Caitlin Lemiski, Director of Policy
Guilda Rostama, Senior Policy Analyst

Office of the Information and Privacy Commissioner for BC

Privacy Impact Assessments

Essential information for public bodies and organizations

27th Annual Victoria International Privacy & Security Summit, Victoria, BC

March 12, 2025

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

AGENDA

1. What is a PIA and why do one
2. Getting buy in: the benefits of PIAs
3. The single best way to start a PIA
4. Five common PIA mistakes - and how not to make them
5. Demystifying common or integrated program agreements
6. Demystifying security requirements
7. Getting the right signatures at the right time
8. Deciding whether to publish PIAs online as a transparency measure
9. Deciding whether to submit a PIA to the OIPC for review
10. Conclusion: 5 key takeaways from the session

WHAT IS A PIA?

- A PIA is a compliance tool.
- Public bodies **have to** do one because it is the law.
- Organizations **should do** one because it's a great way to demonstrate compliance.
- PIA template for FIPPA is downloadable from the Ministry's website (alon with the regulations). PIA template for PIPA is downloadable from the OIPC's website.
- The OIPC reviews PIAs but we do not approve them. Submit to info@oipc.bc.ca.

GETTING BUY-IN

- You can show your own value with a good PIA
- You can network with new people within your workplace
- You can learn a lot of new and useful things
- You can save your organization a lot of money
- Knowing how to do a PIA is a marketable skill in BC, in Canada, and beyond

THE BEST WAY TO START A PIA

- Pretend you are a journalist chasing a story.
- Forget the template for now. Just start learning as much as you can about the project.
- Why are we doing this? What problem is it going to solve? What other options did they consider?
- What is all the data that is going to be involved? (includes metadata)
- Do a lot of open-source research with information that is already publicly available. You can often learn a lot.

5 COMMON MISTAKES

- *Not* doing an informational interview
- *Not* taking into account the security part and guessing
- *Not* understanding it so well that you could easily explain it to a friend over dinner
- *Not* understanding the basic legal notions and guessing
- *Not* updating the PIAs when needed (Privacy Officer should have a regular review schedule)

COMMON/INTEGRATED PROGRAM AGREEMENTS

- A CIPA is a type of contract and a legal authority under FIPPA or PIPA
- A CIPA agreement can be under five pages. Tip: Don't make more complicated than it needs to be
- A public body has full control over whether it wants to enter into a CIPA or not
- CIPAs are very powerful. That's why OIPC must by law review them
- Private companies can become part of a CIPA too
- The OIPC has a guide on CIPAs on its website.

SECURITY REQUIREMENTS

- You do NOT need to be a security professional to complete a PIA.
- You do NEED to find out who the security person is. There is always someone (even if it is the vendor). They are your ally.
- Connect directly with the security person and **talk** to them. Bring a curious, open and positive perspective.
- Use the PIA to highlight security strengths *and* vulnerabilities.
- Understand what a STRA is and what a SOAR is.

THE RIGHT SIGNATURES

- Make sure a high level executive signs the PIA.
- Make sure the privacy officer signs the PIA.
- Make sure the person who wrote the PIA signs the PIA.
- Make sure the program area lead signs the PIA.
- Do not have the privacy officer sign off until the security person has signed off.

PUBLISHING A PIA OR NOT?

- Often not a good idea to publish the full PIA for security reasons, but sometimes it is possible.
- Not every PIA should be published, but some of them can be
- Be transparent about which version you are publishing and why, and what you have left out (and why)
- Consider publishing a directory of PIAs (and STRAs/SOARs) for transparency and accountability

SHARING WITH OIPC

- Only a CIPA PIA must by law be sent to the OIPC for review
- Suggest submitting a PIA: If the project is high risk, high dollar value, likely to be subject to public scrutiny, or uses new technologies
- If you are new to your role and want us to review your work and support you
- We will not write a PIA for you, but we will identify areas that we think need more work and provide comments

5 KEY TAKEAWAYS

- A PIA is a great way to show compliance and improve your own career
- Take on each PIA with an investigative reporter's mindset
- The PIA should honestly represent the benefits and risks of the project
- Security colleagues are your allies
- The OIPC is the regulator, but we are also here to help

Thank you.

Questions?

(250) 387-5629

info@oipc.bc.ca

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA