt a Commonwealth identifier as its own?

Yes ❑ No ❑

(If yes, please specify what steps will be taken and how compliance will be monitored. If no, please specify why it will be appropriate to have an organisation adopt a Commonwealth identifier as its own, and how it is proposed to comply with the Privacy Act.)

4) Will steps be taken to ensure that the organisation does not use or disclose Commonwealth identifiers, beyond its obligations to the agency?

Yes ❑ No ❑

(If yes, please specify what steps will be taken and how compliance will be monitored. If no, please specify why not; why it will be necessary for the organisation to use or disclose Commonwealth identifiers; and how it is proposed to comply with the Privacy Act.)

If you have answered "No" to questions 2, 3 or 4 above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this NPP.

2) NPP 8 – Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

For the Privacy Commissioner's Guidelines in relation to this NPP see www.privacy.gov.au/publications/nppgl_01.pdf.

1) Will individual have the option not identifying themselves for any specified transactions with the organisations?

Yes ❑ No ❑

(If yes, please specify how this will be done. If no, please specify why an anonymous option will not be provided, and describe the relevant transactions.)

If you have answered "No" to the question above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this NPP.

3) NPP 9 – Transborder data flows

An "organisation" in Australia or an external Territory may only transfer personal information to a foreign country if:

- the recipient is subject to a law, binding scheme or contract which upholds information handling principles similar to the NPPs; or
- the individual "consents" to the transfer; or
- the transfer is "necessary for the performance of a contract" between the individual and the organisation, or for "necessary pre-contractual measures" taken in response to the individual's request; or
- the transfer is necessary for the conclusion or performance of a contract, in the interest of the individual, between the organisation and a third party; or
- all of the following apply:
  - the transfer benefits the individual; and
  - it is "impractical to obtain consent"; and
  - if it were practical, the individual would be likely to consent; or
- the organisation has taken "reasonable steps" to ensure that the information will not be held, used or disclosed by the recipient inconsistently with the NPPs.

(NB This is a summary of the NPP only. Please refer to Schedule 3 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this NPP see www.privacy.gov.au/publications/nppgl_01.pdf.)

1) Is it proposed that personal information, managed under a contract with an organisation, will be transferred to a foreign country?

Yes ❑ No ❑

(If yes, please specify which NPP 9 provisions will be relied upon for the proposed transfer; the proposed contractual provisions; which countries or third parties will be involved; and how compliance will be monitored.)

2) If no foreign transfer is contemplated, will the contract with an organisation still provide for NPP 9 protections?

Yes ❑ No ❑

(This is not strictly an IPP requirement, but is nonetheless worth considering in case foreign transfers are not originally intended but later become necessary. If yes or no, please specify why.)

If you have answered "Yes" to question 1 above but have not specified how the requirements of NPP 9 will be satisfied, or which countries or third parties will be involved, or if you have answered "No" to question 2, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this NPP.

4) NPP 10 – Sensitive information

An "organisation" must not collect "sensitive information" about an individual unless:

- the individual has "consented"; or
- the collection is "required by law"; or
- the collection is "necessary to prevent or lessen a serious and imminent threat to the life or health of an individual", where the individual is "physically or legally incapable of giving consent" or "cannot communicate consent"; or
- if the information is collected in the "course of the activities" of non-profit organisations, provided the conditions in NPP 10.1(d)(i) and (ii) are met; or
- the collection is "necessary for the establishment, exercise or defence of a legal or equitable claim"; or
- the conditions set out under NPP 10.2 to 10.4 are satisfied.

(NB This is a summary of the NPP only. Please refer to Schedule 3 of the Privacy Act for the full text. For the Privacy Commissioner's Guidelines in relation to this NPP see www.privacy.gov.au/publications/nppgl_01.pdf.)

An organisation will only be a "**non-profit organisation**" under this NPP if it has

> *"...racial, ethnic, political, religious, philosophical, professional trade, or trade union aims."*

1) Is it proposed that sensitive information be collected under a Commonwealth contract?

Yes ❑ No ❑

(If yes, please specify the reason for collection and the protections proposed to be put in contractual arrangements for that collection. If no, please proceed to the next section.)

2) If sensitive information is to be collected, is it proposed to outsource the collection and management of such information?

Yes ❑ No ❑

(If yes, please specify which NPP 10 provisions will be relied upon; how the sensitive information is to be protected; and how compliance will be monitored. If no, please proceed to the next section.)

If you have answered "Yes" to questions 1 or 2 above, you may need to seek further advice (e.g. from your agency's Privacy Contact Officer; other agency expert; legal advice) regarding compliance with this NPP.

IPP COMPLIANCE - CONCLUSIONS

(Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the IPPs. This could include indicating whether some changes or refinements to the project might be warranted. Modules D and F of this Guide will assist when considering what responses might be appropriate to any privacy challenges that arise.)

_____ _____

(Proponent) (Privacy Contact Officer)

Date: _____ Date: _____

MODULE F Privacy Management

The following are some examples of matters which agencies could take into account when considering actions or responses which might appropriately be taken in relation to any negative privacy impacts identified in the PIA.

- **Balancing interests:** provide an appropriate balance between the goals of the project, the interests of the agency and those of individuals who may be affected. Put yourself "in the shoes" of an individual whose personal information is affected by the project. How would ordinary individuals react?
- **Minimum standards:** ensure a minimum standard of privacy protection for individuals affected by the project (the IPPs may not apply in all circumstances or situations). Consider in particular situations where the project involves the transfer of personal information across public or private sectors, or across jurisdictions, including the adequacy of privacy protection and regulatory oversight.
- **Proportionality:** ensure that any privacy infringement is proportional to, or appropriately balanced with, any benefits gained from the infringement. What is the likelihood of achieving the benefits?
- **Transparency and accountability:** ensure that measures affecting privacy are transparent to individuals, through adequate notice and the availability of privacy policies, and that agencies are accountable for how they handle personal information, including through effective complaint-handling, audit and oversight.
- **Flexibility:** be sufficiently flexible to take account of the diversity of individuals affected by the project. Do some individuals have heightened sensitivities, for example, about the personal information involved in the project?
- **Deliverable promises:** ensure that privacy protections are followed through by including them in law or other binding obligations, and by building them in to new technology.
- **Privacy Enhancing Technology:** carefully consider any available privacy enhancing technologies, as well as the impacts of implementing privacy invasive technologies.
- **Review after implementation:** Did the project meet its primary objectives? How will the project's privacy impacts be assessed: e.g. in an internal audit; implementation assessment, an Australian National Audit Office or OPC audit, or scrutiny by a Parliamentary committee?