Top Ten Dos and Don'ts for Privacy Impact Assessments

Office of the Privacy Commissioner of Canada

1. Do – Start Early

Conducting a Privacy Impact Assessment (PIA) is a valuable method for identifying privacy risks and preparing mitigation strategies; however, to get the maximal benefit from the process, we recommend that you begin at the outset of program development. When privacy risks are identified early, mitigation strategies can be incorporated into the design of the program or activity.

2. Do – Consider the Scope

Some PIAs do not adequately identify and assess the privacy risks of programs or initiatives because the scope of what needs to be assessed is not clearly defined from the beginning. Before submitting your PIA, ensure that it clearly describes what is and is not being assessed and that the data flow diagram included in the report is consistent with the scope. For larger or complex programs and initiatives, it may be beneficial to conduct several smaller, more modular PIAs with clearly defined scopes. Remember to also include copies of all relevant documentation with your PIA. Documents provided as part of a PIA submission should be relevant to the scope and pertinent to a review of the program and its associated privacy risks.

3. Don't – Forget to Read up

Our Office has produced guidance documents addressing various privacy issues such as biometrics, cloud computing, mobile apps, covert and overt video surveillance. Visit our website at www.priv.gc.ca to consult our most up-to-date guidance which may help you throughout the PIA process.

4. Do – Meet Expectations

Our guidance document *Expectations: A Guide to Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada* and our complimentary video *Why think about privacy?: A guide to the Privacy Impact Assessment process* are two resources to help you. They provide an overview of the type and depth of information that should be provided by government institutions when submitting final PIA reports. If you are new to PIAs, the Expectations document and the PIA video are great places to begin.

Expectations is available online at:
http://www.priv.gc.ca/information/pub/gd_exp_201103_e.pdf
Why think about privacy? Video can be viewed online at:
http://www.priv.gc.ca/resource/videos/2013/pia_2013_index_e.asp

5. Don't – Do it Alone

During the PIA process, it is important to consider how your program, product or initiative may impact others. Consulting with stakeholders both within and outside your organization can help ensure that all risks to privacy are identified. The privacy experts within your own organization are valuable partners, as they can provide you with advice and recommendations on privacy issues and national and international privacy standards to be considered. Increasingly, government institutions are sharing services centrally, or are collaborating with each other on programs and initiatives. Under these circumstances, the Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment* recommends that a multi-institutional PIA be completed in order to assess the privacy risks of all implicated institutions.

The TBS directive is available online at:
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18308

6. Do – Remember the Technicalities

As the use of information technology solutions for a variety of functions increases across the Government of Canada, it is essential that potential risks to privacy posed by these technologies are assessed and mitigated. The TBS and the Communication Security Establishment (CSE), among others, have created standards and guidelines of which institutions should be aware when completing a PIA. For example, TBS' *Operational Security Standard: Management of Information Technology Security* (MITS) requires that a Threat and Risk Assessment (TRA) must be conducted for every program, system or service. TRAs and PIAs should serve as complementary processes given that technical risks identified in a TRA can often serve as an input to a PIA.

The TBS *Operational Security Standard* is available online at:
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text

7. Don't – Keep it to Yourself

Since 2010, the TBS *Directive on Privacy Impact Assessment* has required that institutions provide a copy of all PIAs to both our Office and to TBS. In support of openness and transparency, the Directive requires that certain sections of a PIA be made publicly available, most commonly in the form of a summary on the institution's website.

8. Don't – Forget to Put the Plan into Action

The PIA process facilitates early identification of privacy risks. In order to be effective, the mitigation measures identified in a PIA report must be implemented and tracked. PIAs should include detailed action plans for proposed mitigation measures, including timelines and target completion dates, as well as assign a specific position or individual with responsibility for implementation. Consult your action plan regularly to ensure that mitigation measures are implemented as scheduled and that all identified privacy risks are addressed.

9. Do – Keep it Fresh!

As initiatives are implemented and evolve, new privacy risks may arise. PIAs should be updated regularly to ensure that they remain current and that new risks to privacy are addressed. Should a program or initiative undergo major revisions, an addendum to the original PIA or a new PIA should be submitted to our Office and TBS.

10. Do – Get in Touch with OPC

Whether you are new to PIAs, or a seasoned veteran of the process, you may encounter new or complex issues during the development of the PIA. Our PIA Team is happy to consult with institutions during the PIA process so that potential privacy issues can be discussed. If you would like to consult with us, please send an email to *PIA-EFVP@priv.gc.ca*.