National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

~~TOP SECRET // SI // CEO~~

NSIRA Review 08-501-02

January 8, 2020

The Honourable Harjit Sajjan
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Subject: Review of the Communications Security Establishment's Self-Identified Privacy Incidents and Procedural Errors

Dear Minister:

The purpose of this letter is to provide you with the report of our review of the Communications Security Establishment's (CSE) self-identified privacy incidents and procedural errors, as identified through the Privacy Incidents File (PIF). This review was conducted under the authority of paragraph 8(1)(a) of the *National Security and Intelligence Review Agency Act*. This report is provided to you pursuant to section 34 of the *NSIRA Act*.

The review of the PIF is the first ever review of CSE by the National Security and Intelligence Review Agency (NSIRA) since the coming into force of the *NSIRA Act* in 2019. Given the unique circumstances of NSIRA's recent establishment and the various logistical and procedural challenges associated with this transition, I appreciate CSE's assistance in completing this review in a timely manner. Before this review was finalized, CSE officials had an opportunity to review it for factual accuracy.

Building on the foundation of this review, NSIRA looks forward to working with CSE to expand our knowledge and understanding of CSE's mission and challenges.

NSIRA officials will work with CSE to redact the final report for release to the public. We hope the process for redaction will be completed in eight weeks or less. NSIRA also intends to engage with the Office of the Privacy Commissioner in relation to certain aspect of this review.

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *1-833* 890-0293 Fax: *613* 907-4445

As I mentioned in my letter of December 19 2019, I would be pleased to meet with you to discuss this review and brief you on NSIRA's role more broadly.

Yours sincerely,

Murray Rankin, Q.C.,
Chair, National Security and Intelligence Review Agency

cc: Shelly Bruce, Chief, Communications Security Establishment

National Security and Intelligence
Review Agency

Office de surveillance des activites en matiere
de security nationale et de renseignement

~~TOP SECRET // SI // CEO~~

REVIEW OF CSE'S SELF-IDENTIFIED PRIVACY INCIDENTS AND PROCEDURAL ERRORS

(NSIRA REVIEW 08-501-2)

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *1-833* 890-0293 Fax: *613* 907-4445

I EXECUTIVE SUMMARY

1. According to the Communications Security Establishment (CSE), a privacy incident occurs when the privacy of a Canadian, or a person in Canada, is put a risk in a manner that runs counter to, or is not provided for, in its policies. Privacy incidents are unavoidable due to the nature of CSE's activities. Accordingly, the National Security and Intelligence Review Agency (NSIRA) does not expect that CSE's operations should result in zero privacy incidents.

2. CSE reports and documents all known privacy incidents by cataloguing them into the Privacy Incidents File (PIF). NSIRA examined a selected sample of incidents reported in the PIF for the period of July 1, 2018 to July 31, 2019. NSIRA examined electronic records, files, correspondence, and other documentation, such as policies, procedures and any legal advice relevant to the selected sample of incidents. Additionally, tests were conducted by NSIRA staff on the information obtained from CSE against CSE's systems for independent verification.

3. Based on the records provided by CSE and an independent verification from NSIRA, for the privacy incidents examined, NSIRA believes that CSE employed compliance measures in a timely manner and according to policy. However, NSIRA has made the following five findings and corresponding recommendations to improve CSE's documentation, assessment, and mitigation of privacy incidents:

- CSE has adopted a layered approach to increasing privacy protection measures. However, CSE is not using the PIF, or any similar collated record of privacy incidents, to prevent systemic incidents from re-occurring, or to identify any areas of weakness in existing policy and/or practice. Accordingly, NSIRA recommends that CSE examine the totality of all privacy incidents with the view to identifying systemic trends or any areas of weakness in existing policy and/or practices that may reduce the occurrence of privacy incidents.

- The mitigation, documentation, and reporting of privacy incidents was inconsistent and did not always meet the transparency and accountability objectives set out in CSE internal policy. Moreover, incidents were not always assessed with a view to determining the impact on lawfulness and/or the privacy of Canadians. NSIRA recommended that CSE adopt a consistent approach to assessing and documenting all privacy incidents.

- For some incidents, the mitigation measures after an incident is discovered focuses on deleting the information with a privacy interest. CSE does not examine how the information may have been used prior to its deletion, or the potential that this information exists in a format beyond the control of CSE. NSIRA recommends that CSE always examine how information may have been used prior to deletion in order to determine if further mitigation measures are warranted.

- Furthermore, CSE's assessment of whether an incident was a material privacy breach was limited. As per the Treasury Board of Canada Secretariat's Directive on Privacy Practices, CSE must report the occurrence of material privacy breaches. NSIRA recommends that CSE standardize its policy on assessing whether incidents constituted a material privacy breach.

- Finally, CSE's policy of granting a for the inadvertent naming of a Canadian or person in Canada in SIGINT reports, is not an appropriate method to mitigate the impact and risk to privacy in cases of inadvertent naming. NSIRA recommends that CSE rescind this practice or obtain a legal opinion on this mitigation mechanism.

4. This review did not include an analysis to identify trends or systemic weaknesses, which was an area of focus for previous PIF reviews conducted by the Office of the Communications Security Establishment Commissioner. However, this will be a priority in future NSIRA reviews.

5. Additionally, under the authority of section 15.1 of the *NSIRA Act*, NSIRA intends to work with the Office of the Privacy Commissioner to determine the process for reporting future privacy incidents at CSE.

II AUTHORITIES

6. This review was conducted under the authority of the National Security and Intelligence Review Agency (NSIRA), as articulated in subsections 8(1)(a) and 8(1)(b), as well as sections 9 and 11, of the *National Security and Intelligence Review Agency Act*.

III INTRODUCTION

7. The Communications Security Establishment (CSE) reports and documents any privacy incidents that are associated with its activities, or those of its Second Party agencies[1] or domestic partners, where the privacy of a Canadian, or a person in Canada, is put at risk in a manner that runs counter to, or is not provided for, in existing policy. This is known as a privacy incident.[2] The incidents are recorded in one of three sub-files, depending on where the incident occurred and its potential to cause harm:

- **The Privacy Incidents File (PIF):** the PIF is a record of incidents attributable to CSE involving information about a Canadian (person or business), or any person

[1] Second Party partners are the national cryptologic agencies of Australia (Australian Signals Directorate), Great Britain (Government Communications Headquarters), New Zealand (Government Communications Security Bureau), and the United States of America (National Security Agency). CSE works collaboratively with Second Party partners in the interest of responding to shared intelligence priorities and advancing common objectives.
[2] *Mission Policy Suite,* Part A, section 33.4, and *Mission Policy Suite,* Part B, section 27.2.

in Canada, that was handled in a manner counter to, or is not provided for, in existing policy. This type of mishandling is labelled a "privacy incident."[3]

- **The Second Party Incident File (SPIF):** The SPIF is a record of privacy or compliance incidents that involve a Canadian or a person in Canada, and are attributable to a Second Party partner or a domestic partner. These incidents may be identified by partners or by CSE. This type of mishandling is also labelled as a "privacy incident."[4]
- **The Minor Procedural Error File (MPEF):** The MPEF is a log of operational compliance incidents where CSE improperly handled information about a Canadian or a person in Canada, but the information was contained within CSE. This type of mishandling is labelled a procedural error.[5]

8. Collectively these three sub-files are known as the PIF. The PIF is used to collate records of self-reported incidents that may have a privacy impact, despite the privacy measures that are in place. As such, it represents a portion of CSE's overall efforts to protect the privacy of Canadians. It is also important to recognize that these are CSE's self-identified incidents. According to CSE, the PIF is used to demonstrate compliance with its operational policies and legal requirements, and to prevent further incidents.[6]

9. NSIRA is conscious that privacy incidents are unavoidable due to the nature of CSE's activities and the nature of the global information infrastructure. For instance,

NSIRA does not expect that CSE's operations should result in zero privacy incidents or procedural errors.

10. The review of the incidents in the PIF was an annual review by the Office of the Communications Security Establishment Commissioner (OCSEC), CSE's previous external review body. This year's review of the PIF is the first ever review of CSE by NSIRA since the coming into force of the *NSIRA Act*.

11. Given the unique circumstances of NSIRA's recent establishment and the various logistical and procedural challenges associated with this transition, this review was only made possible with the support of CSE staff. In addition, NSIRA had to familiarize itself with CSE's unique and complex operational environment and activities while simultaneously carrying out this review. Building on this early foundation, NSIRA will work with CSE to obtain more background technical briefs to continue to build a solid foundational knowledge on CSE's mission and challenges.

---

3 Information Sharing, *Standard Operational Procedure 4: Handling Privacy Incidents*, section 3.1.
4 Information Sharing, *Standard Operational Procedure 4: Handling Privacy Incidents*, section 4.1.
5 Information Sharing, *Standard Operational Procedure 4: Handling Privacy Incidents*, section 5.1.
6 Information Sharing, *Standard Operational Procedure 4: Handling Privacy Incidents*, section 3.1.

IV BACKGROUND

12. It is a shared responsibility across CSE to report privacy incidents, mitigate incident impacts, and to log incidents into the PIF (see Annex F for a process flowchart). Dependant on the mandate under which the incident occurred, two different compliance teams manage incidents. is responsible for privacy incidents that occurred under the foreign intelligence mandate. The is responsible for incidents under the cyber security mandate.[7]

13. Incidents are typically self-reported by analysts through a webform to their respective compliance team as soon as an incident happens, however some incidents are discovered through internal reviews and compliance activities. Once a privacy incident is discovered, document, mitigate, and monitor the incident according to their respective policies.[8]

14. After an incident is managed and follow-up activities are completed, if there is a privacy interest that affects a Canadian or a person in Canada (Canadian privacy interest), the details of the incident are sent to the group for inclusion in the PIF.[9] informs of incidents as soon as an incident occurs, whereas informs of incidents on a quarterly basis. Once is informed of an incident for inclusion in the PIF, will assess the incident to determine if it constitutes a material privacy breach.[10]

15. For incidents attributable to Second Parties, the Second Party will contact directly, who will then, among other things, request that the Second Party take appropriate actions to mitigate the privacy impact on the Canadian or person in Canada.

16. For the review period, a combined total of 123 incidents were included in the PIF, SPIF and MPEF. Through the PIF and the MPEF, incidents were attributable to CSE. Of those incidents, incidents occurred under CSE's foreign intelligence mandate. incidents occurred under CSE's cyber security mandate, and incidents occurred under CSE's assistance mandate.[11]

17. incidents in the SPIF, were attributable to a domestic partner. sharing incidents in the SPIF. The remaining privacy incidents were due to activities by Second Party partners.

---

[7] Information Sharing, "The Privacy Incidents File" deck, presented to NSIRA on August 19, 2019.
[8] CSE response to RFI-6, questions 20-21, received by NSIRA on October 16, 2019.
[9] CSE response to RFI-6, questions 20-21, received by NSIRA on October 16, 2019. Note that an incident may be considered a compliance incident, which is an activity contrary to policy with no Canadian privacy aspect to the incident.
[10] CSE response to RFI-6, question 21, received by NSIRA on October 16, 2019.
[11] In the PIF, incidents are recorded as occurring under CSE's Part C Assistance mandate. Upon clarification by NSIRA, incident was mistakenly listed as occurring under Mandate C. CSE response to RFI-6, question 1, received by NSIRA on October 29, 2019.

incidents

18. Incidents can be categorized into types of incident, which often dictate the corresponding mitigation actions that CSE would take in response (explained in Annex C). Common incidents for activities under the foreign intelligence mandate, such as targeting, naming, , and searching incidents have defined policy, operating procedures or working aids on how to mitigate the incident. Other incident types are less comparable to each other since they vary in scope and consequence, such as data handling and retention incidents. There are no standard mitigation measures developed for these types of incidents.

19. The incidents included in the PIF for the review period, broken down by incident type (for a description of incident types, please see Annex C) and sub-file is as follows:

	Collection	Data Handling/ Retention		Naming	Search	Sharing	Targeting	Targeting and Naming	Total
PIF									
SPIF									
MPEF									

20. In OCSEC's review of the PIF from July 1, 2017 to June 30, 2018, CSE identified 44 privacy incidents for inclusion in the PIF, 31 incidents in the SPIF, and 11 errors in the MPEF. While entries in the SPIF and MPEF are consistent this year compared to last, there is an increase for incidents in the PIF. Due to the delay in receiving the PIF from the previous four years,[12] NSIRA was not able to assess trends in privacy incidents for this review.

V FINDINGS AND RECOMMENDATIONS

Uses of the PIF at CSE

21. As outlined in CSE's *Mission Policy Suite* (MPS),[13] Part A (foreign intelligence mandate), section 33.4, CSE is responsible for reporting and documenting privacy incidents in order to:

- Meet policy and legal requirements;

[12] Initially requested in RFI-1, sent to CSE on August 22, 2019. Received by NSIRA on October 15, 2019, and October 24, 2019.
[13] The *Mission Policy Suite* is CSE's policy framework that guides all operational activities.

- Prevent similar incidents from occurring; and
- Identify any areas of weakness in existing policy and/or practice.

22. Likewise, in Part B (cyber security mandate) the MPS, section 27.2, it is CSE's responsibility to report and document privacy incidents in order to:

- Correct or mitigate the potential harm to the individual or entity;
- Meet legal requirements for accountability;
- Prevent similar incidents from occurring; and
- Identify any opportunities for clarification in existing policies and/or practices.

23. NSIRA expected to see that the documentation and reporting of privacy incidents through the PIF was used by CSE as a means to prevent similar privacy incidents from occurring and to identify any areas of weakness in existing policy and/or practice. However, NSIRA found that CSE is not using the collated documentation and reporting of privacy incidents to prevent systemic incidents from re-occurring, or to identify any areas of weakness in existing policy and/or practice that may reduce the occurrence of privacy incidents. The utility of reporting and documenting privacy incidents is questioned if there is limited strategic action or commitment by CSE to use the documentation of incidents to reduce the potential impact of its activities to Canadian privacy interests.

24. CSE has mitigation methods for some types of common incidents to ensure that the same factual scenario causing an incident does not re-occur. For example, in targeting incidents, an analyst will protect the Canadian and their associated selectors to ensure that they are not re-targeted, thus preventing another incident based on the same selectors from re-occurring.

25. **Finding no. 1: For privacy incidents where a policy existed for compliance measures, CSE employed these measures in a timely manner and according to policy.**

26. NSIRA did not come across any evidence that CSE is implementing a strategic or comprehensive approach to reducing the total occurrence of privacy incidents. During the period of review, have not made any recommendations to senior management based on identified areas of weakness in existing policy or practices due to a privacy incident or procedural error.[14]

27. The lack of changes in policies and practices based on privacy incidents raises questions for the period of review as privacy incidents increased by 81% from the previous year.[15] The increase in privacy incidents is something NSIRA will follow up on

[14] CSE response to RFI-3, question 6, received by NSIRA on October 4, 2019.
[15] 80 incidents in the PIF from July 1, 2018 to July 31, 2019, versus 44 from July 1, 2017 to June 30, 2018.

in a future study or review.

28. Within the broader compliance framework at CSE, both are required to maintain an annual compliance framework or plan to facilitate internal reviews and to monitor activities for compliance with CSE policies and procedures. The results of these compliance activities are circulated to senior management on a bi-annual basis through the compliance reports, which also include reporting on privacy incidents. Regularly planned compliance reviews may also inform recommendations to management and policy teams.

29. NSIRA recognizes that internal compliance frameworks and activities are important to CSE's enforcement of policy and privacy protection measures. CSE compliance efforts are fuelled by both technical expertise and an intimate knowledge of operations. However, NSIRA observed that internal CSE compliance initiatives are rooted in existing compliance review frameworks that are the product of already established policies and procedures.

30. Based on the annual compliance frameworks and reporting available to NSIRA at the time of review,[16] it was difficult to identify what actions CSE is taking to reduce systemic occurrences of privacy incidents in the SIGINT program. reporting on privacy incidents appears to focus on the quantity of privacy incidents and rarely provided detailed analysis of why incidents might be occurring or provided recommendations to reduce their frequency. Rather, compliance review frameworks focused on reviews of activities to ensure that privacy protection measures are in place and functioning.

31. **Finding no. 2: While CSE has adopted a layered approach to increasing privacy protection measures, CSE is not using the PIF, or any similar collated record of privacy incidents, to prevent systemic incidents from re-occurring, or to identify any areas of weakness in existing policy and/or practice that may reduce the occurrence of privacy incidents.**

Recommendation no. 1: CSE should look at the totality of all privacy incidents with the view to identifying systemic trends or any areas of weakness in existing policy or practices.

32. As stated earlier, NSIRA is conscious that privacy incidents are unavoidable due to the nature and volume of CSE's activities. NSIRA does not expect that CSE's

[16] As part of RFI-1, NSIRA was only able to view 2017 Annual SIGINT Compliance Report and their semi-annual compliance report for January-June 2018 and July-December 2018, as the semi-annual report for the first half of 2019 was not available at the time of review. NSIRA received Internal Compliance Reports for April 1, 2018 to September 30, 2018; and October 1, 2018 to March 31, 2019. The remaining bi-annual reports for the period of review were not available at the time of review.

operations should result in zero privacy incidents or procedural errors. However, the reporting and documentation of privacy incidents should be used as a tool to reduce incidents of a similar nature. Currently, _ compliance and reporting framework does not appear to incorporate strategic plans for reducing privacy incidents related to SIGINT activities.

Assessing and Documenting Privacy Incidents

33. The PIF is intended as a summary document and is not expected to include all of the details of a particular incident. NSIRA expected that all essential information about an incident would be captured in the supporting records, in whatever form they may take, such as the incident webform or email correspondence, and be available for review by NSIRA.

34. Upon examination of the PIF and all supporting records related to incidents, NSIRA found that, as part of the incident management process, CSE did not consistently conduct a thorough analysis of the authorities underpinning the incident and the privacy impacts, pursuant to their obligations under the MPS.

35. The MPS is a developed set of policy principles that derive from the CSE legal framework comprised of the *National Defence Act*, the *Privacy Act*, Ministerial Authorizations, Ministerial Directives and other relevant Canadian legislation. The MPS requires that CSE mitigate and document privacy incidents for management awareness and accountability. MPS, Parts A and B further outlines transparency and accountability as a broad policy principle that governs the lawful conduct of CSE's activities.[17] Before an incident is included in the PIF, assess, document and mitigate incidents according to their own policies. However, NSIRA observed that the approach to assessing and documenting incidents differed between and resulted in inconsistencies in the way that CSE met their transparency and accountability obligations.

36. For MPS, Part B, section 27.2.1 requires an incident report be created for every privacy incident. This includes an assessment of:

- Why the incident is a privacy incident, including the policies or laws that were breached;
- Recommendations for corrective action and to prevent incidents of a similar nature from reoccurring; and
- An analysis of the affected privacy interest.

[17] Transparency and accountability is a broad policy principle that governs the lawful conduct of CSE's activities under the foreign intelligence mandate and the cyber security mandate, as per CSE's Mission Policy Suite. Under the foreign intelligence mandate, activities are subject to internal and external review, and all related records of decision must be logged and documented to facilitate the review (MPS, Part A, section 2.5). Under the cyber security mandate, activities are subject to internal and external review, and activities must be accompanied by documentation to facilitate the review process (MPS, Part B, section 2.5).

37. Reports also include an *Impact Assessment* based on an *Impact Assessment Tool*, which is used to support consistent analysis of the scope and severity of a compliance or privacy incident.[18] This calculation is based on the risk to confidentiality, integrity, and availability of the data. NSIRA received a privacy incident report for all incidents under the responsibility of privacy incident reports were detailed and clearly outlined how had followed-up on each incident. Further, the reports demonstrated that every privacy incident evaluated in NSIRA's directed sample was assessed with a view to determining the impact to privacy interests.

38. However, reports did not always include a rationale as to how incidents were assessed, nor did they include how the risk to confidentiality, integrity and availability of data was assessed with regards to the facts underlying the incident. NSIRA suggests that continue the routine consideration of privacy impacts for each incident, and go further to ensure that all reports include justifications for the conclusions reached on the impact assessment.

39. In contrast, does not complete a similar report for each privacy incident. Currently, CSE policy does not require a routine analysis of privacy impacts for every incident. MPS, Part A, section 33.4.1, only requires an analysis of privacy impacts for complex cases. Moreover, in the *Incident Handling Guide,* a privacy impact assessment is only conducted if incidents are escalated to senior management.

40. NSIRA believes that by not creating a report for each privacy incident, the policy principles of transparency and accountability are not reflected in documentation and reporting practices. A policy that defers an analysis of an incident's impact on privacy and does not consider the policy instruments that were breached does not demonstrate the requisite degree of accountability and transparency.

41. The information included in the PIF and supporting documentation did not indicate that the incident's impact on privacy was considered. Likewise, the information did not identify the authorities under which the activity was conducted nor the policy instruments that were breached. During the period of review, only one SIGINT-related incident was clearly assessed for privacy impacts when it was briefed to senior management through a quarterly PIF report.[19] NSIRA notes that the practice of only assessing the privacy impacts of an incident when it is flagged to senior management is inadequate, as it permits little or no analysis of the impact of such incidents on the privacy of Canadians.

---

[18] CSE response to RFI-6, question 13, received by NSIRA on October 28, 2019.

[19] Incident CSE response to RFI-4, question 6, received by NSIRA on October 16, 2019. For context, this item was reported differently as it was identified, investigated, and mitigated by given that it involved an error in the technical implementation of a Five-Eyes agreement to limit the dissemination of certain lines of reporting. Therefore, this incident was handled differently as it was detected and managed by an area outside of the program.

42. Furthermore, the methodology and criteria used for determining the privacy impacts for the one SIGINT-related incident briefed to senior management is unclear. For this incident, reports containing were disseminated incorrectly, resulting in unauthorized individuals viewing these reports. The privacy impact of the incident was determined by whether the incident could be expected to cause serious injury or harm, which is a criterion for an analysis of a material privacy breach. This analysis did not refer to CSE's other privacy protection obligations under the MPS, the *Privacy Act* in the use and disclosure of personal information, obligations under the *National Defence Act,* or any requirements from Ministerial Authorizations. As NSIRA did not see any documentation that indicated CSE's Directorate of Legal Services (DLS) was consulted when an incident occurs, it is not apparent the extent to which DLS is consulted when a privacy incident occurs since it is not required within policy.

43. Moreover, CSE's file documentation seems to consider that any harm is limited since individuals who accessed this information had a TOP SECRET clearance, were indoctrinated to SPECIAL INTELLIGENCE, and accessed the report on . The scope and number of individuals who wrongly viewed the report is clearly a factor for consideration. However, having the requisite security clearance to access the report does not completely remove any privacy impacts, yet CSE did not examine how this information might have been used. Further, relying on a clearance status as a mitigating factor the privacy assessment does not account for the 'need-to-know' basis of all SIGINT reporting.

44. The failure to identify the policy or legal instruments that were breached, as well as an assessment of the privacy impacts of incidents, results in a gap in responsibility and does not meet accountability and transparency standards. For example, without any documentation to support an incident assessment, it appears that CSE simply concluded that the privacy impact of an incident is low. Since the extent of an incident's impact is not thoroughly assessed, there is a risk that similar incidents may re-occur and that existing areas of weakness in policy or practice not be identified.

45. The lack of SIGINT incident reports made it difficult for NSIRA to track and follow-up on mitigation incidents, especially for incidents where NSIRA requested supporting documentation from CSE. NSIRA observed that for incidents under the control of , the supporting documentation provided was sparse and inconsistent, and was missing information in some cases.[20] This made it difficult to understand the narrative and context of a SIGINT-related incident, whether there was any analysis of the incident, and whether mitigating actions were taken. A consistent incident report format would provide for a more complete record of an incident and would ensure that there is enough information for NSIRA and CSE's management to

[20] For example, in cases of or targeting where traffic must be purged, email confirmation that a traffic purge was completed was not always included in the supporting documentation. In other incidents, correspondence would be referred to that was not included in the supporting documentation. Refer to RFI-6, question 16: "Please provide confirmation... that a purge or deletion occurred in the following incidents".

assess the incident.

46. **Finding no. 3: CSE's approach to assessing and documenting privacy incidents was inconsistent and did not meet their transparency and accountability objectives in relation to the self-reporting of privacy incidents.**

Recommendation no. 2: should emulate approach to reporting on privacy incidents, so that an incident report is completed for every incident with a Canadian privacy interest.

47. NSIRA suggests that for each privacy incident, reports should:

- Identify the program or authority under which the activity was conducted;
- Identify the contravened policy instruments or authorities; and
- Assess and document the privacy impacts of the incident.

48. already has tools available to guide the implementation of such a requirement. One incident during the period of review included a incident report, which included a detailed description of the incident and why it occurred, mitigation actions, recommendations based on the incident, and whether managerial attention is required.[21] Additionally, *Stakeholder Interview Questionnaire*[22] includes essential and useful information that is not currently captured in the PIF or supporting documentation, such as a series of questions on whether the privacy of Canadians was compromised. These tools could be utilized to gather evidence and document an incident in a manner that allows for a comprehensive understanding and assessment.

Mitigation Measures for Privacy Incidents

49. NSIRA found that the mitigation actions of are focused on stopping the continued potential harm after an incident was discovered. For some types of incidents, such as those where information never left the control of CSE, forward-focused actions are sufficient to limit the harm. For incidents where data containing Canadian Identity Information (CII) was incorrectly shared, or SIGINT products were created resulting from the inadvertent targeting of a Canadian and inadvertently include unsuppressed CII, CSE will cancel or delete the information. Normally, CSE will cancel or delete the information without examining how, if at all, this information was used before it was cancelled.

---

[21] Incident

[22] This questionnaire is included in the *Incident Handling Guide*, and was developed to ensure that document all details of the incident in cases when the incident is escalated to senior management.

50. While it is standard practice for to request viewership logs for cancelled reports resulting in a privacy incident, does not routinely examine who might have viewed a report prior to its cancellation. CSE is able to verify user logs to check who has accessed information with a privacy interest via . For some incidents, verified who viewed reports prior to their cancellation to ascertain the extent to which information was accessed.[23] However, this was not done in all incidents where a report inadvertently contained unsuppressed CII. This is problematic as report viewership may be essential to understanding the extent to which an individual's privacy might have been impacted. Moreover, CSE generally does not examine whether the information with a Canadian privacy interest may exist in some other format, such as through a printed-paper copy of the report.

51. When a SIGINT product with a Canadian privacy interest is inadvertently released via , the SIGINT report is cancelled or reissued as mitigation actions to ensure that CII is appropriately suppressed. The cancellation ensures that the report is automatically purged from systems, thereby preventing any future use of the information. The report author's supervisor is responsible for following up to ensure the information was removed from all holdings. All users are notified when a CSE or Second Party report they have viewed is cancelled or corrected, and includes a direction to destroy copies and any information derived from the report. The cancellation of the report also stops further use or dissemination of the report, since there is no longer a report to reference on .[24]

52. Cancelling a SIGINT product, in NSIRA's opinion, is insufficient to mitigate the potential harm arising from inadvertently including Canadian information within a report. While the potential harm is limited from the moment the report is cancelled, information with a Canadian privacy interest might still have been used prior to the product's cancellation. For example, under CSE policy SIGINT clients are allowed to use SIGINT information for research and lead purposes within their department. SIGINT clients may also make a request to CSE to use the information for other purposes by making an action-on[25] or sanitization request.[26]

53. However, CSE does not inquire whether there was an action-on or sanitization request of a report containing information with a Canadian privacy interest and CSE does not contact the clients who viewed the reports to confirm whether they would have used those reports for lead purposes.[27] Action-on and sanitization requests might indicate whether information with a Canadian privacy interest that was inadvertently collected or shared was acted on, which would increase the likelihood that potential harm might have occurred to the individual. The impact of the privacy incident, including

---

[23] For example,) where : prior to its cancellation.
[24] CSE response to RFI-6, question 20(4), received by NSIRA on October 16, 2019.
[25] Action-on is any action, or decision to act, taken on the basis of SIGINT information.
[26] Sanitization is the process of editing or otherwise distinguishing SI material to protect sensitive sources, methods techniques or other sensitive characteristics of the data, and proving plausible cover. The aim of sanitization is to permit wider dissemination of information outside of SI channels.
[27] CSE response to RFI-8, question 2(b), received by NSIRA on October 18, 2019.

an assessment of the potential for harm, is not thoroughly assessed since CSE does not examine who accessed the information and what they did with it.

54. NSIRA suggests that for all privacy incidents where a report was issued, CSE should routinely verify who viewed the reports and whether any sanitization or action-on requests were made. If action-on or sanitization requests were made, CSE should follow-up with the requesting organization to ensure that the privacy impact to the individual is properly assessed and to mitigate accordingly. If CSE is able to confirm that the report was accessed, but no action-on or sanitization request was made, CSE should perform a risk assessment to determine whether contacting those who viewed the report is required in order to determine whether the information was used and whether there is an impact to the affected individual. The risk assessment should consider the type of information inadvertently shared, who accessed the information, and any other relevant information.

55. In some cases, information with a Canadian privacy interest exists, or might exist, beyond SIGINT channels where cancellation is not possible. For example, one privacy incident involved CSE cancelled the report, which automatically made the report inaccessible . However, hard or soft copies of reports can be made prior to a report's cancellation. This is reflected in the cancellation notice of reports that viewers receive, which instructs the reader to purge any soft or hard copies of the cancelled report.[28] For this incident, CSE did not contact to ensure that the incorrectly disseminated report was purged from all of their systems, and not just the reporting repositories.[29]

56. It is possible that information with a Canadian privacy interest continues to exist outside of , and that cancelling the report does not entirely delete the information with a Canadian privacy interest. For privacy incidents where a product with a Canadian privacy interest was created and released via ,[30] CSE should have examined report viewership and whether an action-on or sanitization request was made. This information would indicate the extent of potential to harm individuals affected by the privacy incident, and possibly indicate a need for further corrective action beyond cancelling a report.

57. For some incidents in the PIF, CSE was aware of who had viewed information with a Canadian privacy interest, but did not follow up with these individuals. CSE maintains that the cancellation of reports on provides the necessary protections by preventing any further disclosure of information and any activities from

[28] CSE response to RFI-6, question 2(d), received by NSIRA on October 28, 2019.
[29] CSE response to RFI-6, question 2(c), received by NSIRA on October 28, 2019.
[30] Incidents:

being further directed at the entity in question. did not consistently confirm with unauthorized viewers that the information was not used, retained, or further disseminated. For incidents, CSE was not able to confirm or provide evidence that an external party deleted the information with a Canadian privacy interest.[31] At the time of this review, it is still unclear the extent to which this information was used or retained.

58. For different incidents, the passage of time between the occurrence of an incident and its discovery was used as a justification for not verifying the incident's impacts or fully mitigating any potential harm.[32] CSE considered the passage of time as one consideration taken into account when deciding on the most effective way to mitigate the privacy impact on an individual.[33]

59. CSE should mitigate the impacts of an incident for which it is responsible. There is no connection between the passage of time and a reduced likelihood that the information was retained or further used. Accordingly, CSE's obligation to inquire as to whether information with a privacy interest was used or retained does not expire based on the time that has elapsed between the occurrence of an incident and its discovery.

60. For privacy incidents under the Cyber Security Mandate,[34] CSE was aware of who accessed the information with a Canadian privacy interest but assumed that their recollection of the data would be unreliable due to the passage of time.
data containing CII was copied to an internal platform available to all individuals at CSE. Through the program's viewer logs, examined which individuals accessed this information without the proper authorization do to so. did not contact these individuals to ensure that the information was not used or retained. Due to the time that had elapsed between the incident discovery and date of last access of the information, assessed that individuals would be unlikely to recall the incident and therefore their attestation as to whether they had used or recorded any of the information would be unreliable.[35]

61. NSIRA disagrees with CSE's justification for not inquiring whether information with a Canadian privacy interest was used or retained in incidents with a gap in time between the occurrence of an incident and its discovery. The assumption that the

---

[31] Incidents CSE response to RFI-6, question 16, received by NSIRA on October 30, 2019.
[32] Incidents
[33] CSE response to RFI-6, question 7(a), received by NSIRA on October 28, 2019. , CII was mistakenly sent to the , but was not retracted. Since the CII was disclosed at least six months prior to the discovery of , a decision was made that any use of the information (subject to caveats) would have already been made. NSIRA notes that CSE did reconsider this decision not to reach out after OCSEC's Annual Review of Disclosures of Canadian Identity Information 2017-2018. On July 25, 2019, CSE requested a retraction of the erroneously shared information, which was confirmed by on July 30, 2019.
[34] Incidents
[35] CSE response to RFI-3, question 38, received by NSIRA on October 15, 2019. CSE response to RFI-6 questions 8 and 12, received by NSIRA on October 30, 2019.

answers of individuals would be unreliable does not remove CSE's obligation to inquire about the possibility. Likewise, the assumption does not address the concern that these individuals might have retained the information with a Canadian privacy interest.

62. **Finding no. 4: CSE's mitigation measures for some privacy incidents focus only on deleting information with a privacy interest after an incident is discovered and do not examine how the information may have been used or extracted prior to its deletion.**

Recommendation no. 3: CSE should always examine what may have already been done with the information with a Canadian privacy interest in order to determine if further mitigation measures are warranted in the circumstances of a specific privacy incident.

CSE's Assessment of Whether an Incident Constitutes a Material Privacy Breach

63. As per the Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Practices*, CSE must report whether a material privacy breach occurred. According to CSE, an agreement was reached in 2016, for a bifurcated reporting structure that would lead to any privacy breaches related to operationally-sensitive activities being reported to OCSEC, while any significant (including material) privacy issues would be reported to the Office of the Privacy Commissioner (OPC).[36] NSIRA will explore options of following-up with the OPC regarding the 2016 agreement with OCSEC.

64. In TBS guidelines, a material privacy breach occurs if an incident:

- 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.[37]

65. For the period under review, CSE did not report any material privacy breaches.[38] Moreover, to date, CSE has not determined any privacy incident to be material.[39]

66. According to CSE, all determinations of a material privacy breach are done in accordance with TBS guidelines.[40] The group is responsible for assessing whether a privacy incident constitutes a material privacy breach once the incident is sent to for data entry into the PIF. An assessment for

[36] Letter from Secretary of Treasury Board to Chief of Communication Security Establishment on January 27, 2016.
[37] See www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/breach-management/material-privacy-breaches.html.
[38] CSE response to RFI-3 question 1, received by NSIRA on October 4, 2019.
[39] CSE response to RFI-6 question 22.1, received by NSIRA on October 16, 2019.
[40] CSE response to RFI-3 question 1, received by NSIRA on October 4, 2019.

potential material privacy breach is to occur following every CSE privacy incident.[41]

67. However, there are conflicting accounts concerning how CSE applies TBS guidelines to assess an incident. In a response to a RFI sent to NSIRA on October 16, 2019, it was explained to NSIRA that in order to apply the TBS guidelines to an incident, would assess whether sensitive personal information was involved in the incident.[42] will then assess whether serious injury came to the individual, however CSE assesses that serious injury is highly unlikely given the classified channels in which each incident occurs.[43]

68. CSE's draft *Standard Operational Procedure 4: Handling Privacy Incidents* (SOP) further outlines the process for how the analyst must assess an incident to determine if a material privacy breach occurred. This SOP remains a draft document, however it was explained that the procedures outlined in this document are representative of how the PIF was managed during the period of review.[44] As per section 3.4 of the SOP, upon notification of a privacy incident, the analyst will assess if sensitive personal information is involved. If so, the analyst will check databases to determine if any action-on request were processed relating to this sensitive information. If action-on requests were processed, the analyst will assess if serious harm to the individual occurred. This differs from the above analysis, as the SOP requires a determination of how sensitive information was used. Furthermore, the SOP process does not assume that serious injury is unlikely.

69. It is not clear which of those processes, if any, CSE applies when making a determination of whether an incident constitutes a material privacy breach. The only documentation and assessment that NSIRA could locate was a column in the PIF that indicates whether the incident was a material privacy breach with a yes or no response. NSIRA found no indication of an analysis of the sensitivity of information or a consideration of whether serious harm occurred to the individual. Likewise, NSIRA did not come across any documentation or evidence that analysts assessed whether there were any action-on requests for the incidents in question. In privacy incidents included in the PIF,[45] checking to see if an action-on request was processed would have been appropriate in order to assess for a material privacy breach.

70. NSIRA suggests that that the assessment for injury or serious harm to the individual should not be based on whether an action-on request was processed. Action-on requests require SIGINT information, which excludes this analysis from occurring in incidents where no SIGINT product was created, such as incidents under the cyber security mandate. Incidents without SIGINT products may contain personal information

---

[41] CSE response to RFI-6 question 21(1), received by NSIRA on October 16, 2019.
[42] CSE response to RFI-6 question 21(1), received by NSIRA on October 16, 2019.
[43] CSE response to RFI-6 question 21(1), received by NSIRA on October 16, 2019.
[44] CSE email to NSIRA Researcher, September 23, 2019.
[45] Incidents:

that has potential for serious injury or harm to the individual. Without examining how all-sensitive personal information was used outside of SIGINT channels, CSE cannot accurately assess whether serious harm occurred. To ensure an accurate determination of whether a material privacy breach occurred, the analysis of serious harm or injury to the individual should not only be determined by action-on requests.

71. **Finding no. 5: CSE does not sufficiently assess whether an incident constitutes a material privacy breach.**

Recommendation no. 4: CSE should standardize the policy on how to assess whether a privacy incident constituted a material privacy breach. Furthermore, after an assessment of sensitive personal information occurs, CSE should develop methods for analyzing whether serious harm or injury has occurred that is not triggered solely on whether an action-on request was processed.

as a Mitigation Method

72. As per the MPS

as a mitigation measure or person in Canada, a is defined in section 33.4.1(d) of the MPS:

>] is granted when correcting, cancelling or reissuing reports may draw unwanted attention to the inadvertently identified Canadian or person in Canada. Approvals eliminate the need to correct, cancel or reuse reports in which a Canadian or person in Canada was inadvertently identified... does not extend to future reporting. No subsequent reporting unsuppressed.

73. When a Canadian or person in Canada has been inadvertently named in a SIGINT report, CSE calls this a "naming incident". While there are specific circumstances under the former *National Defence Act* and the current *CSE Act* where a Canadian or a person in Canada is authorized to be named,[46] a naming incident refers to situations outside these specific circumstances. CSE was not able to provide the legal basis or authority, other than CSE internal policy, for using as a mitigating technique in privacy incidents.[47]

---

[46] Information about Canadians or persons in Canada may only be included in SIGINT reports if the information is Foreign Intelligence as defined in the NDA; the information is essential to protect the lives or safety of individuals or any nationality; or the information pertains to serious criminal activity relating to the security of Canada. CSE is also authorized to disclose CII if it concludes that doing is necessary to international affairs, defence, security or cybersecurity and if the recipient has both the authority and operational justification to receive the information (Section 44, *CSE Act*).

[47] CSE response to RFI-6, question 4(b), received by NSIRA on October 28, 2019.

74. During the review period, as a mitigating measure for incidents included in the SPIF, was granted by CSE to to name a Canadian in [48]

75. The CSE practice of was developed to respond to cases where Canadians or persons in Canada were inadvertently named without any authority and were named in . CSE considers the process of to be a mitigating measure because, in their view, would draw unwanted attention to the named individual. While this may be a valid policy consideration, it can not be used as sufficient authorization to name a Canadian or a person in Canada in a SIGINT report. The internal policy on specifies that does not authorize any future naming. Rather, the approval serves only to that contained the inadvertent naming.

76. Further, given that some of these incidents may involve the inadvertent naming of a Canadian, it is concerning to NSIRA that this process does not appear to meet Ministerial Authorization criteria that requires satisfactory measures be put in place to protect the privacy of Canadians to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.[49] The practice does not seem to perform any assessment with regard to whether retaining or releasing the information itself is essential to international affairs, defence or security. Naming a Canadian or a person in Canada in a SIGINT report has the potential to engage section 8 of the *Charter*. The practice of does not appear to consider whether, despite the information already being in the possession of the government, the individual has any "residual" privacy interest in relation to such information and its treatment by the government.[50]

77. Moreover, NSIRA finds that describing the process as a mitigation measure is misleading, as the process does remedy the problem caused by the inadvertently released information. There is no evidentiary basis to support the conclusion that would draw unwanted attention to the individual and be more harmful than Canadian or person in Canada Nor is it apparent why reports would draw unwanted attention to the inadvertent naming, versus a lower number of reports.

78. NSIRA also finds that there is no persuasive connection between the quantity of reports that contain an inadvertent naming and the justification for of the person. It is difficult to reconcile that an individual who is named in would see his name from all reporting (or the

[48] Incidents .

[49] Although the Five Eyes agencies respect each other's laws and policies, they are not accountable to conduct their activities in accordance with CSE's MAs.

[50] The Supreme Court of Canada in *R v. Wakeling,* found, for example, that there is a residual, albeit diminished, expectation of privacy in wiretap information after it has been lawfully collected. *Wakeling v. United States of America,* 2014 SCC 72.

reports in their entirety be cancelled) but an individual who is named in may see his name remain in an accessible report.

79. **Finding no. 6: is not an appropriate method to mitigate the impact and risk to privacy in cases of inadvertent naming.**

Recommendation no. 5: CSE should rescind the practice of Should it continue to use as a mitigation measure, CSE should obtain a legal opinion on the lawfulness of the practice.

VI CONCLUSION

80. The review of the PIF is the first ever review of CSE by NSIRA since the coming into force of the *NSIRA Act* in 2019. As numerous challenges resulted in a narrowed scope of review, NSIRA will examine CSE's handling of privacy incidents and strategic actions for reducing their occurrence in future reviews.

81. Overall, NSIRA commends CSE's timely response to reporting and mitigating privacy incidents. However, CSE should take additional measures to ensure that the impacts of privacy incidents are thoroughly assessed, mitigated and documented. NSIRA urges CSE to rescind the practice of , especially due to its potential to engage section 8 of the *Charter*.

82. Building on the foundation of this review, NSIRA looks forward to working with CSE to expand our knowledge and understanding of CSE's mission and challenges. Importantly, NSIRA intends to coordinate its activities with those of the Privacy Commissioner to determine the reporting process for future privacy incidents at CSE, including incidents that constitute a material privacy breach.

ANNEX A: Objectives

The objectives of this review were to assess and evaluate:

- CSE's policies and procedures on assessing whether incidents constituted a material privacy breach;[51]
- CSE's methodology for identifying and categorizing privacy incidents and procedural errors;[52] and
- The extent to which CSE's policies and procedures mitigate the impacts of privacy incidents and procedural errors.

The review of the PIF is also an opportunity for NSIRA to identify trends or systemic weaknesses that might suggest a need for corrective action, changes to CSE's procedures or policies, or an in-depth review of a specific incident or activity. This review was conducted during the first three months of the inception of NSIRA. Technological challenges, including impediments to document access, and a condensed time-period to conduct the assessment, resulted in a narrowed scale of review. As a result, an analysis to identify trends or systemic weaknesses was not possible. However, this will be a priority in future NSIRA reviews.

[51] Treasury Board Secretariat's *Guidelines for Privacy Breaches* defines a privacy breach as material if the breach 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.
[52] The previous PIF review (2017–2018) by the Office of the Communications Security Establishment Commissioner encouraged CSE to standardize its methodology for logging PIF, SPIF, and MPEF entries.

ANNEX B: Scope and Methodology

This review examined a selected sample of incidents reported in the PIF, SPIF, and MPEF for the period of July 1, 2018 to July 31, 2019. Of the 123 incidents included in the PIF for the period of review, NSIRA researchers requested additional information for 72 incidents. NSIRA researchers examined written and electronic records, files, correspondence, and other documentation, such as policies, procedures and any legal advice relevant to the selected sample of incidents.

While traditionally, the annual review of the PIF encompasses a period of 12 months, this review period was 13 months to account for the coming into force of the *CSE Act* on August 1, 2019. It is important to note that this scope refers to the date that incidents were reported for inclusion in the PIF, and not the dates on which incidents occurred.

NSIRA researchers submitted eight requests for information to CSE from August 7 to October 16, 2019. Responses were received by NSIRA from August 23 to October 31, 2019. Five briefings and information sessions were organized by CSE for NSIRA. Dates and topics are listed in Annex D. Additionally, informal meetings were held with NSIRA researchers' counterparts at CSE to discuss the status of the review and to clarify information and document requests.

Researchers also examined CSE policies, procedures, and practices relating to the reporting and associated corrective actions of privacy incidents and procedural errors. Additionally, researchers tested the information obtained against [redacted][53] and [redacted][54] for independent verification of CSE's mitigation actions. In recognition of operational impacts and time constraints, NSIRA randomly selected ten incidents for verification in CSE's targeting system.[55]

---

[53] [redacted] is a repository for SPECIAL INTELLIGENCE (SI) reports and some releasable cyber security products issued by CSE

[54] [redacted] s CSE's SIGINT targeting and selector management database.

[55] CSE email to NSIRA Researcher, received on October 21, 2019.

ANNEX C: Incident Types and Mitigation Methods

Privacy incidents can be categorized into the following types of incidents.

- **Targeting incidents** occur when CSE or a Second Party partner unknowingly targets a Canadian or person in Canada. The incident would constitute a targeting and naming incident if the information derived from the targeting were included in a report that resulted in a Canadian or person in Canada being named. In targeting incidents, the analyst must immediately de-target the selectors associated with the individual and protect the individual in If a SIGINT product was issued based on collected traffic, it must be cancelled.
- **Naming incidents** involve CSE unknowingly naming a Canadian or person in Canada, or any of their associated selectors, in a SIGINT Product, however the individual was not directly targeted. The SIGINT product must be cancelled or corrected, as appropriate.
- **Searching incidents** involve querying selectors associated with a Canadian or person in Canada in certain databases without the knowledge that the individual was a Canadian or located in Canada. Mitigating actions involve deleting the query results or query history, and protecting the selectors in .[56]
- **Sharing incidents** involve CSE inadvertently sharing Canadian identifying information through incorrect channels or by sending the information to the wrong recipients. Mitigating actions include ensuring that all records are appropriately purged.
- **Collection incidents** concern technical errors in collection methods that accidently captured traffic associated with Canadians or persons in Canada. In these cases, the cause of the inadvertent collection must be identified and appropriately addressed.
- **Data handling and retention incidents** involve technical issues under the cybersecurity mandate, where data was accidentally made available on the unclassified side or accidentally retained for longer than allowed. Mitigation actions differ for each of these incidents, but generally involve deleting the data.

[56] Note that in some cases, the selectors must be added to and then protected, as they had not been targeted prior to the incident.

ANNEX D: Meetings and Briefings

- August 19, 2019: Briefing on the Privacy Incidents File
- October 9, 2019: Meeting with a Policy Analyst,
- October 16, 2019: Meeting with a Supervisor and an Analyst, Compliance, Security, and Risk Management
- October 23, 2019: Meeting with the Manager of the Privacy and Disclosures Team
- October 23, 2019: Demo

ANNEX E: Findings and Recommendations

Finding no. 1: For privacy incidents where a policy existed for compliance measures, CSE employed these measures in a timely manner and according to policy.

Finding no. 2: While CSE has adopted a layered approach to increasing privacy protection measures, CSE is not using the PIF, or any similar collated record of privacy incidents, to its full potential as a tool to prevent systemic incidents from re-occurring, or to identify any areas of weakness in existing policy and/or practice that may reduce the occurrence of privacy incidents.

Recommendation no. 1: CSE should look at the totality of all privacy incidents with the view to identifying systemic trends or any areas of weakness in existing policy or practices.

Finding no. 3: CSE's approach to assessing and documenting privacy incidents was inconsistent and did not meet their transparency and accountability objectives in relation to the self-reporting of privacy incidents.

Recommendation no. 2: should emulate approach to reporting on privacy incidents, so that an incident report is completed for every incident with a Canadian privacy interest.

Finding no. 4: CSE's mitigation measures for some privacy incidents focus only on deleting information with a privacy interest after an incident is discovered and do not examine how the information may have been used or extracted prior to its deletion.

Recommendation no. 3: CSE should always examine what may have already been done with the information with a Canadian privacy interest in order to determine if further mitigation measures are warranted in the circumstances of a specific privacy incident.

Finding no. 5: CSE does not sufficiently assess whether an incident constitutes a material privacy breach.

Recommendation no. 4: CSE should standardize policy on how to assess whether a privacy incident constituted a material privacy breach. Furthermore, after an assessment of sensitive personal information occurs, CSE should develop methods for analyzing whether serious harm or injury has occurred that is not triggered solely on whether an action-on request was processed.

Finding no. 6: is not an appropriate method to mitigate the impact and risk to privacy in cases of inadvertent naming.

Recommendation no. 5: CSE should rescind the practice of
Should it continue to use , as a mitigation measure, CSE should obtain a legal opinion on the lawfulness of the practice.

ANNEX F: CSE's Privacy Incidents File