SELECT STANDING COMMITTEE ON FINANCE AND GOVERNMENT SERVICES

JANUARY 2023

Supplementary budget submission

Fiscal Years 2023/24-2025/26

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

O.R.L. office of the registrar of lobbyists BRITISH COLUMBIA

TABLE OF CONTENTS

OVERVIEW

I am pleased to submit this supplementary budget submission for the Office of the Information and Privacy Commissioner (OIPC) for the fiscal years 2023/24 to 2025/26.

The Information and Privacy Commissioner requests supplemental funding to support the amendments made to the *Freedom of Information and Protection of Privacy Act* (FIPPA) in Bill 22, the *Freedom of Information and Protection of Privacy Amendment Act,* 2021 and the subsequent resources required to support this implementation with my office. This will result in a total operating budget for fiscal years 2023/24 to 2025/26 of $10,162,000, $9,891,000 and $9,622,000 respectively. The resulting capital budget requested for the same three years is $277,000, $52,000, and $82,000 respectively.

I appreciate the opportunity to present this supplementary request to the Select Standing Committee on Finance and Government Services (SSCFGS) as an important part of the OIPC's accountability to the Legislative Assembly and the people of British Columbia.

MANDATE OF THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

The OIPC is the independent oversight agency responsible for monitoring and enforcing compliance with two statutes, the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

Under FIPPA, the OIPC enforces compliance with access to information and protection of privacy legislation by more than 2,900 public bodies in British Columbia, including ministries, Crown corporations, health authorities, municipalities, self-governing professions, universities, and school districts.

In discharging its mandate, the OIPC investigates and mediates access appeals and privacy complaints; conducts formal hearings; issues binding orders; comments on the access and privacy implications of proposed legislation, programs, policies and technologies; and educates the public about their access and privacy rights and public bodies about their legal obligations.

The work of the OIPC is to ensure that decisions and actions taken by public bodies remain open and accountable and that public bodies properly control and manage the personal information of citizens they collect in order to deliver public services.

PIPA sets the rules private sector organizations (including businesses, labour organizations, political parties, interest groups, and non-profits) must follow in the collection, use, and disclosure of customer, client, and employee personal information. Similar to our duties under FIPPA, it is the OIPC's responsibility to enforce compliance of PIPA by the estimated one million private sector organizations operating in British Columbia.

Under PIPA, the OIPC investigates complaints, adjudicates disputes, and educates and informs the public about their consumer and employee privacy rights and organizations about their privacy responsibilities.

The legislative changes to FIPPA are making it mandatory for public bodies under our jurisdiction to have a documented privacy management program as well as making it mandatory to report privacy breaches to my office. The impacts of these changes form the substantive content of this submission and the content that follows.

SUPPLEMENTARY BUDGET REQUEST – UPDATES SINCE THE OCTOBER 2022 OIPC BUDGET SUBMISSION

Since my last appearance at the SSCFGS, the BC government has confirmed the coming into force of significant privacy amendments to FIPPA by adding mandatory breach notification and a requirement for public bodies to develop Privacy Management Programs (PMPs). These

amendments will enhance the accountability of public bodies in managing the personal information of people in BC. They will also require the OIPC to undertake additional responsibilities to ensure their implementation.

Ensure the Implementation of FIPPA Amendments: Mandatory Breach Notification and a Requirement to Develop Privacy Management Programs

The fundamental purpose of FIPPA is to make public bodies accountable to the public and to protect personal privacy. In 2015, the OIPC recommended reforms for accountability in protecting personal privacy including a requirement for mandatory breach notification and PMP requirements for public bodies to the Legislature's Special Committee to Review the Freedom of Information and Protection of Privacy Act.[1]

I was pleased the BC Legislature passed *Bill 22, the Freedom of Information and Protection of Privacy Amendment Act* on November 25, 2021. These amendments require public bodies to notify individuals and my office of privacy breaches that might be reasonably expected to cause significant harm to those individuals. They also require BC's public bodies to develop PMPs.

The government has now set February 1, 2023, as the coming into force date of these two major changes.

On November 28, 2022, Order-in-Council 638 (OIC 638) set out the requirements for mandatory breach notification. The Minister responsible for FIPPA also published directions relating to PMPs on December 7, 2022.[2]

These amendments are significant and will improve the accountability of public bodies that are managing the personal information of people in British Columbia. They will enhance public trust in government and all public bodies that handle personal information.

They will also result in an increase in demand for OIPC services beginning February 1, 2023.

New Mandatory Breach Notification Requirements for Public Bodies

Starting February 1, 2023, public bodies are required to notify individuals of a privacy breach if the breach could reasonably be expected to result in significant harm to them.[3]

---

[1] See Nov 18, 2015 Submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*: https://www.oipc.bc.ca/legislative-submissions/1884.

[2] https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/pmp_ministerial_direction_2023.pdf

[3] The amendments state that "significant harm" includes:
(i) bodily harm,
(ii) humiliation,
(iii) damage to reputation or relationships,
(iv) loss of employment, business or professional opportunities,

The notification must be made "without unreasonable delay" and must include:

- the name of the public body;
- the date that the breach came to the attention of the public body;
- a description of the breach, including when the breach occurred and the nature of the personal information involved;
- confirmation that the Commissioner has been or will be notified of the breach;
- contact information for a person that can answer questions about the breach on behalf of the public body;
- a description of steps taken or planned to reduce the risk of harm to the individual; and
- a description of steps, if any, that the individual could take to reduce the risks of harm.

The Regulation requires public bodies to provide notice to individuals directly and in writing, and permits indirect notification in certain circumstances such as when the public body does not have accurate contact information for the affected individual(s). Indirect notification must also be made in writing and must contain the same information that is required in direct notifications.

In addition to notifying individuals, the amendment requires public bodies to notify the Commissioner of any breach that could reasonably be expected to result in significant harm to the individual.

The amendments do not require public bodies to notify individuals if doing so could reasonably be expected to result in immediate and grave harm to their safety or physical or mental health, or could reasonably be expected to threaten another individual's safety or mental health.[4] However, public bodies must still notify the OIPC of these breaches and the Commissioner may notify affected individuals.

There are an estimated 2,900 public bodies in British Columbia. Every year a small percentage of those bodies voluntarily report privacy breaches to our office. Over the past five years, the OIPC has received, on average, approximately 100 voluntary breach notification files per year from 50 different public bodies. While these public bodies voluntarily turn to the OIPC as a resource to help ensure that they respond to a breach in a manner that is adequate and reasonable, there is little doubt that others do not. They may fear reputational harm, legal liability and costs that may flow from notifying my office or affected individuals. However, it

(v) financial loss,
(vi) negative impact on a credit record, or
(vii) damage to, or loss of, property.

[4] s. 36.3(3) of FIPPA.

means every year BC citizens are not informed by public bodies when their personal information is inappropriately disclosed or accessed by bad actors. Hence the new mandatory breach reporting requirements.

The OIPC's preliminary estimate is that these new requirements will result in a 300% increase in breach notifications from public bodies. This preliminary estimate is based on a review of impacts experienced by other jurisdictions who have introduced mandatory breach notification. The review discloses that when mandatory breach notification is introduced, the impact can vary from a low of 50% to a high of 700%.

For example, when the UK and Australia introduced mandatory breach notification in both the public and private sectors, the Privacy Commissioners in these respective offices saw a 700 and 318 percent increase in notifications, respectively.[5] Manitoba introduced mandatory provisions for the public and health sectors on January 4, 2022 and saw an immediate 50 percent increase in notification to the Ombudsman office, with those numbers continuing to trend upward. [6]

When Alberta brought mandatory breach notification to the health sector (both public and private) under its *Health Information Act* (HIA), the Commissioner's office reported a 407 percent increase in breach reports that year, which went up 600 percent for two years before lowering to a 315 percent increase difference after three years.[7]

Federally, mandatory breach notification, though not required by law, is mandated by a Treasury Board policy covering approximately 260 government institutions listed in Schedule 3 of the *Privacy Act*. There has been an approximately 100% increase in notifications to the Commissioner's office between the year before the policy was introduced and the 2021/22 fiscal year.[8]

---

[5] See the Office of the Australian Information Commissioner's Insights Report (https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report) on the operation of the breach notification scheme over the first 12 months in May 2019, and the ICO UK's 2018-19 Annual Report (https://ico.org.uk/media/about-the-ico/documents/4017979/annual-report-201819.pdf), which states that the: "GDPR and DPA 2018 strengthened the requirement for organisations to report [privacy data breaches]. As a result, we received 13,840 PDB reports during 2018-19, an increase from 3,311 in 2017-18."

[6] The breach notification numbers in Manitoba will be reported in the Ombudsperson 2022-23 Annual Report when published.

[7] Mandatory breach reporting came into effect in Alberta under the HIA on August 31, 2018, which was the last 7 months of the fiscal year for 2018-2019. The year prior, notifications to OIPC AB were 133 (2017-2018), jumping to 674 in 2018-2019, 938 in 2019-20, 930 in 2020-21 and 551 in 2021-22. See the Annual Reports & Business Plans – Office of the Information and Privacy Commissioner of Alberta: https://oipc.ab.ca/about-us/annual-reports-business-plans/.

[8] In the 2013/14 FY before the reporting requirement were in effect, the Office of the Privacy Commissioner (OPC) received 242 breach reports. In 2021/22, the OPC received 463 breach reports. The numbers have varied over the years and the OPC highlighted its reasons to believe that there are significant gaps in reporting in its 2017-18 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/#heading-0-0-4-4Stats.

The above comparators, though not identical to our changes, are nonetheless informative. As the new rules in BC apply to all public sector bodies, including in health care, the OIPC expects the increase in breach reporting to the OIPC to fall between the range of numbers that happened in these other jurisdictions. The OIPC has determined that preparing for a 300% increase in breach notifications is reasonable.

Once the OIPC is notified of a breach, the breach is triaged and immediately assigned to either a case review officer or an investigator. The case review officer or investigator will contact the public body to ensure it has complied with the amendments under FIPPA. The staff member assigned also monitors four key areas in the public body's management of the breach:

> **Containing the Breach:** Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking or changing computer access codes, or correcting weaknesses in physical security.
>
> **Evaluating the Risks:** Identify what personal information is involved and how sensitive it is. Determine how long the personal information was exposed, how the breach occurred, and the likelihood of the breach reoccurring. Ascertain how many people are affected by the breach and harms that could result (e.g. identity theft, humiliation/hurt).
>
> **Notifying Affected Individuals:** Complete notification to affected individuals and to the OIPC in accordance with FIPPA if there is a real risk of significant harm resulting from the breach the statutory exceptions to notification do not apply.
>
> **Prevention:** Complete a thorough investigation to identify outstanding risks that could contribute to another privacy breach and then mitigate those risks appropriately. This process could include developing or improving long-term safeguards.

Mandatory breach notification is critical to personal information protection. It ensures that individuals affected by breaches will know about them so they can take steps to protect themselves. In addition, prevention measures reduce the risk of future breaches.

Other privacy regulators that have experienced the implementation of mandatory breach notification have advised us to also prepare for an increase in complaints to the OIPC about whether public bodies have performed their mandatory breach notification responsibilities under FIPPA. This is likely to result from individuals being notified that their personal information was subject to a breach who have a complaint that their personal information was breached, and in other cases individuals may complain that they have not been notified but believe their personal information has been breached. Those individuals may decide to complain to our office. The OIPC will be required to respond to these new types of complaints spurred by the new amendments. In addition, the OIPC will conduct investigations or audits of alleged non-compliance with the new mandatory breach notification provisions in FIPPA when appropriate.

New Privacy Management Program Requirements for Public Bodies

In addition to bringing into effect mandatory breach reporting requirements, OIC 638 also brings into force a requirement under s. 25 of Bill 22 for the head of a public body to develop a privacy management program in accordance with the Directions of the Minister. Direction 02/2022[9] requires the heads of public bodies to:

- designate an individual(s) responsible for
    - being a point-of-contact for privacy-related questions;
    - supporting the development, implementation, and maintenance of privacy policies and procedures; and
    - supporting the public bodies' compliance with FIPPA.
- establish a process to complete and document privacy impact assessments and information-sharing agreements;
- establish a process for responding to privacy complaints and breaches;
- ensure employees are aware of their privacy obligations through privacy awareness and education;
- make privacy policies and documented processes and practices available to employees;
- implement methods to ensure that service providers are informed of their privacy obligations; and
- routinely monitor the PMP and update it as required.

Public bodies are directed to make the above components reasonable and scaled commensurate with the volume and sensitivity of the personal information managed by the public body.

The OIPC is available and will be called upon to consult with a public body about its PMP at the request of a public body.[10] Over the past five years, there has been no legislated requirement for public bodies to have PMPs, and the OIPC has received very few consultation requests from public bodies about them. We expect to hear from Crown corporations, school districts, post-secondary institutions, and health authorities from across the province whether in Greater Vancouver, Victoria, Kelowna, Vernon, Prince George or Cranbrook. The OIPC preliminary estimate is that there will be at least 50 requests for consultations per year from the approximately 2,900 public bodies in BC as a result of the requirement for public bodies to develop PMPs as of February 1, 2023.

[9] https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/pmp_ministerial_direction_2023.pdf
[10] All consults with the OIPC happen consistent with the Office's Policy on consultations with the OIPC: https://www.oipc.bc.ca/guidance-documents/1432.

Public bodies seeking to consult with the OIPC about their PMP can call or email the OIPC. Once a public body has contacted us, an OIPC Policy Analyst is assigned and responds to the public body to answer their questions, review all of the public body's provided privacy management program documentation, and have discussions and provide resources to the public body about its strategy to implement an effective privacy management program. The OIPC may also proactively contact public bodies to request information about their PMP for the purposes of evaluating whether it meets the requirements of Direction 02/22 and the guidance published by the OIPC.

In addition, the OIPC is preparing to process a new type of complaint: that a public body has not performed its PMP responsibilities under FIPPA.

Ensuring Implementation of FIPPA Amendments for Privacy Breach Notification and Privacy Management Programs

To best serve public bodies and the public, the OIPC is planning an integrated approach to ensuring implementation of the FIPPA amendments relating to mandatory breach notification and PMPs.

Our plan will permit breach notifications and PMP consultations to be processed efficiently while education and enforcement work is carried out. This is consistent with the broad mandate of the Information and Privacy Commissioner that includes monitoring the administration of FIPPA to ensure that its purposes are achieved, informing the public about FIPPA, conducting investigations and audits to ensure compliance with FIPPA, and investigating and attempting to resolve complaints.[11] For example, proactive investigations would assess whether a public body has the foundational components of privacy management in place and can help to address areas of non-compliance pre-emptively before a breach occurs.

To implement the Bill 22 amendments the OIPC will:

- process the estimated increased number of breach notifications;
- process any increase in complaints and other investigations and audits about public bodies that may not be fulfilling their breach notification or PMP responsibilities;
- process the estimated increase in requests for consultation about PMPs, including privacy breach management policies;
- respond to the increase in requests for information about privacy breach notification and PMP requirements;
- respond to requests by public bodies for education and presentations about these requirements; and

[11] Section 42 of FIPPA.

- prepare for the above increases in demands for service by:
    - revising the OIPC privacy breach notification processes and privacy management program consultations for public bodies to align with the new requirements under FIPPA,
    - establishing monitoring systems for processing voluntary notification files and mandatory notification files,
    - developing an early resolution process for breaches reported to the OIPC that do not meet the real risk of significant harm threshold or that otherwise merit an early resolution,
    - reviewing and updating the OIPC website and guidance documents in line with the amendments, and
    - updating the OIPC case tracker system for metrics for public reporting of statistics related to breaches and PMPs.

To ensure the implementation of privacy breach notification requirements and privacy management program requirements under Bill 22, the OIPC requires a conservative estimate of 7.5 FTEs:

- 2 FTEs for Case Review Officers that will support intake, early resolution of breach notification, and basic requests for information;
- 3 FTEs for Investigators that will support processing the increase in mandatory breach notifications and any increase in investigations or audits related to public bodies not performing their breach notification or PMP responsibilities;
- 2 FTEs that will support consultations on PMPs, including privacy breach response policies, and complex requests for information. This is necessary to support organizations to comply with the legislation and offer guidance in how to do so; and
- 0.5 FTE for the communications team to support education work through the OIPC website, presentations, and publication of investigation and audit reports.

The OIPC will receive significant increases in requests for information, breach notifications and requests for consultation on PMPs from public bodies. The approach outlined above is a strategic one that anticipates an increased need for the OIPC to educate and consult with public bodies about privacy breaches and PMPs.

The secure management and processing of personal information is necessary for public bodies to gain the trust and confidence of the people of British Columbia. We will closely monitor the impacts of these amendments on the OIPC to determine future resources, and will report back to the committee as appropriate.

SUPPLEMENTARY BUDGET REQUEST FOR FISCAL YEAR 2023/24 TO 2025/26

This supplementary budget request is for the fiscal year 2023/24 and should be read together with my office's October 2022 budget submission to the SSCFGS for fiscal years 2023/24 – 2025/26.[12] For the consolidated budget proposal, please refer to Table 1: 2023/24 Supplementary Funding Request & Impact on Fiscal 2024/25-2025/26.

The OIPC has a staff complement of 51 positions, plus the Commissioner. Without additional resources, our ability to deal with mandated cost increases comes primarily from salaries (e.g., not hiring staff) or a reduction in outside professional advice, such as legal advice. I have examined our budget in 2022/23 and have determined that, while we can accommodate the costs of supporting the implementation of the amendments to FIPPA this fiscal year, that we cannot absorb it for fiscal years 2023/24 – 2025/26.

I ask the SSCFGS to consider the following supplementary budget request to support the OIPC in implementing Bill 22:

- an additional $890,000 for operating costs, for a total operating budget of $10,162,000 in 2023/24, and
- an additional $16,000 for capital costs, for a total capital budget of $277,000 in 2023/24 to support capital costs relating to additional staff.

This represents an increase of 9.6 percent for operating costs and 6.1 percent for capital costs. This will result in an operating budget for fiscal years 2024/25 to 2025/26 of $9,891,000 and $9,622,000 respectively, and a resulting capital budget for the same three years of $52,000, and $82,000 respectively.

Thank you for your attention.

January 13, 2023

ORIGINAL SIGNED BY

_____

Michael McEvoy
Information and Privacy Commissioner for British Columbia
Registrar of Lobbyists

[12] See OIPC, Budget Fiscal Years 2023/24 – 2025/26, October 2022: https://www.oipc.bc.ca/budget-service-plans/3713.

Table 1: 2023/24 Supplementary funding request & impact on fiscal 2024/25 – 2025/26

Statement of Operations (in $000s)

		2023/24 Budget (Approved)	2023/24 Supplementary Budget (Proposed)*	2023/24 Total Budget (Approved + Proposed)	2024/25 Budget (Approved)	2024/25 Budget (Change from Approved)*	2025/26 Budget (Approved)	2025/26 Budget (Change from Approved)*
Operations								
Revenue		5	-	**5**	5	-	**5**	-
	Total Operating Appropriation	**9,272**	**890**	**10,162**	**9,001**	**890**	**8,732**	**890**
Expenses								
	Salaries and Benefits							
	50 Base Salaries	4,557	618	**5,175**	**4,479**	618	**4,295**	618
	51 Supplementary Salary Costs							
	52 Employee benefits	1,252	159	**1,411**	**1,232**	159	**1,185**	159
	54 Legislative Salaries and Indemnities	324	-	**324**	**324**	-	**324**	-
	Total Salaries and Benefits	**6,133**	**777**	**6,910**	**6,035**	**777**	**5,804**	**777**
	Operating Costs							
	57 Public Servant Travel	52	-	**52**	**52**	-	**52**	-
	60 Professional Services	462	-	**462**	**412**	-	**412**	-
	63 Information Systems - Operating	542	23	**565**	**429**	23	**419**	23
	65 Office and Business Expenses	209	15	**224**	**209**	15	**201**	15
	67 Informational Advertising & Publications	-	-	**-**	**-**	-	**-**	-
	68 Statutory Advertising and Publications	18	-	**18**	**18**	-	**18**	-
	69 Utilities, Materials and Supplies	35	-	**35**	**35**	-	**35**	-
	70 Operating Equipment and Vehicles	-	-	**-**	**-**	-	**-**	-
	73 Amortization	165	-	**165**	**210**	-	**210**	-
	75 Building Occupancy Costs	780	-	**780**	**780**	-	**780**	-
	85 Other Expenses (CSS)	879	75	**954**	**824**	75	**804**	75
	Total Internal Recoveries	(1)	-	**(1)**	**(1)**	-	**(1)**	-
	Total External Recoveries	(2)	-	**(2)**	**(2)**	**-**	**(2)**	**-**
	Total Operating Costs	**3,139**	**113**	**3,252**	**2,966**	**113**	**2,928**	**113**
	Total Operating Budget	**9,272**	**890**	**10,162**	**9,001**	**890**	**8,732**	**890**

Capital							
Total Capital Appropriation	261	16	**277**	**47**	**5**	**77**	**5**
Spending Plan							
Furniture and Equipment	10	-	**10**	**10**	-	**10**	-
Information Systems	251	16	**267**	**37**	5	**67**	5
Tenant Improvements	-	-	**-**	**-**	-	**-**	-
Other	-	-	**-**	**-**	**-**	**-**	**-**
Total Capital Budget	**61**	**16**	**277**	**47**	**5**	**77**	**5**

Notes (Explanations of Variances)

* Funding for a total of 7.5 FTE's for implementation of Bill 22 - the *Freedom of Information and Protection of Privacy Amendment Act,* 2021