Engagement on PMP and Mandatory Breach Regulation - Local Government FOI coordinators

From: Holmes, Kjerstine L s.15
s.15

To: Lowe, Charmaine CITZ:EX <Charmaine.Lowe@gov.bc.ca>
Cc: Stock, Cathy CITZ:EX <Cathy.Stock@gov.bc.ca>, Harriman, Rheannon CITZ:EX <Rheannon.Harriman@gov.bc.ca>
Sent: May 13, 2022 3:54:26 PM PDT
Attachments: Agenda - FOIPPA PMP and Mandatory Breach discussion - Local gov_2022-05-16.docx, FOIPPA Breach and PMP presentation_2022-05-16.pptx

Hello Charmaine,

Attached for your information, please find the deck and agenda that will be shared on Monday, May 16th with the local government FOI Coordinators. That group will be the first in our series of engagement sessions with broader public sector organizations. Similar sessions are planned with privacy managers in the Health Authorities (May 19), Crown Corporations (May 18) and then with the K-12 school districts and post-secondary institutions.

Please do not hesitate to reach out if you have any questions or concerns. We will keep you posted on the outcome of these sessions.

Kjerstine Holmes (She/Her)
Project Director, Strategic Policy & Legislation Branch
Corporate Information and Records Management Office
Ministry of Citizens' Services
Desk 250 419 8888
Cell 236 638 1591

I would like to acknowledge the traditional and unceded Coast Salish territory of the lək̓ʷəŋən peoples where I am privileged to live and work as an uninvited guest. Specifically, the Songhees and Esquimalt Nations and the W̱SÁNEĆ peoples whose historical relations to the land continue today.

BRITISH COLUMBIA | Ministry of Citizens' Services

Agenda

FOIPPA Privacy Management Program and Mandatory Breach Engagement
Local Government sector

Date: May 16, 2022
Time: 2:00 – 3:00pm
Location: via Teams

Local Government sector:	**Jennifer Borland, Records Management and Privacy Coordinator, City of North Vancouver**
	Cobi Falconer, Director, Access to Information and Privacy, City of Vancouver
	Sophie Loehrich, Records and Privacy Manager, City of Surrey
	Kimberly Ho, Information and Privacy Officer, Metro Vancouver
	Kim Paterson, Records Coordinator and FOI Clerk, City of Vernon
	Louise Simkin, Administrative, Information & Privacy Coordinator, District of North Vancouver
	Robyn Biggar, Records and FOIPPA Administrator, City of Port Coquitlam
	Troy Vink, Records and Information Administrator, City of Burnaby
	Kate O'Connell, Director of Corporate Support Services, City of Courtenay
	Brooke Holtz, FOI and Privacy Coordinator, City of New Westminster
Citizen's Services:	**Janet Donald, ED, Privacy, Compliance & Training Branch**
	Keleigh Annau, Director, Strategic Privacy, Policy and Training, PCT
	Cathy Stock, ED, Strategic Policy & Legislation Branch
	Kjerstine Holmes, Project Director, Strategic Policy & Legislation Branch
	Rheannon Harriman, Director, Strategic Policy & Legislation Branch
	Carm Plater, Manager, Legislation and Policy, Strategic Policy & Legislation Branch

#	ITEM	LEAD
1	Welcome and introductions	Cathy Stock
2	Mandatory Breach Notification – framework overview and discussion	Kjerstine Holmes
3	Privacy Management Program – framework overview and discussion	Kjerstine Holmes
4	Next steps and closing	Cathy Stock

FOIPPA update: Regulations and directions

Mandatory Breach Notifications and Privacy Management Programs

May 16, 2022

BRITISH COLUMBIA | Ministry of Citizens' Services

Agenda

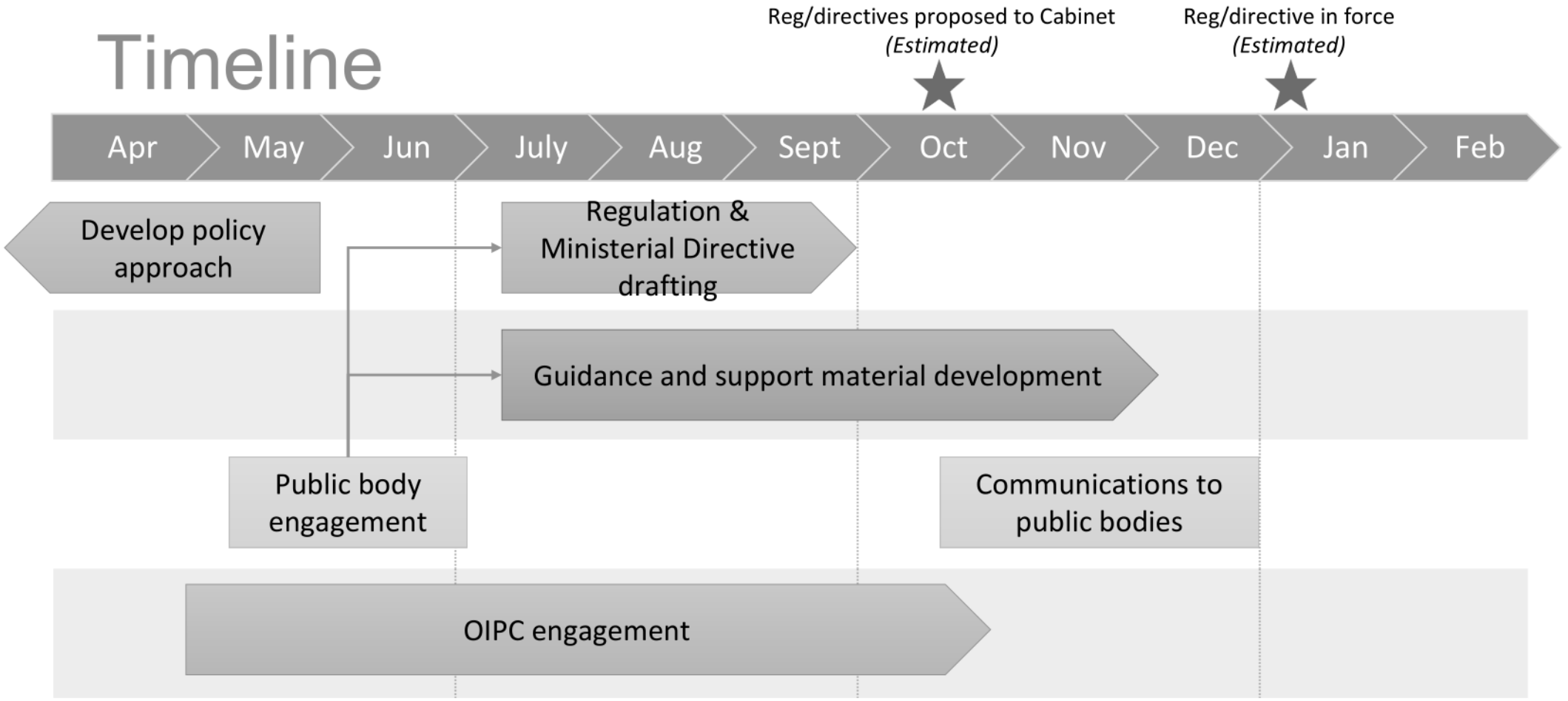
- Overview
- Mandatory Breach Notification
- Privacy Management Program components
- Next steps

Overview

FOIPPA 2021 Amendments

- FOIPP Amendment Act received royal assent Nov. 25
- Most changes came into force at that time
- Some were delayed to allow for development of regulations and support for implementation, including:
  - Mandatory breach notifications
  - Privacy management programs
  - Data-linking (future work)

Timeline


Reg/directives proposed to Cabinet
(Estimated)
Reg/directive in force
(Estimated)
Apr
May
Jun
July
Aug
Sept
Oct
Nov
Dec
Jan
Feb
Develop policy approach
Regulation & Ministerial Directive drafting
Guidance and support material development
Public body engagement
Communications to public bodies
OIPC engagement

Mandatory Breach Notification

Section 36.3 – Privacy Breach Notifications

Overview: If a privacy breach is reasonably expected to result in significant harm to an individual, section 36.3 requires public bodies to issue a notification about that breach to the affected individual and to the Information and Privacy Commissioner.

Section reference:

(1) In this section, "privacy breach" means the theft or loss, or the collection, use or disclosure that is not authorized by this Part, of personal information in the custody or under the control of a public body.

(2) Subject to subsection (5), if a privacy breach involving personal information in the custody or under the control of a public body occurs, the head of the public body must, without unreasonable delay,

(a) notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant

(i) bodily harm,

(ii) humiliation,

(iii) damage to reputation or relationships,

(iv) loss of employment, business or professional opportunities,

(v) financial loss,

(vi) negative impact on a credit record, or

(vii) damage to, or loss of, property, and

(b) notify the commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph (a).

(3) The head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to

(a) result in immediate and grave harm to the individual's safety or physical or mental health, or

(b) threaten another individual's safety or physical or mental health.

(4) If notified under subsection (2) (b), the commissioner may notify an affected individual.

(5) A notification under subsection (2) (a) or (b) must be made in the prescribed manner.

Manner of notice to the individual

Notification in writing indicating:

- name of the public body(s)
- contact information for someone who can respond to inquiries about the privacy breach and the Information and Privacy Commissioner
- description of the nature of the privacy breach
- date the privacy breach came to the attention of the public body
- description of any steps the public body has taken or will be taking to reduce the risk of harm

Include additional information if known:

- type of personal information that is the subject of the breach
- date of the privacy breach
- potential risk(s) to the affected individual;
- potential steps the individual could take to mitigate the risk of harm

Note: Indirect notifications are allowable (e.g., via media, websites, etc.) if direct notification would be unreasonable or impracticable.

Manner of notice to the Commissioner

- Notice to the Commissioner must be in writing
- Notice will include the same information as the individual notice plus:
  - An estimate of the number of individuals to whom there is a real risk of significant harm

Discussion

- Does this manner of notice seem feasible for your organization?
- What supports would your organization need to implement this approach?
- What are your thoughts on a requirement to identify potential risk(s) to the affected individual and steps to mitigate that risk of harm?

Privacy Management Programs

Section 36.2 – Privacy Management Programs

Overview: Section 36.2 requires each public body to develop a privacy management program.

Section Reference:

- The head of a public body must develop a privacy management program for the public body and must do so in accordance with the directions of the minister responsible for this Act.

Overview

- Draft framework outlines the key components of a privacy management program for public bodies.
- As the amount or sensitivity of personal information in the care of public bodies can vary substantially, the requirements will be scalable.
- Aims to be adaptable for all organization sizes and business types.
- Implementing the components will support public bodies in:
  - setting expectations for privacy accountability; and
  - complying with the privacy requirements of FOIPPA.

Key components

Accountability

Designated individual(s) responsible for:

- Being a contact person for privacy related matters.
- Supporting development of privacy policies and/ or procedures.
- Supporting the public body's compliance with FOIPPA.

Consistency

- Process to complete and document PIAs and ISAs.
- Process for responding to privacy complaints and breaches.
- Process for regularly monitoring and updating PMP to align with public body activities and compliance with FOIPPA.
- Ensuring privacy obligations regarding collection, use, disclosure and security of personal info are covered in contracts with service providers.

Transparency

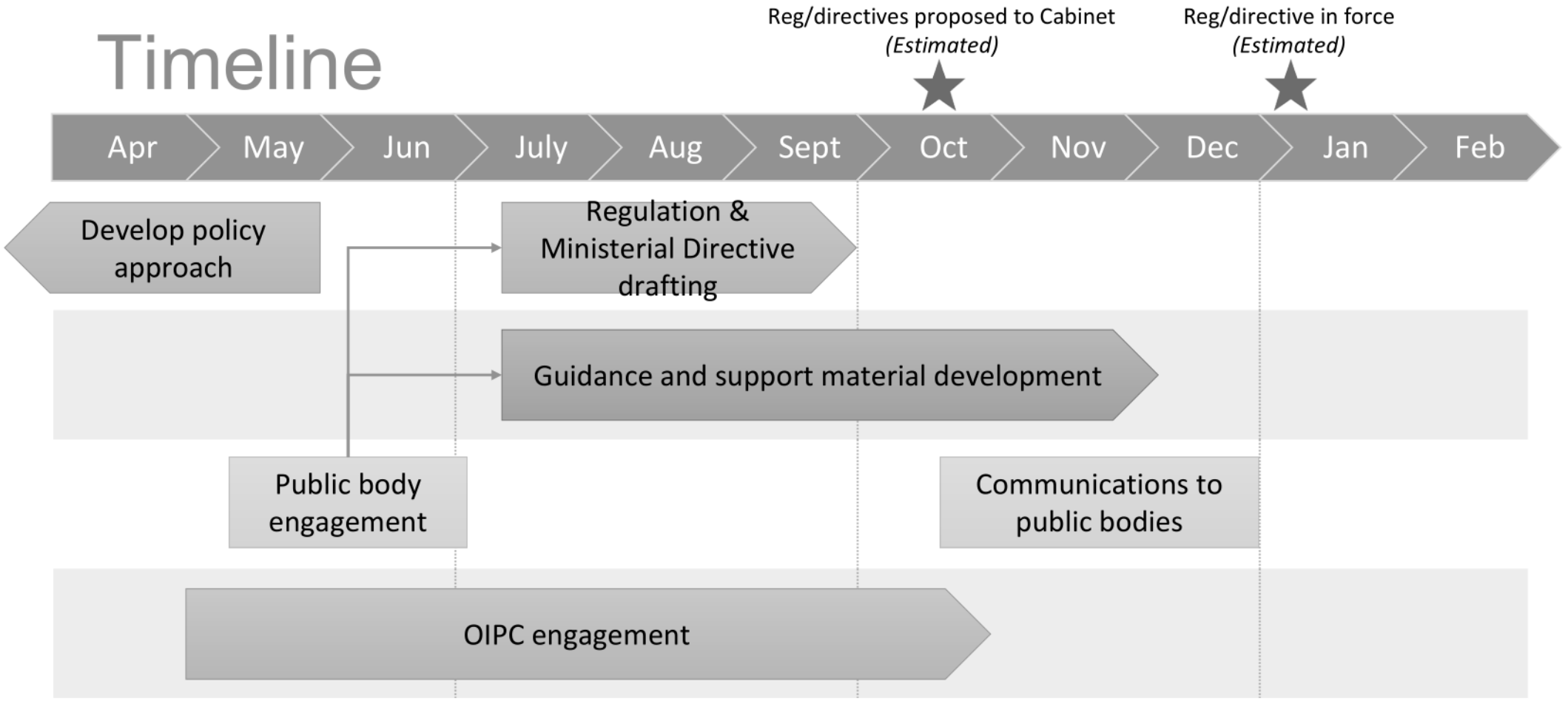
- Scalable, timely privacy awareness and education activities to ensure employees are aware of their privacy obligations.
- Ensure information specifying how privacy obligations are met can be accessed by employees and the public (e.g., make privacy policies available).

Discussion

- Do these directions seem feasible for your organization?
- What supports would your organization need for implementation?

Next steps

Timeline


Reg/directives proposed to Cabinet
(Estimated)
Reg/directive in force
(Estimated)
Apr
May
Jun
July
Aug
Sept
Oct
Nov
Dec
Jan
Feb
Develop policy approach
Regulation & Ministerial Directive drafting
Guidance and support material development
Public body engagement
Communications to public bodies
OIPC engagement

Questions?

Ministry of Citizens' Services

Corporation Information and Records Management Office

Strategic Policy and Legislation Branch

IM.ITPolicy@gov.bc.ca

FW: breach notifications and PMP - approval to move forward

From: Stock, Cathy s.15
To: charmaine.lowe@gov.bc.ca
Sent: July 26, 2022 1:55:46 PM PDT
Attachments: s.13

Hello
Please review the drafting instructions for breach notification – I would like to get it to leg council today or tomorrow if possible.

From: Stock, Cathy CITZ:EX
Sent: July 15, 2022 1:46 PM
To: Lowe, Charmaine CITZ:EX <Charmaine.Lowe@gov.bc.ca>
Cc: Carling, Emma CITZ:EX <Emma.Carling@gov.bc.ca>
Subject: breach notifications and PMP - approval to move forward

Hello Charmaine,

We are looking for your approval to send the drafting instructions for breach notification to Legislative Counsel.
Please see attached the DN, as well as the drafting instruction for breach notification and the PMP Directions.
CS

Cathy Stock
Executive Director
Strategic Policy and Legislation | Ministry of Citizens' Services
e: cathy.stock@gov.bc.ca | t: (250) 953-3703

Page 22 of 67 to/à Page 31 of 67

Withheld pursuant to/removed as

s.13

FW: Draft PMP Direction for Public Bodies

From: Stock, Cathy CITZ:EX <Cathy.Stock@gov.bc.ca>
To: Statz, Len CITZ:EX <Len.Statz@gov.bc.ca>, Donald, Janet CITZ:EX <Janet.Donald@gov.bc.ca>, Romanow, Holly CITZ:EX <Holly.Romanow@gov.bc.ca>
Cc: Holmes, Kjerstine L CITZ:EX <Kjerstine.Holmes@gov.bc.ca>
Sent: September 15, 2022 2:13:16 PM PDT
Attachments: s.13

Just a background – here is the email that went out to them requesting feedback.

From: Lowe, Charmaine CITZ:EX <Charmaine.Lowe@gov.bc.ca>
Sent: September 7, 2022 3:02 PM
To: McEvoy, Michael OIPC:EX <MMcEvoy@oipc.bc.ca>; Van Den Bulk, Jeannette OIPC:EX <JVanDenBulk@oipc.bc.ca>
Cc: Stock, Cathy CITZ:EX <Cathy.Stock@gov.bc.ca>; Holmes, Kjerstine L CITZ:EX <Kjerstine.Holmes@gov.bc.ca>
Subject: s.13

Dear Michael and Jeannette:

I hope this email finds both of you well and that you are both wonderfully rested after a lovely summer break. I, myself, am just back from s.22 which I enjoyed immensely.

I am writing today to share with you consultation drafts of the mandatory breach regulation and Privacy Management Program ministerial directions. These drafts were developed in consultation with your staff, as well as public bodies and Indigenous partners and organizations over the past several months.

As we would like to move these directions and regulation forward as soon as possible, we would appreciate receiving any final feedback or recommendations you or your office may have by Friday September 16, 2022. If this is not possible, please do let me know at your earliest convenience so that we might adjust our timelines accordingly. Thank you in advance for supporting this important work.

Sincerely,

Charmaine Lowe
ADM, Corporate Information and Records Management Office
Ministry of Citizens' Services

Page 33 of 67 to/à Page 38 of 67

Withheld pursuant to/removed as

s.13

RE: Draft PMP Direction and MBN Reg

From: Stock, Cathy CITZ:EX <Cathy.Stock@gov.bc.ca>
To: Holmes, Kjerstine L CITZ:EX <Kjerstine.Holmes@gov.bc.ca>
Sent: September 15, 2022 4:44:05 PM PDT

From: Stock, Cathy CITZ:EX
Sent: September 15, 2022 2:09 PM
To: charmaine.lowe@gov.bc.ca
Cc: Holmes, Kjerstine L CITZ:EX <Kjerstine.Holmes@gov.bc.ca>
Subject: RE: s.13

Hi Charmaine,

OIPC staff came back with a few questions to your request for feedback from the Commissioner. Our responses are below in blue. Ideally we would like to respond by EOD to ensure they meet the September 16 deadline. Please let me know if you have any concerns.

s.3

Page 40 of 67 to/à Page 42 of 67

Withheld pursuant to/removed as

s.3

s.3

From: Lowe, Charmaine CITZ:EX <Charmaine.Lowe@gov.bc.ca>
Sent: September 7, 2022 3:02:15 PM
To: Michael McEvoy; Jeannette Van Den Bulk
Cc: Stock, Cathy CITZ:EX; Holmes, Kjerstine L CITZ:EX
Subject: s.13

Dear Michael and Jeannette:

I hope this email finds both of you well and that you are both wonderfully rested after a lovely summer break. I, myself, am just back from s.22 which I enjoyed immensely.

I am writing today to share with you consultation drafts of the mandatory breach regulation and Privacy Management Program ministerial directions. These drafts were developed in consultation with your staff, as well as public bodies and Indigenous partners and organizations over the past several months.

As we would like to move these directions and regulation forward as soon as possible, we would appreciate receiving any final feedback or recommendations you or your office may have by Friday September 16, 2022. If this is not possible, please do let me know at your earliest convenience so that we might adjust our timelines accordingly. Thank you in advance for supporting this important work.

Sincerely,

Charmaine Lowe
ADM, Corporate Information and Records Management Office
Ministry of Citizens' Services

FW: OIC Mandatory Breach Notifications/PMP - Nov 23rd cabinet meeting

From: McKamey, Kristy CITZ:EX <Kristy.McKamey@gov.bc.ca>
To: Laidlaw, Susan CITZ:EX <Susan.Laidlaw@gov.bc.ca>
Sent: November 23, 2022 7:28:27 PM PST
Attachments: RE: CITZ OIC for November 23

Approved by cabinet, see attached.

From: Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>
Sent: November 23, 2022 4:34 PM
To: Brown, Taylor J CITZ:EX <Taylor.Brown@gov.bc.ca>; McKamey, Kristy CITZ:EX <Kristy.McKamey@gov.bc.ca>
Cc: Jarmson, Lindsay CITZ:EX <Lindsay.Jarmson@gov.bc.ca>; Garcia, Cherrie-Len CITZ:EX <CherrieLen.Garcia@gov.bc.ca>
Subject: RE: OIC Mandatory Breach Notifications/PMP - Nov 23rd cabinet meeting

Hi, Yes, it did go through today. I rec'd a note from the OIC coordinator. See attached.

Thanks.
JC

From: Brown, Taylor J CITZ:EX <Taylor.Brown@gov.bc.ca>
Sent: November 23, 2022 4:25 PM
To: McKamey, Kristy CITZ:EX <Kristy.McKamey@gov.bc.ca>; Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>
Cc: Jarmson, Lindsay CITZ:EX <Lindsay.Jarmson@gov.bc.ca>; Garcia, Cherrie-Len CITZ:EX <CherrieLen.Garcia@gov.bc.ca>
Subject: RE: OIC Mandatory Breach Notifications/PMP - Nov 23rd cabinet meeting

CJ said it was and went through without her or Colleen needing to participate.

From: McKamey, Kristy CITZ:EX <Kristy.McKamey@gov.bc.ca>
Sent: November 23, 2022 4:16 PM
To: Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>
Cc: Jarmson, Lindsay CITZ:EX <Lindsay.Jarmson@gov.bc.ca>; Brown, Taylor J CITZ:EX <Taylor.Brown@gov.bc.ca>; Garcia, Cherrie-Len CITZ:EX <CherrieLen.Garcia@gov.bc.ca>
Subject: OIC Mandatory Breach Notifications/PMP - Nov 23rd cabinet meeting

Hi Jeannette,

Just wondering if the OIC Mandatory Breach Notifications and PMP was brought forward to cabinet today?

Cabinet Dates:

- Nov 23: **OIC mandatory breach notifications and privacy management programs**

Thank you!
Kristy

RE: CITZ OIC for November 23

From: McKay, Kirsten PREM:EX <Kirsten.McKay@gov.bc.ca>
To: Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>
Sent: November 23, 2022 1:45:03 PM PST

Hi Jeannette,

This was approved at Cabinet today.

Thanks,

Kirsten McKay *(she/her)*
OIC Coordinator
Cabinet Operations | Office of the Premier
236 478-1216 | Kirsten.McKay@gov.bc.ca

From: McKay, Kirsten PREM:EX
Sent: November 18, 2022 6:02 PM
To: Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>
Subject: CITZ OIC for November 23

Hi Jeannette,

This is to confirm the following OIC will be considered at Cabinet on Wednesday:

Non-CABRO
R6253

As no specific timing requirements were indicated, this OIC will be processed in a timely manner, pending its approval at Cabinet.

Please let me know ASAP if your Minister has requested any staff support at Cabinet.

Best,

Kirsten McKay *(she/her)*
OIC Coordinator
Cabinet Operations | Office of the Premier
236 478-1216 | Kirsten.McKay@gov.bc.ca

FYI: PMP and OIC Now Posted

From: Harriman, Rheannon CITZ:EX <Rheannon.Harriman@gov.bc.ca>
To: Laidlaw, Susan CITZ:EX <Susan.Laidlaw@gov.bc.ca>, Rice, Colleen A CITZ:EX <Colleen.Rice@gov.bc.ca>
Cc: Buck, Caitlin CITZ:EX <Caitlin.Buck@gov.bc.ca>
Sent: December 2, 2022 12:30:50 PM PST

Hi Susan and Colleen – just wanted to let you know that the OIC and PMP Directions are now posted on the PCT resources page.

We connected with PCT (Holly/David) and have decided to hold the communications to broader public sector until we get the guidance material posted. In the meantime, I believe they will be sending a message to the MPOs early next week to let them know everything was approved and posted.

Let me know if you have any questions. Thank you!

Rheannon
250-208-7809

From: Romanow, Holly CITZ:EX <Holly.Romanow@gov.bc.ca>
Sent: December 2, 2022 12:00 PM
To: Buck, Caitlin CITZ:EX <Caitlin.Buck@gov.bc.ca>; Harriman, Rheannon CITZ:EX <Rheannon.Harriman@gov.bc.ca>; Holmes, Kjerstine L CITZ:EX <Kjerstine.Holmes@gov.bc.ca>
Subject: FYI: PMP and OIC Now Posted

Hi everyone,

The PMP Directions and OIC for MBR are up on the resources page: Privacy & Personal Information Resources - Province of British Columbia (gov.bc.ca)

Note:
- The Ministerial Orders & Directions section is organized in descending order.
- You'll also notice we removed the separate section for FOIPPA amendments since a year has passed and we use the term modernization instead of amendments.

Thanks to Rheannon for making this happen and being a lovely human about the whole thing.

Thanks,
Holly

Privacy Management Program Guidance for B.C. Public Bodies

Corporate Information and Records Management Office

BRITISH COLUMBIA

December 2022 | Version 1

TABLE OF CONTENTS

Introduction 3

Privacy Management Program Components 3

1. Designating a Privacy Contact Person 3
2. Privacy Impact Assessments and Information-Sharing Agreements 4
3. Privacy Complaints and Privacy Breaches 5
4. Privacy Awareness and Education Activities 6
5. Making Privacy Practices and Policies Available 7
6. Informing Service Providers of Privacy Obligations 7
7. Monitoring and Updating 8

Contact 8

INTRODUCTION

Section 36.2 of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires B.C. public bodies to develop a privacy management program (PMP).[1] A PMP is an evolving set of policies, procedures and tools developed by a public body to enable systematic privacy protection throughout the personal information lifecycle.

The Privacy Management Program Directions (PMP Directions), issued by the minister responsible for FOIPPA, describe the mandatory components for PMPs.

Use this guidance to understand the requirements for PMPs. This guidance is for non-ministry public bodies in B.C.

For ministries, the B.C. government follows the Privacy Management and Accountability Policy.

PRIVACY MANAGEMENT PROGRAM COMPONENTS

1. DESIGNATING A PRIVACY CONTACT PERSON

The PMP Directions require that the head of the public body appoint a privacy contact.

The head of the public body may decide to assign more than one privacy contact depending on several factors, including the size and structure of the organization. While many public bodies may opt for a single privacy contact, a public body with multiple locations and/or a large amount of personal information may choose to appoint more than one privacy contact.

POINT OF CONTACT FOR PRIVACY MATTERS

The privacy contact is the point of contact for privacy-related matters such as privacy questions or concerns. The public body may wish to list the individual's contact information on their website and in their communications materials. It may also be helpful to incorporate the contact information and a role description in onboarding materials for new employees.

SUPPORT DEVELOPMENT OF PRIVACY POLICIES AND/OR PROCEDURES

The privacy contact supports the development, implementation, and maintenance of the public body's privacy policies and/or procedures. An example that can be used by public bodies is the B.C. government's Privacy Management and Accountability Policy.

Whether or not a public body already has privacy policies and procedures in place, it could consider conducting a self-assessment to understand where policy gaps may exist or if existing policies and procedures need updating to ensure the public body meets the mandatory PMP components.

Public bodies may want to consider developing policies and procedures on the following topics:

---

[1] Note that FOIPPA and the corresponding regulation are in the process of being updated to reflect the new requirements.

- Collection notices;
- Consent;
- Accuracy and correction of personal information;
- Permitting individuals to access their own personal information;
- Records retention (and disposal) schedules;
- Reasonable security for the personal information in the public body's custody or under its control;[2] and
- Completing privacy impact assessments (PIAs).

Keep in mind that the PMP policies and procedures can be scaled in proportion to the volume and sensitivity of the personal information in the custody or under the control of the public body.

SUPPORT COMPLIANCE WITH FOIPPA

There are numerous resources available for support:

- The B.C. government's Guide to Good Privacy Practices contains useful information relevant to both government ministries and non-ministry public bodies.
- The Office of the Information and Privacy Commissioner's (OIPC) website has guidance documents for dealing with FOIPPA obligations. Topics range from common privacy concerns to privacy best practices to interpreting FOIPPA requirements.
- The B.C. government's Privacy and Access Helpline (email: privacy.helpline@gov.bc.ca or call 250-356-1851) is available for anyone who has questions related to privacy. This includes ministries, non-ministry public bodies, the private sector, and citizens. While the Privacy and Access Helpline staff cannot provide legal advice, they can provide guidance on privacy-related matters.

Executive support and commitment are also necessary factors in creating a culture of privacy within a public body, which helps support compliance with FOIPPA.

2. PRIVACY IMPACT ASSESSMENTS AND INFORMATION-SHARING AGREEMENTS

The PMP Directions require that a public body has a process in place for completing and documenting Privacy Impact Assessments (PIAs) and Information-Sharing Agreements (ISAs).

PRIVACY IMPACT ASSESSMENTS

A PIA is a step-by-step review process to make sure that a public body is meeting its privacy requirements under FOIPPA and helps a public body identify and mitigate any privacy risks involved in a particular initiative. Section 69 (5.3) of FOIPPA requires that public bodies complete PIAs, and the PMP Directions require a process for completing and documenting PIAs.

[2] For definitions of "custody" and "control," see Schedule 1 of FOIPPA or the FOIPPA Policy and Procedures Manual.

PIAs are typically completed with the help of privacy contacts and the individuals working on the initiative. As noted in the PIA Directions, the goal is to work together to identify, evaluate and manage privacy risks. The PIA Directions also provide guidance on the required elements of a PIA.

For example, the B.C. government has a 5-step PIA review process to complete and document PIAs. There is also a PIA template for non-ministry public bodies that can be used.

INFORMATION-SHARING AGREEMENTS

As defined under section 69 of FOIPPA, an information-sharing agreement (ISA) is an agreement that sets the conditions on the collection, use or disclosure of personal information by the parties to the agreement.

The PMP Directions require public bodies to have a process in place for completing and documenting ISAs as appropriate under FOIPPA. Even if a public body does not expect to initiate ISAs, the process will be helpful if another entity wishes to initiate an ISA with the public body.

The B.C. government has developed guidance for ISAs and a sample ISA template. Public bodies may have other pieces of legislation and/or regulations besides FOIPPA that authorize information sharing. It is recommended that public bodies confirm their legal requirements before adapting the government examples for their specific context.

3. PRIVACY COMPLAINTS AND PRIVACY BREACHES

A privacy breach is the theft or loss of personal information, or the access, collection, use or disclosure of personal information in the custody or control of a public body that is not authorized by FOIPPA. A privacy complaint is a complaint from an individual about a breach of their own personal information.

Note that a privacy breach is not limited to written or recorded information. Personal information that is breached verbally may need to be responded to in the same manner as other breaches.

The PMP Directions require public bodies to have a documented process in place to respond to any privacy breaches and complaints. As an example, the B.C. government has developed an Information Incident Management Policy (IIMP).

As outlined in section 36.3 of FOIPPA, if a privacy breach is reasonably expected to result in significant harm to an individual, public bodies are required to issue a notification about that breach to the affected individual and to the Information and Privacy Commissioner. Refer to the Guidance on Mandatory Privacy Breach Notifications for more information.

A documented breach response process may include the following aspects:

1. Mechanism for employees to immediately report actual or suspected breaches to a supervisor and privacy contact so that the alleged breach can be confirmed and dealt with.
2. Determining the level of harm and the need for breach notification in accordance with the *Freedom of Information and Protection of Privacy Regulation*. Refer to the Guidance on Mandatory Privacy Breach Notifications.

3. Notifying affected individuals and the Information and Privacy Commissioner as required under section 36.3 of FOIPPA.
4. Containment and recovery steps that the public body may take depending on the circumstances. Containment involves preventing further spread of the breached personal information. Recovery involves retrieving the records containing the breached personal information.
5. Mechanisms for investigating the nature, extent and/or cause of the breach.
6. Preventative measures to avoid breaches from occurring in the future. This may include improving security measures.
7. Documentation of breaches and keeping this documentation in accordance with the public body's records retention requirements.[3]
8. Responding to privacy complaints.[4]
9. Administrative fairness practices.[5] Examples of administrative fairness may include ensuring individuals under investigation are aware of the allegations against them and have a fair opportunity to respond to the allegations; and investigators and decisions-makers are free from conflict and are unbiased, and decisions are made based on evidence.

4. PRIVACY AWARENESS AND EDUCATION ACTIVITIES

Privacy training and awareness helps employees identify personal information, understand their privacy obligations, and are an important part of breach prevention.

Awareness and education activities can be scaled based on the volume and sensitivity of the personal information in the public body's custody or control and based on the role of the employee. For example, the privacy obligations of an employee who infrequently handles low sensitivity personal information are different from the employee who often handles sensitive personal information. Therefore, the training and awareness required for those two employees is not necessarily the same.

Education activities should be timely. For example, training should be implemented when there are significant changes to how the public body collects personal information, when systems or processes change, as part of new employee onboarding processes, and periodically to refresh employees' knowledge.

The following privacy topics for education activities are relevant for most public bodies:

- An understanding of what constitutes personal information.
- Appropriate collection, use and disclosure of personal information.
- Reasonable security measures and access controls to protect personal information.

---

[3] Section 31 of FOIPPA requires public bodies retain personal information for at least one year if it is used to make a decision that directly affects an individual.
[4] Privacy complaints may result when an individual has concerns about how a public body handled or processed their personal information.
[5] Fairness in Practice Guide, the Office of the Ombudsperson. In B.C., fairness and good public administration is overseen by the BC Ombudsperson for the broader public sector.

- Identification and reporting of privacy breaches and privacy complaints.

Training on the following topics may also be included:

- Privacy impact assessments.
- Privacy and security requirements for storage of sensitive personal information outside of Canada.

The B.C. government has developed FOIPPA Foundations: Privacy and Access Fundamentals. This course can be used by public bodies when educating their employees and service providers. This free, interactive, online course provides information on privacy and access fundamentals in B.C.

Employees may also benefit from understanding why privacy is important and the underlying principles for privacy protection. The 10 Privacy Principles and Guide to Good Privacy Practices can help with this understanding.

5. MAKING PRIVACY PRACTICES AND POLICIES AVAILABLE

As outlined in the PMP Directions, public bodies are required to make their privacy policies and any documented privacy processes or practices available to employees and, where practicable, to the public.

For employees, this could include adding privacy information to onboarding materials and creating a privacy section on public body internal websites.

Public bodies can decide on the best approach for making these materials available to the public. For example, if the public body has a website, they may wish to publish their privacy policy and related privacy processes or practices online. Smaller public bodies may wish to have their privacy polices on hand in case someone from the public asks to see them. The key is to determine what is practicable for the public body or what the public body is capable of doing to make those policies, processes, or practices available.

In addition, public bodies should consider publishing any privacy awareness and education activities as well as summaries of PIAs and ISAs where appropriate. For example, the B.C. government publishes a summary of PIAs and ISAs through the Personal Information Directory, which documents the management of personal information holdings of government and assists the public in identifying the location of personal information about them held by government.

6. INFORMING SERVICE PROVIDERS OF PRIVACY OBLIGATIONS

When service providers handle personal information related to the provision of services for a public body, the public body must inform them of their privacy obligations.

Contracts are one way to demonstrate privacy obligations for service providers. The B.C. government's privacy protection schedule is an example that can be modified by other public bodies to suit their needs.

PIAs are another useful tool to demonstrate how public bodies and service providers can meet their privacy obligations. By completing a PIA, a public body can assess the services, confirm compliance for

such things as collection, use and disclosure of personal information under FOIPPA, and identify privacy risks.

Privacy training, policies and processes will also support a service provider in complying with their privacy obligations when providing services for a public body.

7. MONITORING AND UPDATING

It is important to review the PMP regularly and ensure it is still relevant to the public body's activities and personal information holdings. For example, this could include an annual review or a review when there is a large change in the public body's operations.

Suggested guiding questions for the review include:

- What are the latest privacy or security threats and risks that the public body needs to be aware of?
- Are the public body's policies and procedures reflecting the latest guidance or complaint and audit findings of the OIPC?
- Are new services being offered that involve increased collection, use or disclosure of personal information? Has the PMP been updated to reflect these new services?
- Is training occurring? Is training effective?
- Are privacy policies and procedures being followed?
- Are contracts with service providers up to date and being followed?

Examples of PMP assessment tools include:

- Privacy Maturity Assessment (Saskatchewan)
- Privacy Program Evaluation (Yukon Ombudsman)
- Privacy Management Program – Gap Analysis for Larger Public Bodies and Municipalities (Nova Scotia)
- Privacy Management Program – Gap Analysis for Smaller Public Bodies & Municipalities (Nova Scotia)
- Accountable Privacy Management in BC's Public Sector (BC OIPC)

These tools and guiding questions can be used to ensure the public body's PMP remains appropriate to their activities and is compliant with FOIPPA.

CONTACT

For questions or comments regarding these guidelines, please contact:

Privacy, Compliance and Training Branch
Corporate Information and Records Management Office
Ministry of Citizens' Services
Telephone: (250) 356-1851
Email: privacy.helpline@gov.bc.ca

ID: 26901, Title: OIPC Mtg Material: Breach Reg

Full Name:
Approval Route:
Assigned To: Stock, Cathy CITZ:EX Rush: No Meeting Materials - Meeting Note/Materials Signature: Assistant Deputy Minister
Branch: CIO-CIRMO-ADMO Other Number: N/A
Link: N/A
Due Date: 9/6/2022 Date Completed: N/A Date Initiated: 8/29/2022 N/A

Item History

9/7/2022 02:50 PM
Sullivan, Michelle A [Assignee] forwarded an eApprovals item to Stock, Cathy CITZ:EX for action
Hi Cathy, approved with changes to cover email as per Charmaine.

9/7/2022 02:45 PM
Lowe, Charmaine [Assignee] approved the item and forwarded it to Sullivan, Michelle A for action
Approved with changes to cover email

9/7/2022 02:16 PM
Stock, Cathy CITZ:EX [Assignee] approved the item and forwarded it to Lowe, Charmaine for action
Changes made and email coming shortly

9/7/2022 02:15 PM
Stock, Cathy CITZ:EX added a document: ADM email - Commissioner McEvoy_MB PMP consultation v2.docx

9/7/2022 02:14 PM
Stock, Cathy CITZ:EX deleted a document: ADM email - Commissioner McEvoy_MB PMP consultation.docx

9/7/2022 01:45 PM
Lowe, Charmaine [Assignee] forwarded an eApprovals item to Stock, Cathy CITZ:EX for action
Please make the changes to the cover email as discussed

9/1/2022 03:54 PM
Carling, Emma [Assignee] forwarded an eApprovals item to Lowe, Charmaine for action
Will be reviewed at Sept 7 briefing - then for your approval. Please see Cathy's comments for more info. Thanks

9/1/2022 03:18 PM
Stock, Cathy CITZ:EX [Assignee] approved the item and forwarded it to Carling, Emma for action
We are ready to share the consultation drafts of the mandatory breach reg and PMP ministerial directions with the Commissioner. We are suggested an email from you to the Commissioner (attached in the e-app).

We have prepared a summary of the rationale for you in case the Commissioner has questions or requests a meeting (draft only as we are still waiting for PCT comments). We are briefing you on Wed Sept 7, but I thought you might like an opportunity to review in advance.
We have a tentative OIC date for Oct 26 so our goal is to have the e-apps ready for your review and final MO approval by Sept 16.

9/1/2022 03:15 PM
Stock, Cathy CITZ:EX added a document: MB reg and PMP line by line rationale v2 DRAFT.docx

9/1/2022 12:14 PM
Holmes, Kjerstine L [Assignee] approved the item and forwarded it to Stock, Cathy CITZ:EX for action
Email to Commissioner with consultation drafts for approval

9/1/2022 12:12 PM
Holmes, Kjerstine L added a document: ADM email - Commissioner McEvoy_MB PMP consultation.docx

8/31/2022 11:35 AM
Holmes, Kjerstine L deleted a document: Appendix 1 MB Jursidictional Scan.docx
Not needed for meeting with Commissioner

8/30/2022 02:09 PM

Holmes, Kjerstine L added a document: Appendix 1 MB Jursidictional Scan.docx

8/30/2022 02:09 PM
Holmes, Kjerstine L deleted a document: Appendix 1 Jursidictional Scan.docx
Replaced with updated version/file name

8/30/2022 02:07 PM
Holmes, Kjerstine L added a document: Appendix 1 Jursidictional Scan.docx

8/30/2022 02:03 PM
Holmes, Kjerstine L added a document: 2022-08-30 FOIPPA Consultation Draft.pdf

8/29/2022 04:15 PM
Holmes, Kjerstine L added a document: Draft PMP Directions for Public Bodies 5.0 Final.docx

8/29/2022 04:13 PM
Stock, Cathy CITZ:EX [Assignee] forwarded an eApprovals item to Holmes, Kjerstine L for action

8/29/2022 02:24 PM
Stock, Cathy CITZ:EX [Assignee] has shared an eApprovals item with Holmes, Kjerstine L.

8/29/2022 01:25 PM
Carling, Emma has created a new eApprovals item and assigned it to Stock, Cathy CITZ:EX

8/29/2022 01:25 PM
Carling, Emma created this item

Page 57 of 67 to/à Page 62 of 67

Withheld pursuant to/removed as

s.3

Page 63 of 67 to/à Page 66 of 67

Withheld pursuant to/removed as

s.13

Withheld pursuant to/removed as

s.3