



AVR 05 2018
APR

TOP SECRET//SI//Canadian Eyes Only
Cerrid #40568553

BRIEFING NOTE FOR THE MINISTER OF NATIONAL DEFENCE

Response to CSE Commissioner's Annual Review of the CSE Privacy Incidents File, Second Party Incidents File, and Minor Procedural Errors File

(For Approval)

Summary

- The CSE Commissioner recently completed his *Annual Review of the CSE Privacy Incidents File, Second Party Incidents File, and Minor Procedural Errors File*.
- The three files are used by CSE to record operational compliance incidents of privacy interest, and the measures that CSE took to mitigate them.
- The Commissioner was satisfied that CSE took appropriate corrective actions in response to the privacy incidents and minor procedural errors it identified and recorded during the review period.
- There were no recommendations made as a result of this review.

Background

- You received a letter and report from the CSE Commissioner, dated 5 March 2018, providing the results of his *Annual Review of the CSE Privacy Incidents File, Second Party Incidents File, and Minor Procedural Errors File*.
- CSE had put these three files in place to record operational compliance incidents where an activity had run counter to, or in a manner not provided for in, an operational policy. The process enables CSE to demonstrate its commitment to protecting privacy and improving internal practices.
- The CSE Privacy Incident File and Second Party Incidents File record compliance incidents by CSE and its Second Party Partners respectively, where the privacy of a Canadian or a person in Canada may have been impacted due to the nature of the activity or dissemination of the information. The Minor Procedural Error File summarizes incidents where the information was not exposed to external parties and remained within CSE.

- The CSE Commissioner's annual review seeks to examine whether CSE has effectively identified and mitigated the incidents and procedural errors.

Decision/Direction

- This review examined operational compliance incidents recorded by CSE between 1 July 2016 and 30 June 2017. The Commissioner also examined whether the incidents reveal any systemic deficiencies or material privacy breaches.
- The CSE Commissioner was satisfied that CSE took appropriate corrective actions in response to the privacy incidents and minor procedural errors it identified and recorded over the review period, and that there were no material privacy breaches.
- The CSE Commissioner noted that CSE does record sufficient details regarding the incidents in these three files. He encouraged CSE, however, to harmonize vocabulary used to describe the corrective measures undertaken for clarity.
- He indicated that one particular incident will be examined in more detail during an already planned comprehensive review of the activity involved. The Commissioner was, however, satisfied that CSE's response to the incident was adequate.
- The CSE Commissioner provided no recommendations.

Next Steps

- Attached is a proposed package for your consideration and response to the CSE Commissioner.



Greta Bossenmaier
Chief

Minister
of National Defence



Ministre
de la Défense nationale

Ottawa, Canada K1A 0K2

SECRET
CERRID # 40570998

The Honourable Jean-Pierre Plouffe
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Station B
Ottawa, Ontario, K1P 5B4

Dear Commissioner Plouffe:

I am writing to respond to your report dated 5 March 2018, entitled *Annual Review of the CSE Privacy Incidents File, Second Party Incidents File, and Minor Procedural Errors File*.

I am pleased to note that your review demonstrated that CSE took appropriate measures in response to the privacy incidents identified and recorded during the review period. Your findings emphasize CSE's commitment to improving internal practices, and ensuring the lawfulness of its activities.

Thank you for advising me of the results of this review.

Sincerely,

The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

cc: Greta Bossenmaier, Chief

Canada

A-2018-00030--00003

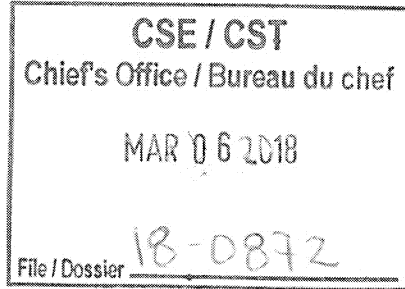
Communications Security
Establishment Commissioner



Commissaire du Centre de la
sécurité des télécommunications

The Honourable Jean-Pierre Plouffe, CD

L'honorable Jean-Pierre Plouffe, CD



TOP SECRET//SI//CEO

Our file # 2200-118

March 05, 2018

The Honourable Harjit S. Sajjan, PC, OMM, MSM, CD, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Subject: Annual Review of the CSE Privacy Incidents File, Second Party Incidents File, and Minor Procedural Errors File

Dear Minister:

The purpose of this letter is to provide you with the results of my annual review of the Communications Security Establishment (CSE) Privacy Incidents File (PIF), Second Party Incidents File (SPIF) and Minor Procedural Errors File (MPEF) during the review period of July 1, 2016, to June 30, 2017. According to CSE, a privacy incident occurs when the privacy of a Canadian is put at risk in a manner that runs counter to, or is not provided for, in its operational policies.

To ascertain whether CSE has effectively identified, mitigated and reported privacy incidents and procedural errors, I have reviewed the PIF, SPIF, and MPEF records, received answers from CSE to my questions, and performed an independent verification of CSE's reporting databases.

Annex A provides additional background information.

I concluded that **CSE complied with the law and protected the privacy of Canadians:**

- I am satisfied that CSE took appropriate corrective actions in response to the privacy incidents, Second Party incidents, and minor procedural errors it identified and recorded over the review period.
- My review did not reveal any material privacy breaches, systemic deficiencies or issues that require a follow-up review not already planned.
- I am making no recommendations.

Findings

A) MPEF Results

I agree with CSE's assessment that the 10 errors in the July 1, 2016, to June 30, 2017, MPEF were minor and did not result in a privacy incident. [redacted] in the MPEF consisted of unopened files that may have contained Canadian identity information (CII) that were kept beyond the retention period allowed.

[redacted] concerned a technical malfunction affecting a list whose purpose is to control CSE staff access to certain types of information. The malfunction temporarily prevented the system from denying access to the information by persons who no longer had the appropriate permission. The issue was addressed.

[redacted] concerned CII being visible on an internal communication tool; however, only permitted persons saw the information, which was then deleted.

[redacted] concerned a malfunctioning collection system which, for a period of time, risked collecting two-end Canadian information. However, no such information was collected before the issue was addressed. [redacted] would have constituted a privacy incident, and not a minor error, had two-end Canadian information been collected during the malfunction period.

B) SPIF Results

I agree with CSE's assessment that the 33 incidents listed in the SPIF

[redacted] In all instances, CSE requested that the identified issue be rectified and followed-through to ensure corrective steps were taken by the party concerned.

[redacted] entries concerned the identification of CII in Second Party reports. All reports were reissued, corrected, cancelled, or retroactively exempted.

[redacted] entries concerned

[redacted] entries concerned gaps in awareness or understanding of CSE's Canadian privacy protection policies by groups within a Second Party or a Canadian partner. In [redacted] cases, the concerned party provided remedial policy awareness materials to the concerned groups.

C) PIF Results

Over the July 1, 2016, to June 30, 2017, review period, CSE identified a total of 48 privacy incidents, none of which CSE has considered amounting to material privacy breaches; I agree with such an assessment.

entries concerned the use or identification of unsuppressed CII. I am satisfied that appropriate corrective actions, such as suppressing the exposed CII and correcting, reissuing, or cancelling reports, were taken by CSE in each case.

entries are interlinked:

were appropriately addressed and corrected.

entries concerned appropriate remedial measures were taken

I am satisfied that

entries concerned I am satisfied CSE took appropriate remedial action when necessary,

CSE.

In the majority of cases, a privacy incident was recorded

concerning will be examined in-depth in the upcoming, planned review of this topic. Given the exceptional circumstances and the urgent, threat-to-life nature of I am satisfied that, although the employee's actions were contrary to CSE policy, CSE's response was adequate. I am informed that corrective policy measures have recently been formalized.

TOP SECRET//SI//CEO

concerned a malfunctioning collection tool which allowed CII to be ingested into CSE repositories over a certain period of time. The satisfactory identified and corrected.

D) General Observations

Respecting the contents and form of the PIF, SPIF, and MPEF records, I am satisfied that they contained sufficient details.

I encourage CSE to ensure that the vocabulary surrounding reporting between SIGINT and IT Security activities be harmonized. For example, CSE should ensure consistency of use and meaning behind the verbs “cancelled,” “reissued,” and “corrected.” In addition, given that issues with an IT Security report are sometimes solved by modifying access control lists, CSE should consider developing a term to reflect this corrective measure.

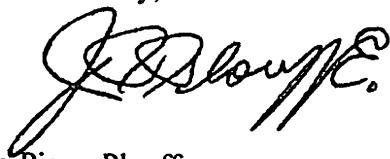
I would also like to take this opportunity to commend the IT Security Program Oversight Centre (IPOC) team for the quality of its IT Security privacy incident reports, which are clear and informative.

I intend to continue to conduct an annual review of CSE’s PIF, SPIF, and MPEF.

Before this report was finalized, CSE officials had an opportunity to review it for factual accuracy.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,



Jean-Pierre Plouffe

cc: Ms. Greta Bossenmaier, Chief, CSE

Annex A

Background

This review was undertaken under the Commissioner's general authority as articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act* (NDA) and covers the period from July 1, 2016, to June 30, 2017.

CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities* (August 2, 2016), requires CSE foreign signals intelligence (SIGINT) and IT Security analysts, supervisors and managers to report and document privacy incidents. The reporting and tracking of privacy incidents and procedural errors is one measure used by CSE to promote compliance with legal and ministerial requirements and operational policies and procedures, and to enhance the protection of the privacy of Canadians by documenting incidents and errors, and associated corrective actions.

CSE examines compliance incidents to determine whether internal or external recipients were exposed to sensitive personal information of Canadians without appropriate authorization, and whether the incidents could result in potential harm to the Canadians. The PIF is a record of incidents attributable to CSE involving activities conducted in a manner counter to CSE operational policy and privacy guidelines and information being exposed to external stakeholders who ought not to have received it. The SPIF is a record of similar compliance incidents attributable to Second Party partners. These incidents may be identified by the partners themselves, or by CSE. The MPEF is a record of incidents where the information was contained within CSE and not exposed to external recipients.

The annual review of the PIF, SPIF, and MPEF focuses on incidents not examined in detail in the course of other reviews. It permits the identification of trends or systemic weaknesses that might suggest a need for corrective action, changes to CSE's processes or policies, or for the Commissioner's office in-depth review of a specific incident or activity. For example, the Commissioner's office could investigate an incident identified by CSE as a material privacy breach or could examine an incident to determine whether it was a material privacy breach.

Treasury Board of Canada Secretariat (TBS) defines a material privacy breach as a breach that "involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals," — (*Guidelines for Privacy Breaches*, section 4, May 20, 2014). The Deputy Chief Policy and Communications is CSE's Chief Privacy Officer, and is responsible to determine, in consultation with the Department of Justice Canada, if an incident constitutes a material privacy breach. Such determination is guided by the TBS diagnostic tools relating to material privacy breaches and CSE's internal policies and procedures.