Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET // SI // CEO

Our file # 2200–88

March 31, 2014

The Honourable Robert Nicholson, P.C., Q.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Dear Minister:

The purpose of this letter is to provide you with the results of my annual review of the Communications Security Establishment Canada's (CSEC) Privacy Incident File (PIF) and Minor Procedural Errors Report (MPER) for calendar year 2013. This review was undertaken under my general authority as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*).

According to CSEC, 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. CSEC requires its foreign signals intelligence (SIGINT) and information technology (IT) security employees to report and document privacy incidents in order to demonstrate compliance with legal and ministerial requirements, with CSEC policies, and to prevent further incidents. The PIF records those incidents where privacy was breached. On the other hand, the MPER contains operational errors that occurred in connection with privacy information but that did not result in privacy information leaving the control of CSEC, or privacy information being exposed to external recipients who ought not to have received that information. The PIF and MPER represent a voluntary CSEC initiative to record what CSEC defines as privacy incidents.

My reviews of CSEC activities generally include an examination of any privacy incident relating to the subject of the review. The annual review of the entire PIF and MPER focuses on incidents not examined in detail in the course of my other reviews, to assure myself that CSEC took appropriate corrective actions for all privacy incidents it identified in the PIF and the MPER.

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
T: 613-992-3044 F: 613-992-4096

The objectives of the review of the PIF and the MPER were to: acquire knowledge of the incidents, procedural errors and subsequent actions by CSEC to correct the incidents or mitigate the consequences; to inform development of my work plan by determining what privacy incidents, procedural errors and related activities, if any, may raise issues about compliance or the protection of the privacy of Canadians, and therefore should be subject to follow-up review; and to assist me in evaluating CSEC's policy compliance validation framework and monitoring activities.

Based on my review of the PIF and MPER records as well as an independent verification by my office of a sample of specific reports in [redacted] — CSEC's database of SIGINT reports — I am satisfied that CSEC took appropriate corrective actions in response to the privacy incidents and minor procedural errors it identified and recorded during 2013. My review did *not* reveal any systemic deficiencies or issues that require follow-up review. However, I am making one recommendation, which I describe later in this letter.

I found that the [redacted] errors in the MPER for 2013 were minor and, in fact, did not result in a privacy incident. [redacted] entries in the MPER were errors about information that did not leave the control of CSEC and [redacted] entries concerned Canadian identity information exposed to external recipients not resulting in a breach of privacy.

In 2013, CSEC identified and recorded [redacted] privacy incidents in its PIF. Of these, [redacted] involved the unintentional sharing or inclusion, in a report or in e-mail exchanges, of Canadian identity information by CSEC or by one of its second party partners in the United States, the United Kingdom, Australia or New Zealand. [redacted] incidents concerned CSEC or a second party partner unknowingly targeting a Canadian or a person in Canada. [redacted] incidents involved CSEC unintentionally conducting a metadata query [redacted] a Canadian without proper pre-authorization.

[redacted] privacy incidents involved CSEC's second party partners. The majority of these incidents involved the inadvertent targeting or reporting of a Canadian by a Second Party. [redacted] incidents involved Government of Canada departments or agencies other than CSEC. [redacted] incidents involved multiple violations of privacy, for which CSEC provided a retroactive blanket naming exemption to avoid drawing unwarranted attention to the Canadian.

CSEC provided satisfactory answers to all of my questions about the privacy incidents. CSEC did *not* become aware of any adverse impact on the Canadian subjects of the privacy incidents.

I am particularly pleased with certain follow-up activities taken by CSEC to prevent future privacy incidents and minor procedural errors similar to those identified. For example, a certain group has created a document of suppressed Canadian identity information to help prevent the unintentional naming in CSEC end-product reports of

entities already known to be Canadian. To protect the privacy of the Canadians found on the list, this document is accessible only to a small group of team leaders. Also, CSEC's policy development team identified imprecise portions of CSEC's policy OPS-1-7, *Operational Procedures for Naming in SIGINT Reports* (revised effective July 17, 2012), that it will be clarifying in an upcoming update. I will monitor the impact of the changes to this policy in future reviews.

One privacy incident resulted from the provision of a list of telephone numbers provided by [redacted] to a particular team within CSEC's Directorate General Intelligence, which resulted in CSEC not suppressing a Canadian's name and phone number in a report, and [redacted] without proper authorization. [redacted] SIGINT Programs Oversight and Compliance (SPOC) advised the team at CSEC to standardize its procedures to prevent the recurrence of that type of incident. In his February 2013 *Review of CSEC Activities Relating to* [redacted] my predecessor raised the clarity of language as an issue when information is shared between CSEC and its Government of Canada partners. He recommended the following:

> It is recommended that CSEC promulgate policy guidance respecting how to clearly and consistently identify in its communications with Government of Canada and second party partners whether an identifier or selector is believed to be used by an entity, used by an associate or contact of an entity, or suspected to relate to an entity (p. 20).

In my February 2014 *Review of the Activities of the Office of Counter Terrorism*, I discuss the implementation of the Information Needs disclosure process introduced by CSEC in 2006–2007 to standardize and assist it in tracking sensitive disclosures by federal law enforcement and security agencies that wish to share foreign lead information. This process has helped prevent the use of imprecise and inconsistent language in such exchanges. I accept CSEC's explanation of why a technical issue at that time resulted in this particular exchange being made outside of the Information Needs process. I will continue to monitor CSEC information exchanges with partners to ensure proper processes are followed and that there is clarity of language.

As stated by my predecessor in his July 2013 *Review of CSEC SIGINT Information Sharing with the Second Parties*, "[t]he amount of [foreign signals intelligence] CSEC provides to and receives from the Second Parties is extensive. Information sharing is an essential component of CSEC SIGINT collection and other activities." (p. 27) As a result of this extensive information sharing, the majority of privacy incidents filed by CSEC involve second party partners including Canadian identity information in their reports or unintentionally targeting a Canadian. I find that CSEC takes appropriate measures to protect the privacy of Canadians when a privacy incident involves a Second Party. For example, when it becomes aware of a second party report containing Canadian identity

information, CSEC may request the Second Party to re-issue a report suppressing such information, and to stop targeting the Canadian, if such is the case. CSEC subsequently verifies the cancellation — or reissuance with the Canadian identity information suppressed — of the report in its [redacted] database of reports.

However, when CSEC sends a request to a Second Party to stop targeting a Canadian, it is not a general practice for CSEC to seek confirmation of such de-targeting. Because of the enhanced potential of the violation of the privacy of a Canadian if a Second Party targets that Canadian, **I recommend** that CSEC request second party partners to confirm de-targeting of Canadians, and indicate in the PIF whether the Second Party has confirmed that it stopped targeting that Canadian. This measure will enhance the protection of the privacy of Canadians and support you as Minister of National Defence in your accountability for CSEC. I recognize that although the Second Parties pledge *not* to direct activities at each other's citizens, they are sovereign nations and may derogate from their agreements, if it is judged necessary for their respective national interests.

I intend to continue to conduct an annual review of CSEC's PIF and MPER. I will monitor developments with regard to the findings and recommendation I have made in this review.

CSEC officials were provided an opportunity to review and comment on the results of the review, for factual accuracy, prior to finalizing this letter.

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

Yours sincerely,

Jean-Pierre Plouffe

c.c. Mr. John Forster, Chief, CSEC