

# Investigation Report

Investigation into the unauthorized disclosure of an Office of the Comptroller General  
Investigation Report

Date of Report: March 10, 2017

## Corporate Information and Records Management Office

Privacy, Compliance and Training Branch Investigations Unit

**Prepared by:**

Ken McLean  
Senior Director, Investigations and Audits  
Corporate Information and Records  
Management Office

Ainslie Avery  
Manager, Investigations and Audits  
Corporate Information and Records  
Management Office

**Incident Details:**

Investigation No: 2016-0282	Date Incident Occurred: Unknown	Date Incident Reported: February 25, 2016
DIPC Incident Identifier: F16-65049, F16-65510, F16-65511, F16-65362	Date Fieldwork Concluded: February 27, 2017	

An investigation report prepared by the Office of the Comptroller General (OCG) was disclosed to the Vancouver Sun without authorization and in contravention of information and privacy protection requirements. The investigation report contained findings and evidence in relation to an OCG investigation into the Ministry of Health's Pharmaceutical Services Division (PSD). This report describes the investigation into this unauthorized disclosure.

## Introduction

On February 25, 2016, a reporter from the Vancouver Sun contacted an employee of the Government Communications and Public Engagement (GCPE) branch to say that he had obtained an unredacted copy of an investigative report by OCG. The OCG's investigative report (the Report) was completed in June 2015 (project number 026115) and related to work conducted by the OCG Investigations and Forensics Unit into allegations of procurement and contract irregularities in the Ministry of Health's PSD.

As the Report contained confidential personal information and other confidential government information, its unauthorized disclosure constituted an information incident and, accordingly, it was reported to the Privacy Compliance and Training Branch (PCT) of the Corporate Information and Records Management Office (CIRMO), Ministry of Finance.

The PCT responded immediately by coordinating activities required under the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and the Government's information management policies. The PCT's initial response included efforts to contain and minimize any further distribution of the Report, and to assess the risk of harm to individuals impacted by the unauthorized disclosure of the Report.

The PCT also initiated a thorough investigation into the cause of the unauthorized disclosure. The scope of the investigation included identifying government employees or other individuals who may have had access to the Report, and determining whether the relevant ministries complied with the requirements of FOIPPA and government information management policies.

This investigative report sets out the results of the PCT's investigation and includes forward looking recommendations intended to help prevent similar incidents from occurring in the future.

## The Report

The Report contained personal information about PSD employees and others who participated in events examined by the OCG in relation to its investigation. PCT's view was that the

unauthorized disclosure of the Report to the Sun could create a potential risk of harm to individuals in the form of hurt, humiliation or damage to reputation.

## **Information Incident**

The Privacy Compliance and Training Branch (PCT) is responsible for investigating information incidents within government, including privacy breaches. An information incident is an event that threatens privacy or information security within government. Information incidents include the collection, use, disclosure, access, disposal or storage of information, whether accidental or deliberate, that is contrary to government policy.

Information incidents include privacy breaches, which are a collection, use, disclosure, access, disposal or storage of personal information that are not authorized by FOIPPA.

The unauthorized disclosure of the Report constituted a significant information incident for government and warranted a thorough investigation into the possible sources of the breach of government information management policies and of FOIPPA.

## **Scope of Investigation**

An executive committee was established, which included representatives of the Ministry of Finance and the BC PSA to oversee PCT's investigation and monitor its progress (members are listed in Appendix A below). PCT's investigation was also monitored by both the BC PSA and the law firm Gall Legge Grant & Munroe LLP, which was retained as external counsel to monitor and provide advice to ensure PCT's investigation was conducted fairly and in accordance with best practices in the conduct of administrative investigations.

The scope of this investigation, set out in Terms of Reference dated March 3, 2016 (see Appendix A), includes the following:

### **Information Incident response:**

1. The coordination of efforts to contain the incident with the Vancouver Sun, which included the issuance of a formal demand for the Vancouver Sun to destroy the personal information in their possession pursuant to s.73.1 of FOIPPA and/or additional actions as may be appropriate;

2. Consideration of further unauthorized distribution beyond the Vancouver Sun;
3. An assessment of the risk of harm to individuals impacted by this incident, and documentation of the actions taken to notify impacted individuals where appropriate; and
4. Additional actions in support, or on behalf, of the public body as may be appropriate in the circumstances.

**Investigation:**

1. Efforts to identify whether any government employee(s) may have disclosed the Report to the Vancouver Sun;
2. Whether the incident involved a collection, use, disclosure, access, disposal or storage of personal information that was not authorized by FOIPPA and/or applicable government policy;
3. Examining which government employees or other individuals may have had access to the Report, including from OCG, The Ministry of Health, IAO, and/or any other government department that may have received an unredacted copy of the Report;
4. Examining whether the involved ministries and other bodies complied with the requirements of FOIPPA and applicable government policy in the storage and handling of the Report, the Draft Report and any redline copies.
5. The issuance of forward-looking recommendations intended to prevent similar incidents from occurring in future.

The scope of this investigation expressly does not include the following:

1. Whether any government employees may have violated the Standards of Conduct for BC Public Service Employees. The Public Service Agency (PSA) was apprised of the investigation and is provided with a copy of the report into the unauthorized disclosure. Any potential employment issues that result are up to the PSA to address.
2. Investigation of the possibility of any employees of agencies other than ministries having released the Report to the Vancouver Sun.

The investigation was conducted in two phases in accordance with the Terms of Reference:

Phase 1: The objective is to establish how broadly the Report was accessible within government, and to determine whether there was credible evidence to support conducting

investigative interviews which would occur in Phase 2. A decision to proceed to Phase 2 was made in conjunction with the executive committee.

Phase 2 involved conducting follow-up interviews to establish the identity of individuals who may have disclosed the Report. The outcomes of Phase 2 interviews were used to determine whether there was sufficient evidence to suggest that a specific individual was the source of the unauthorized disclosure. Phase 2 also involved identifying any information management and practice issues to be addressed in prevention recommendations.

### **Summary of Findings:**

- The investigation did not result in determining the source of the unauthorized disclosure to the Vancouver Sun.
- The investigation found that, in the view of the investigators, a defined number of individuals collected and/or disclosed the Report in a manner not authorized under FOIPPA.
- Access to the Report within government was broad and included actual or potential access to the Report by 114 individuals. However, there was no indication that this access resulted in the unauthorized disclosure of the Report to the Vancouver Sun.
- The investigation identified six recommendations to enhance government information controls.

## **The Investigation**

### **Authorities**

FOIPPA defines the requirements for how public bodies collect, use, store and disclose personal information. There must be appropriate authorities to collect, use and disclose personal information that is in the custody and control of the public body.

FOIPPA provisions, which establish requirements for the handling of personal information include, but are not limited to the following:

- s.26 Collection of personal information
- s.27 Indirect collection of personal information

- s.30 Protection of personal information
- s.30.4 Unauthorized disclosure prohibited
- s.32 Use of personal information
- s.33.1 Disclosure inside or outside Canada
- s.33.2 Disclosure inside Canada only

The *BC Government Core Policy and Procedures Manual* s.12.3.1 establishes the requirements of the *Appropriate Use of Government Information and Information Technology Resources* (Appropriate Use Policy), which stipulates:

11. Employees must store electronic Records that relate to government business in Protected Government Systems.

- a) In extenuating circumstances, an electronic government Record may be temporarily stored outside of a Protected Government System, as long as the following conditions are met:
  - i. The electronic Record is stored on the system or Device only as long as it is necessary to deal with the extenuating circumstances;
  - ii. At the first available opportunity, the Record is transferred to a Protected Government System; and
  - iii. Duplicate copies of any electronic Record containing Confidential Information are deleted from the other system or Device as soon as possible.

The Appropriate Use Policy defines a Protected Government System as “a computer system in a data centre that has met the approved security requirements for the storage of Confidential Information (for example, an Employee’s network drives).”

## Privacy Breach Incident Response

### **Office of the Information and Privacy Commissioner:**

On February 25, 2016, PCT reported the privacy breach to the Office of the Information and Privacy Commissioner (OIPC), in accordance with established protocols and provided periodic updates throughout the course of the investigation.

### **Individuals Affected:**

The *Information Incident Management Process*<sup>1</sup> requires an assessment of harms that may result from an unauthorized disclosure of personal information. Potential harm is assessed according to a number of factors including risks to an individual's financial security, physical safety, and the potential for hurt, humiliation, embarrassment, damage to reputation or employment opportunities.

The PCT conducted a harms assessment by reviewing the Report to identify all breaches of personal information. Investigators determined that in total 94 individuals were affected by the breach to varying degrees. The investigators quickly established four categories of risk ranging from high risk to negligible risk based primarily on concerns for hurt, humiliation, or damage to reputation, and/or damage to business or employment prospects for these individuals. The following four categories of risk were established to facilitate assessment of which individuals should be notified of the privacy breach:

- Individuals facing a high degree of risk, and for whom notification was recommended immediately;
- Individuals facing a moderate degree of risk, and for whom notification was recommended immediately;
- Individuals facing a low degree of risk, and for whom notification was recommended out of an abundance of caution; and
- Individuals facing negligible risk, and for whom notification was not recommended.

Each of the 94 individuals was assessed and assigned to one of the four categories. In total, PCT recommended that 24 individuals be notified. As part of the effort to notify impacted parties, PCT requested and received formal approval from the OIPC under s.42(1)(i) of FOIPPA to indirectly collect contact information for 6 of the 24 impacted individuals for whom PCT was not able to obtain valid contact information from within the Ministry of Health or the Ministry of Finance. As a result, PCT was able to collect contact information and notify an additional 5 individuals, but was not able to complete notification to one person as investigators were unable

---

<sup>1</sup> URL: <http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents>

to locate current contact information for this individual. Notification of the privacy breach went to 23 individuals between March 3 and March 15, 2016.

Notification letters included an individualized summary of information contained in the Report as it related to the specific individual.

On March 30, 2016, PCT issued a follow-up notice to all 23 individuals who had received an initial notification. In this notice, investigators described actions taken to contain and remediate the exposure, and to prevent similar incidents from occurring in the future.

PCT received a number of responses from individuals who had been notified, and PCT addressed specific questions as they arose.

### **Containment of any further disclosure of the Report**

On March 1, 2016, the PCT took steps to contain further unauthorized release of the Report by issuing a demand to the Vancouver Sun under s. 73.1 of FOIPPA. The Vancouver Sun acknowledged receipt of the demand notice on March 4, 2016, and on March 16, 2016 the Vancouver Sun responded stating their position that they were authorized to possess the Report and that s.73.1 of FOIPPA was of no force or effect due to the application of section 2(b) of the *Canadian Charter of Rights and Freedoms*, which protects freedom of the press. The Vancouver Sun proceeded to publish three stories referencing the Report, including the Report's findings that individuals had engaged in conflict of interest. Two stories were published on March 12 and one was published on March 17, 2016. The Vancouver Sun did not publish the Report in its entirety.

Although the Ministry took steps to assert the government's objections to the Vancouver Sun's actions, it was ultimately decided that there was little practical purpose to pursuing court proceedings under the circumstances. As of the date when this report was released, no additional stories were published by the Vancouver Sun which reference the contents of the Report.



## Investigation

### Phase 1

Phase 1 of the investigation began on February 25, 2016 and was concluded on February 20, 2017. The objective of phase 1 was to examine the distribution of the Report within government, and to identify potential sources of the unauthorized disclosure for further follow-up in Phase 2.

Phase 1 included information gathering and assessments of available evidence, and targeted interviews focused on developing:

- A comprehensive inventory of all organizations and individuals with access to the Report;
- A determination of the appropriateness of each individual's access to the Report with respect to their employment responsibilities;
- An assessment of each individual's handling of the Report within government information systems; and
- A review of the potential motives for an individual to have released the Report and the interrelationships between those with known or suspected access to the Report.

The first step was to identify who may have had access to the Report. This process included canvassing all programs within government in which the Report was thought to have been broadly accessible. These programs included Ministry of Health, Legal Services Branch (LSB), Information Access Operations (IAO) and OCG.

Investigators then began collecting evidence using a standardized methodology which included capturing message tracking logs (MTLs), also known as email logs, Managed Print Service (MPS) logs, and audit logs for IAO's AXIS database. MPS logs showed all print-related functions (printing, photocopying, and scanning) associated with an individual's government credentials. MTLs showed header information (e.g. date/time, message size, sender, recipient, subject heading, and metadata) for all emails transiting through an individual's government email account. MTLs do not show the contents of emails, nor do they capture emails transiting through an individual's personal email account unless that email also transited through a government email account. MTLs were selected as providing the appropriate level of detail

without constituting an invasive review of email traffic, which could include personal email messages.

Where warranted, PCT also collected additional evidence such as calendar information, mailboxes, and lists of employees who had access to locations where the Report was known to be stored.

PCT determined that a total of 114 individuals had access to the Report, or had access to a location where the Report was stored. Of those, 53 individuals were found to have confirmed access; these included employees from IAO, the Ministry of Health, LSB, GCPE, and the Office of the Deputy Minister to the Premier.

The Report had been the subject of two Freedom of Information (FOI) requests received in June and July 2015. The PCT investigation therefore included a review of anyone associated with processing the FOI requests including IAO which manages the processing of information access requests on behalf of all government ministries. In the course of processing the FOI requests, the IAO provided the Report to the Ministry of Health, LSB, and GCPE.

The OCG, IAO, and LSB each subsequently canvassed their staff and provided lists identifying staff who had access to the Report, including at what point access occurred, and for what purpose. This information formed the basis for further inquiry and investigation by the PCT investigators.

In addition to the internal review, PCT notified external recipients of the Report—the RCMP, the Office of the Auditor General, and the Office of the Ombudsperson—of the unauthorized disclosure, and suggested that those agencies may wish to conduct their own review of the handling of the Report to establish whether a member of their agency could have disclosed the Report. Each agency responded to PCT to advise that they had conducted their own investigation and determined that their agency had not been the source of the unauthorized disclosure.

## Phase 2

Phase 2 of the investigation was initiated on August 25, 2016 and investigative fieldwork was concluded on February 27, 2017.

The objective of Phase 2 was to identify potential sources of the unauthorized disclosure to the Vancouver Sun. PCT investigators considered all Phase 1 evidence to determine whether sufficient behavioural indicators and/or questions regarding access to the Report were present to warrant a Phase 2 interview. PCT selected individuals to interview based on two factors:

1. The individual had access to the Report and had a discernible or perceived motive for releasing the Report.

Discernible or perceived motives contemplated by the investigators included:

- An individual involved in either the Ministry of Health investigation or the OCG investigation may have disclosed the Report to demonstrate that substantive issues were investigated:
- A member of government executive, including elected or appointed officials, may have disclosed the Report for political reasons or to demonstrate that government's actions were justified:

Investigators also considered that any employee who had access to the Report may have disclosed the Report because they felt it was in the public interest for the Report's findings to be publicized.

2. The individual handled or interacted with the Report in a manner that raised questions as to whether access was required as part of their duties (e.g. having printed the Report outside the timeframe when they interacted with the Report as part of their duties).

In total, the investigators interviewed 20 individuals in Phase 2. The purpose of the interviews was to ensure that the investigators understood how the Report had been processed, to resolve any questions arising from Phase 1, and to assess possible sources of the unauthorized disclosure to the Vancouver Sun.

Over the course of this comprehensive investigation, investigators identified and fully explored a number of possible sources of the disclosure to the Vancouver Sun. Any leads were followed up utilizing the rigorous methodology identified in this report, including a thorough investigation into all available electronic records.

#### Personal Information

## CONCLUSION

Ultimately, the investigation did not result in determining the source of the unauthorized disclosure to the Vancouver Sun.

PCT investigators have no doubt that the disclosure of the Report to the Vancouver Sun was done intentionally. While the investigation identified circumstances of concern as noted above, none of these circumstances were substantiated to have resulted in the unauthorized disclosure of the Report to the Vancouver Sun.

PCT noted that the Report had been accessible to 114 government employees. This level of access was largely explained by the Report having been part of a number of different administrative processes. Given the sensitivity of the Report, additional controls may have minimized the risk of unauthorized disclosure. However, there is no evidence that this accessibility resulted in the breach.

## PREVENTION MEASURES AND RECOMMENDATIONS

A goal of each information incident investigation is to identify measures that will help prevent similar incidents from occurring again in the future. Under the *Information Incident Management Process*<sup>2</sup> PCT is authorized to issue advisory and/or mandatory recommendations. These recommendations reflect a focus on continuous improvement and do not imply wrongdoing on the part of the entities or their employees.

PCT acknowledges that, during the course of this investigation, no evidence was found to suggest that any particular program area bore responsibility for the unauthorized disclosure of the Report to the Vancouver Sun, and PCT observed no evidence that the disclosure to the Vancouver Sun resulted from any systemic issues. PCT recognizes that government has established policies and training that define expectations and processes for the appropriate management of government information for both ministries and staff. These resources include

---

<sup>2</sup> Information Incident Management Process (September, 2011), URL: [http://www.cio.gov.bc.ca/local/cio/information\\_incident/information\\_incident\\_management\\_process.pdf](http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf)

the BC Government Core Policy and Procedures Manual, Appropriate Use of Government Information and Information Technology Resources (Appropriate Use Policy), and IM 111 government's mandatory privacy and information sharing training curriculum.

PCT also acknowledges that government has recently undertaken a number of initiatives which should reduce the risk of privacy breaches and other information incidents from occurring. Government has launched a new mandatory training module (IM117), which is intended to provide additional training and awareness for government employees related to information management, has engaged in recent policy development related to information security (e.g. Mobile Devices), and is expecting to launch, in 2017, a new comprehensive information management compliance and audit program which will evaluate and promote strong information management and protection practices across government. These initiatives are recognized by PCT as valuable mechanisms that will enhance organizational and individual compliance with information security standards.

Within this context, PCT recognises that the recommendations articulated below cannot guarantee a government employee will never intentionally disclose confidential or personal information. Such actions remain possible despite the presence of strong legislative and policy based protections, informational controls, and employee training.

The recommendations outlined below are intended to address observations made by PCT that drive towards continuous improvement in government information management and protection practices and are intended to strengthen government's handling and management of personal and confidential information. While the recommendations are directed to specific government ministries and agencies, PCT encourages a broader corporate implementation where appropriate.

In addition to the foundational controls noted above, PCT notes that a number of preventative measures were undertaken proactively during the course of the investigation by involved ministries and agencies. These measures are as follows:

1. The OCG undertook a review of the information management and protection practices of the OCG's Investigations and Forensics Unit. The review was conducted by Deloitte

between August and November, 2016, in collaboration with CIRMO. OCG has accepted and intends to fully implement the recommendations issued by Deloitte and CIRMO.

2. PCT presented IAO with a series of information protection risks identified during Deloitte's review of OCG's information management practices, as the nature of the inherent risks similarly applied to the work of IAO. IAO considered these risks and provided a response which noted existing strong practices and additional actions that they have committed to implement to further strengthen practices.
3. PCT, IAO and the Ministry of Finance's Information Management Branch jointly developed a process for the production of AXIS log data. These reports will now be available for the production of AXIS log data. These tools will provide an enhanced capacity to monitor and report on individual employee's access to specific FOI records.

Looking forward, PCT issues the following advisory recommendations:

1. That CIRMO and the Office of the Chief Information Officer work with the appropriate authorities to implement an updated information security classification framework to be used to designate certain sensitivity categories as needing to follow a more restricted FOI process.
2. That IAO examine its document storage processes and consider whether access to information can be better segmented, in accordance with the Appropriate Use Policy. The objective of such an examination would be to reduce the number of staff that have access to confidential government and personal information and ensure that information is accessible only to those who have a "need to know". For example, IAO may wish to explore whether restrictions can be applied within the AXIS database.
3. That LSB examine its document storage processes and consider whether access to information can be better segmented, in accordance with the Appropriate Use Policy. The objective of such an examination would be to reduce the number of staff that have access to confidential government and personal information and ensure that information is accessible only to those who have a "need to know".

In issuing this recommendation, PCT notes that only LSB staff involved in the handling of three specific legal files as well as database administrators and a certain LSB staff from the Office of the Assistant Deputy Attorney General had access to the Report.

Further, LSB did not store the Report on common or group LAN drives, the Litigation Document Management System, or the LSB SharePoint database and the majority of LSB staff did not have access to the Report.

PCT consulted with LSB regarding this recommendation, and LSB indicated that, although existing access controls are fairly robust, they are in the process of obtaining a new system for managing legal materials. This new system may address the segmentation of access to confidential information. LSB also indicated that, as legal counsel for government, all materials received by LSB are confidential and are subject to solicitor-client privilege, which requires that these materials are handled in a manner that is consistent with Law Society standards. LSB acknowledged the importance of handling confidential materials, particularly in relation to LSB's professional obligations.

In addition PCT also issues the following mandatory recommendations:

1. That IAO provide advice to ministries to help improve their internal processes relating to processing FOI requests. The advice should focus on containing extremely sensitive personal information and/or highly confidential government business information (e.g. within the FOI harms assessment process), in accordance with the Appropriate Use Policy.

In issuing this recommendation, PCT acknowledges that Deputy Ministers are responsible for ensuring that such records are shared only on a "need to know" basis.

2. That the OCG takes action to implement recommendations arising from the Deloitte review of the OCG Investigations and Forensics Unit's information management and protection practices.
3. That IAO engage with the software provider for AXIS and resolve logging issues which may impact the ability of the AXIS system to log all means by which a user may access a specific FOI request file.

Ultimately, appropriate management of government information is the responsibilities of the ministries and members of the public service charged with its stewardship. Distribution of the Report within government was significant and opportunities to reduce future disseminations of confidential government information, including personal information, should be pursued.



## APPENDIX A: TERMS OF REFERENCE

### Terms of Reference

PCTB Privacy Investigation 2016-0282

Date: March 3, 2016

#### Introduction

This incident involves the discovery on February 25, 2016 that an investigative report prepared by the Office of the Comptroller General (“OCG”) regarding alleged contracting irregularities and conflict of interest in the Ministry of Health Pharmaceutical Division (“the Report”) was released to Mr. Rob Shaw of the Vancouver Sun.

The Report is associated with OCG project number 026115 and is understood to have been finalized in approximately June 2015. There were two earlier draft versions of the report, which were produced in approximately April 2015 (“the Draft Reports”).

The Report and Draft Reports were the subject of two Freedom of Information (“FOI”) requests, tracked as FIN-2015-51929 and FIN-2015-51660. As Information Access Operations (“IAO”) manages the processing of access requests on behalf of government the requested records and any related records were sent to IAO which generated “redline” versions of the Report and Draft Reports. These versions show prospective redactions, but allow the content to remain readable to the viewer. Redacted versions of the Report and Draft Reports, with personal information removed, were released to the applicants.

#### Authority to investigate

Section 30 of the *Freedom of Information and Protection of Privacy Act* (“FOIPPA”) requires public bodies to protect personal information in their custody or under their control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information.

OIPC orders have stated that when a public body fails to satisfy its obligations under s.30 it must undertake a number of actions to remedy the breach. The Privacy, Compliance and Training Branch (“PCTB”) of the Corporate Information and Records Management Office in the Ministry of Finance has been mandated, on behalf of core government, to coordinate, investigate and resolve any actual or suspected Information Incident, which includes privacy breaches.

Government policies which document PCTB responsibilities respecting Information Incidents include:

- The BC Government Core Policy and Procedures Manual (s.12.3.6(b));
- The Information Incident Management Process (“IIMP”);
- The Process for Responding to Privacy Breaches; and
- The Investigation Protocol (December 2015).

NOTE: The PCTB was formerly part of the Office of the Chief Information Officer, which the above listed policies refer to.

## Scope

### I. Incident response

The scope of the PCTB's investigation includes the coordination of activities the public body is required to take under FOIPPA and the IIMP to resolve the privacy breach.

In this instance, the following are in scope:

5. Consideration of further unauthorized distribution beyond the Vancouver Sun;
6. The coordination of efforts to contain the incident with the Vancouver Sun, which included the issuance of a formal demand for the Vancouver Sun to destroy the personal information in their possession pursuant to s.73.1 of FOIPPA and/or additional actions as may be appropriate;
7. An assessment of the risk of harm to individuals impacted by this incident, and documentation of the actions taken to contain this incident and notify impacted individuals where appropriate; and
8. Additional actions in support, or on behalf, of the public body as may be appropriate in the circumstances.

### II. Investigation

PCTB is also responsible for investigating to determine whether any privacy breaches have been committed and what the root cause of the breach was. In this instance, this will include efforts to identify whether any government employee(s) may have released the records in question to the Vancouver Sun.

The basis of PCTB's determination: PCTB will evaluate whether this incident involved a collection, use, disclosure, access, disposal or storage of personal information that was not authorized by FOIPPA and/or applicable government policy.

The following are in-scope of the PCTB's investigation:

1. Examining which government employees or other individuals may have had access to the Report, the Draft Report, or any redline copies – including from:
  - a. Office of the Comptroller General;
  - b. Ministry of Health;
  - c. Information Access Operations (Ministry of Finance); and
  - d. Any other government department that may have received an unredacted copy of the Report.
2. Examining whether the involved ministries and other bodies complied with the requirements of FOIPPA and applicable government policy in the storage and handling of the Report, the Draft Report and any redline copies.
3. The issuance of forward-looking recommendations intended to prevent similar incidents from occurring in future.

The investigation will be led by Ken Mclean, Director of Investigations & Audits, PCTB, Corporate Information and Records Management Office, Ministry of Finance.

## Out of Scope

The following are out of scope of the PCTB's investigation:

1. Whether any government employees may have violated the *Standards of Conduct* for BC Public Service Employees.

PCTB has engaged the BC Public Service Agency ("PSA") and external legal counsel and is keeping them apprised of the investigation on an ongoing basis. Should evidence be uncovered in the course of this investigation to suggest that a government employee may have engaged in misconduct, PCTB will confer with PSA and external counsel, and will also engage the employee's Employer.

2. Investigation of whether any employees of non-government agencies including the Ombudsperson's office, the Office of the Auditor General ("OAG"), the RCMP and/or any other external organization may have released an unredacted copy of the Report to the Vancouver Sun directly or indirectly.

PCTB will contact external organizations that received an unredacted copy of the report to notify them of the document's release. PCTB will indicate they may wish to initiate their own internal examination, and will request they provide information about the outcome of any review they may undertake.

## Approach

PCTB will conduct this investigation in two phases, as follows:

### Phase 1:

The objective is to establish how broadly the Report was accessible within government, and whether credible evidence exists to support conducting investigative interviews with potential witnesses and respondents (which would occur as part of phase 2).

At the conclusion of Phase 1, a recommendation will be prepared regarding whether to move forward with Phase 2 investigative interviews. A decision to conduct Phase 2 or not will be made in conjunction between:

- Athana Mentzelopoulos, Deputy Minister, Finance;
- Cheryl Wenezeki-Yolland, Associate Deputy Minister and Chief Records Officer, Finance;
- Lori Halls, Deputy Minister, BC Public Service Agency;
- David Curtis, Assistant Deputy Minister, Finance;
- External counsel as appropriate; and,
- The head of any ministry/agency that employs potential an individual identified as a potential respondent.

## Phase 2:

The objective is to conduct investigative interviews with witnesses and respondents, premised upon specific evidence identified in Phase 1, to establish the identity of individual(s) who may have disclosed the Report. PCTB would also conduct interviews as part of phase 2 intended to address practice issues that may arise in the course of this investigation and to inform PCTB about prospective recommendations.

During the course of its investigation, the PCTB will:

1. Gather:
  - Information about which government employees and other individuals may have had access to the Report, the Draft Report, or any redline copies;
  - Electronic evidence that may identify the source of the disclosure to the Vancouver Sun – including email and other logs that record information about the electronic activities of government employees; and
  - Additional records which may be deemed relevant to the investigation by the PCTB.
2. Consider, following the collection and analysis of the above information, whether sufficient grounds exist to move forward with investigative interviews and/or additional investigative activities that may be appropriate.
3. Examine email logs or other electronic evidence will be conducted in compliance with the *Canadian Charter of Rights and Freedoms*, FOIPPA and applicable government policy.
4. Observe procedural fairness throughout the investigation, based on the principles of natural justice.
5. Engage and share information with the BC PSA and external counsel from Gall, Legge, Grant & Munroe LLP, as appropriate to ensure the investigation adheres to best practices in the conduct of administrative investigations.
6. Should any investigative interviews be conducted, ensure that unionized employees are provided with a reasonable opportunity to have a union representative attend the interview with the employee. Excluded employees will similarly be provided with an opportunity to have a support person attend the interview.
7. Act as liaison to the OIPC on behalf of the Ministry and will share information with the OIPC where the OIPC requests it.
8. Prepare a report, which documents facts and findings in relation to the in-scope items listed above, the decision that is made about whether PCTB will progress to Phase 2 of its investigation, and the rationale and accountability for this decision.
9. Take reasonable steps during the course of its investigation to ensure that information contained in its report, including any investigative findings, are factually correct, reasoned, and will satisfy the “balance of probabilities” test, which is the established burden of proof for administrative investigations.

Steps to be taken will include, but are not limited to:

- Conducting an interview(s) with any person that may be negatively impacted by a finding which the PCTB is contemplating;
- Fairly presenting available pertinent evidence (culpatory and exculpatory) to any person that may be negatively impacted by a finding which the PCTB is contemplating and providing the person an opportunity to respond;
- Conducting an interview with any other person(s) that are known to, or are likely to, have information relevant to the PCTB's investigation;
- Gathering all available evidence, in any form, which is relevant to the PCTB's investigation, especially where the evidence may impact a finding that the PCTB is contemplating;
- In the report, fairly citing any exculpatory evidence found by the PCTB during its investigation and/or that may be presented by an individual during an interview or otherwise; and
- As appropriate, providing an opportunity for parties to review all or portions of the PCTB's report and seeking comment on any factual errors or omissions to ensure accuracy. This may include the head of any public body which employs an individual found to have leaked the OCG report, the head of any public body which is the subject of a PCTB recommendation, and/or individuals who may be negatively impacted by a PCTB finding. PCTB will amend its report prior to finalization, as appropriate, to ensure factual accuracy based on the comments received.

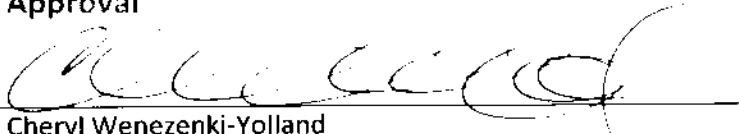
10. Issue the final report including any findings and recommendations to:

- David Curtis (Assistant Deputy Minister, Corporate Information and Records Management Office, Ministry of Finance);
- Cheryl Wenezeki-Yolland (Associated Deputy Minister, Ministry of Finance);
- Athana Mentzelopoulos (Deputy Minister, Finance);
- Lori Hall, Deputy Minister, BC Public Service Agency; and
- The head of any ministry or government agency that employs an individual found to have released the report.
- Further distribution of the final report, portions of the final report or summaries of the material to other entities or those individuals referenced in the material will be determined by the representatives identified above.

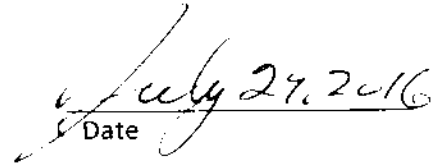
### Timelines

No specific timelines for this investigation are offered.

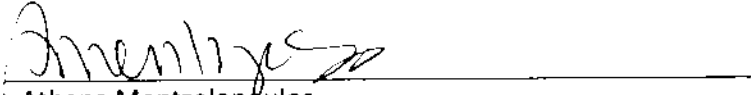
**Approval**



Cheryl Wenezenki-Yolland  
Chief Records Officer and Associate Deputy Minister  
Ministry of Finance  
250-387-8499



Date



Athana Mentzelopoulos  
Deputy Minister  
Ministry of Finance  
250-387-3184

**JUL 29 2016**

Date