

Communications Security
Establishment Commissioner



Commissaire du Centre de la
sécurité des télécommunications

The Honourable Jean - Pierre Plouffe, C.D.

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

CSE / CST Chief's Office / Bureau du chef
AVR 03 2014 APR
CERID # 10398336
ECT # 14-10090
File / Dossier

TOP SECRET // SI // CEO

Our file # 2200-83

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 disclosures by the Communications Security Establishment Canada (CSEC) of Canadian identity information (CII) from foreign signals intelligence (SIGINT) reports to Government of Canada (GC) clients, second party partners and non-five eyes recipients for the period of July 1, 2012, to June 30, 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)*.

The *NDA* and *Privacy Act* require CSEC to take measures to protect the privacy of Canadians, including personal information. CII may be included in CSEC SIGINT reports if it is essential to understanding foreign intelligence. However, with some limited exceptions that are stated in CSEC policy, any information that identifies a Canadian must be suppressed (minimized) in end-product reports — that is, replaced by a generic reference such as “a named Canadian.” When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting GC client or second party partner has both the authority and operational justification for obtaining the CII. Only then may CSEC provide the CII.

Based on the information reviewed and the interviews conducted, CSEC's disclosure of CII from SIGINT reports to GC clients, second party partners, and through GC clients and second party partners to non-five eyes recipients, complied with the law and with ministerial direction concerning the protection of the privacy of Canadians. In accordance with the *NDA* and *Privacy Act*, CSEC effectively applied satisfactory measures to protect personal information and the privacy of Canadians in its disclosures.

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

TOP SECRET // SI // CEO

CSEC confirmed that two privacy incidents occurred pertaining to two Canadians mentioned in four reports. It appears that a second party partner included CII in the SIGINT reports, that is, CII was not initially suppressed in those reports as required by CSEC and second party policies. It is possible that CII may have also been included in other related reports on the same subjects. This is not to suggest that there was any deliberate non-compliance on the part of CSEC or any of its partners. CSEC will record the incidents in its Privacy Incidents File (PIF). The Commissioner's office will examine CSEC's responses to the incidents as part of next year's annual review of a sample of disclosures or annual review of the PIF.

My office also identified and discussed with CSEC a number of minor instances where records of the disclosures were not in accordance with best practices. I will monitor these issues as part of future annual reviews of disclosures.

CSEC has comprehensive policies and procedures that guide its disclosure of CII from SIGINT reports to GC clients, and it is a positive development that CSEC is amending its policy guidance to encompass disclosures to second party partners and to non-five eyes recipients through GC clients and second party partners. CSEC employees interviewed were fully knowledgeable about and complied with the policies and procedures, and CSEC managers routinely and closely monitored disclosures to ensure compliance and privacy protection.

It is also a positive development that CSEC continues to give priority to the completion of the full automation of its process for the disclosure of CII from SIGINT reports and that it plans to include second party partners in its automated systems.

I intend to continue to conduct an annual review of CSEC's disclosures of CII from SIGINT reports to GC clients, second party partners and non-five eyes recipients. I will monitor developments with regard to the findings 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 the enclosed report.

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

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'J. Plouffe', with a stylized flourish at the end.

Jean-Pierre Plouffe

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

Enclosure

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 # 2200-83

**Annual Review of Disclosures by the
Communications Security Establishment Canada
of Canadian Identity Information from
Foreign Signals Intelligence Reports to
Government of Canada Clients,
Second Party Partners and Non-Five Eyes Recipients**

March 31, 2014

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

TABLE OF CONTENTS

I. AUTHORITIES.....	1
II. INTRODUCTION.....	1
Rationale for conducting this review.....	1
III. OBJECTIVE.....	2
IV. SCOPE.....	2
V. CRITERIA.....	2
VI. METHODOLOGY.....	3
VII.BACKGROUND.....	3
Overview of the release process.....	3
[REDACTED] on-line request system for GC clients.....	4
[REDACTED].....	4
GC clients.....	5
Second party partners.....	5
Non-five eyes recipients.....	6
Denials.....	7
VIII.FINDINGS.....	7
Compliance with the law.....	7
Potential privacy incidents.....	9
Ministerial requirements.....	9
Policies and procedures.....	10
IX. CONCLUSION.....	13
ANNEX A — Findings.....	15
ANNEX B — Interviewees.....	16
ANNEX C — Request for Release of Suppressed Information.....	17
ANNEX D — Metrics for GC Agencies.....	21
ANNEX E — Disclosure of CII in SIGINT Infographic.....	22

I. AUTHORITIES

This report was prepared on behalf of the Communications Security Establishment Commissioner under his authority as articulated in Part V.1, paragraph 273.62(2)(a) of the *National Defence Act* (NDA).

II. INTRODUCTION

The *NDA* and *Privacy Act* require Communications Security Establishment Canada (CSEC) to take measures to protect the privacy of Canadians, including personal information. Canadian identity information (CII) may be included in CSEC signals intelligence (SIGINT) reports if it is essential to understanding foreign intelligence. However, with some limited exceptions that are stated in CSEC policy, any information that identifies a Canadian must be suppressed (minimized) in end-product reports — that is, replaced by a generic reference such as “a named Canadian.” When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting Government of Canada (GC) client or second party partner¹ has both the authority and operational justification for obtaining the CII. Only then may CSEC provide the CII. GC and second party partners may request action-on for sharing CII outside the Five Eyes, that is, with non-five eyes recipients. In addition to these requirements, disclosures to non-five eyes recipients [REDACTED] may be subject to a mistreatment risk assessment (MRA).²

This is the first year that this particular annual review included examination of a sample of CSEC disclosures of CII from SIGINT reports to second party partners and to non-five eyes recipients.

Rationale for conducting this review

Since 2008, commissioners have regularly reviewed CSEC disclosures of CII from SIGINT reports.³ Commissioners have found the results of these reviews positive:

- CSEC disclosures of CII to GC clients complied with the law;
- policies and procedures were in place and provided sufficient direction to CSEC employees on the protection of the privacy of Canadians;

¹ The Second Parties are CSEC’s four SIGINT partners: the United States’ National Security Agency (NSA), the United Kingdom’s Government Communications Headquarters (GCHQ), the Australian Signals Directorate (ASD), and the New Zealand Government Communications Security Bureau (GCSB). Collectively with CSEC, the Second Parties are referred to as the Five Eyes.

² An MRA is an assessment of the risk of mistreatment to any individual when sharing information with a non-five eyes partner (see p. 6 for more detail on MRAs).

³ The Commissioners’ disclosure review reports of November 19, 2008, February 16, 2010, February 21, 2011, March 13, 2012, and March 18, 2013, provide detailed background information on CSEC disclosures of CII from SIGINT reports.

- CSEC employees were knowledgeable about, and acted in accordance with, the policies and procedures; and
- CSEC managers monitored these activities to ensure CSEC employees complied with governing authorities.

However, should there be an instance of non-compliance while CSEC discloses CII, the potential impact on the privacy of Canadians could be significant. The sharing of CII by CSEC with its second party partners and non-five eyes recipients has the potential to directly affect the privacy and security of a Canadian. The Commissioner therefore conducts an annual review of disclosures of CII to verify that CSEC continues to comply with the law and effectively applies satisfactory measures to protect the privacy of Canadians.

III. OBJECTIVE

The objective of this review was to verify that, in disclosing CII from SIGINT reports, CSEC complied with the law, ministerial direction, and its operational policies and procedures, and that CSEC protected the privacy of Canadians.

IV. SCOPE

The review encompassed a sample of requests from GC clients and subsequent CSEC disclosures of CII from SIGINT reports, and all requests and subsequent disclosures of CII to second party partners and non-five eyes recipients for the period of July 1, 2012, to June 30, 2013.

The Commissioner's office also examined changes to CSEC policies and practices related to the disclosure of CII from SIGINT reports.

V. CRITERIA

The Commissioner expected that CSEC's disclosures of CII from SIGINT reports to GC clients, second party partners and non-five eyes recipients was conducted in accordance with legal requirements in the *NDA* and *Privacy Act*, with ministerial direction concerning the protection of the privacy of Canadians, and with relevant CSEC policies and procedures, and that CSEC managers monitored the activities to ensure compliance with governing authorities.

VI. METHODOLOGY

The Commissioner's office selected and examined a sample that represented approximately 20% of disclosure request forms and e-mails (408 of 1,968 forms) received by CSEC from all GC clients and second party partners during the period under review, associated SIGINT end-product reports, and any associated disclosures of CII. In total, the Commissioner's office examined approximately 10,000 pages of written and on-line materials.

As it was the first year that this review included disclosures to second party partners and non-five eyes recipients, the Commissioner's office examined all of these disclosures during the period under review (170 disclosures to second party partners and eight disclosures to non-five eyes recipients through GC clients and second party partners).

The Commissioner's office selected and examined approximately 13% (230 of 1,790) of the requests from GC clients, including all requests from client departments that submit requests infrequently. The Commissioner's office also conducted interviews with managers and employees involved in the disclosure of CII from SIGINT reports, including to determine their level of knowledge of applicable policies and procedures. (Annex B is a list of interviewees).

VII. BACKGROUND

Overview of the release process

According to CSEC policy OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports* (revised effective May 8, 2008), all personal or identifying information of a Canadian or allied entity must be suppressed and replaced with a generic identifier in CSEC reports.

If a client or partner believes that it has the authority to receive and an operational need to know the CII, it forwards a *Request for Release of Suppressed Information* form, an automated request in CSEC's [REDACTED] or [REDACTED] on-line request systems (Annex C is a copy of the form and screenshots of [REDACTED] and [REDACTED] or an e-mail request to CSEC's Corporate and Operational Policy section (D2), which is responsible for receiving such requests and for the disclosure of CII from SIGINT reports, if appropriate.

Additionally, a CSEC Client Relations Officer (CRO) may advance the release of CII to a GC client.⁴ In such cases, the CRO is delegated responsibility and is accountable for any release of CII.

⁴ CROs may respond to a client request for the disclosure of CII from a SIGINT report. A CRO may also proactively disclose CII from a SIGINT report, for example: in anticipation of such a request from a senior GC client (like a Minister, Deputy Minister or Ambassador); in an urgent or emergency situation; or if access to a client is difficult or his/her schedule does not permit frequent meetings.

CSEC policy OPS-1-1 also requires that disclosures of CII from SIGINT reports to GC clients and to second party partners include the following caveat respecting “action-on”⁵ and use by the requesting client:

No further action may be taken with regards to this information without the prior approval of CSEC/[Corporate and] Operational Policy. CSEC requests that the Canadian identity information be protected in accordance with SIGINT community’s procedures for the handling allied national identities. Furthermore, this information may not be used in affidavits, court proceedings, or for any other legal or judicial purposes without the prior approval of the Chief, CSEC. Questions should be directed to CSEC/[Corporate and] Operational Policy ([REDACTED]@cse-cst.gc.ca).

[REDACTED] on-line request system for GC clients

[REDACTED] is CSEC’s automated on-line request system for requests and disclosure of CII from SIGINT reports to GC clients. In his February 2010, report on this subject, Commissioner Cory recommended that CSEC “give priority to the development of the automated tools necessary to enable it to accurately and consistently account for and report on the release of all [CII].”

According to CSEC, [REDACTED] was intended to enhance accounting and retrieval of identity release history and to improve the timeliness of responses to clients, consistent with OPS-1-1. Some improvements include: a centralized system for all CII requests; the ability to track requests through the approval process more effectively and efficiently; an automated workflow process for employees and management; and the ability to generate reports for tracking, management, and review purposes. From July 2012 to December 2012, clients from the Canada Border Services Agency (CBSA), the Royal Canadian Mounted Police (RCMP) and CSIS were pilot users of [REDACTED]. By the spring of 2013, CSEC had phased out the old paper-based system of using Microsoft Word forms to request CII, with some exceptions such as for urgent requests, during system outages and for clients that did not yet have a [REDACTED] account.

[REDACTED]

[REDACTED] is a tool and database used by CSEC’s [REDACTED] team, which provides foreign intelligence on [REDACTED] cyber threats. [REDACTED] includes an automated function that, like [REDACTED] is being used for disclosure of CII suppressed in cyber reports, consistent with OPS-1-1. Between mid-June and mid-July 2013, CSEC conducted testing with CSIS on the use of [REDACTED] therefore, only a handful of such disclosure requests were captured as part of this review. [REDACTED] is capable of producing metrics on these disclosures.

⁵ According to OPS-1-1, “action-on” is any action, or decision to act, taken on the basis of COMINT information, which might jeopardize the COMINT source. Action-on usually involves sanitization to disguise COMINT and conceal its source, permitting wider dissemination outside COMINT channels.

GC clients

From July 1, 2012, to June 30, 2013, the majority of requests for the disclosure of CII from SIGINT reports by GC clients were requested by CSIS [REDACTED] CBSA [REDACTED] the RCMP [REDACTED] and to other CSEC employees [REDACTED]

Number of Requests for Disclosures of CII by GC Clients — July 1, 2012, to June 30, 2013



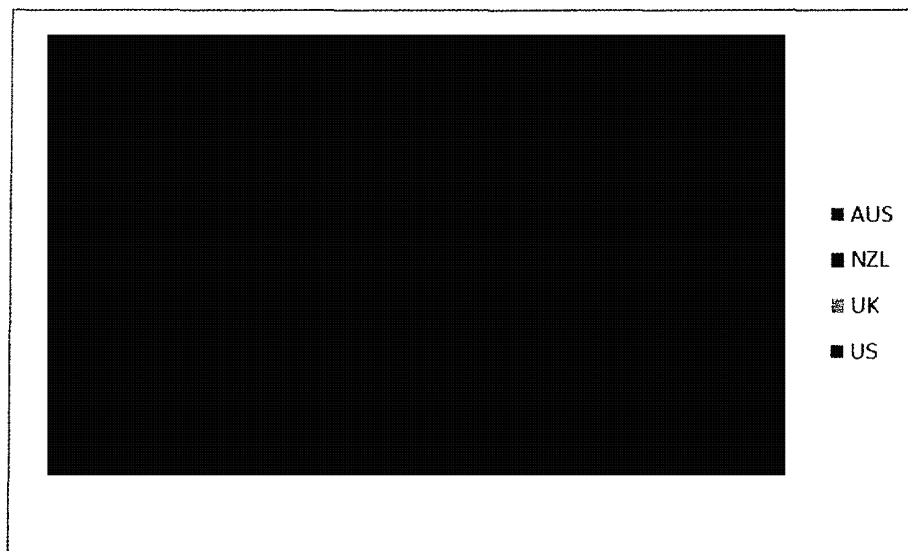
Second party partners

[REDACTED]

[REDACTED] Such requests are handled in the same manner as requests by GC clients; however, the process for second party partners is not yet automated on [REDACTED] and requests are currently submitted by e-mail to D2, using the standard e-mail.

From July 1, 2012, to June 30, 2013, a large majority of requests for the disclosure of CII from second party partners was requested by the NSA [REDACTED]

Number of Requests for Disclosures of CII by Second Party Partners —
July 1, 2012, to June 30, 2013



Non-five eyes recipients

Non-five eyes recipients may receive CII through a GC client or second party partner. That is, GC or second party partners may request action-on or sanitize information for sharing with non-five eyes recipients. The Ministerial Directive on *Framework for Addressing Risks in Sharing Information with Foreign Entities* (effective November 21, 2012) requires CSEC to consider the risk that sharing information [REDACTED] may result in the mistreatment of an individual. It is CSEC's responsibility to conduct an MRA when the request originates from a second party partner, for example, [REDACTED]

This process applies regardless of the nationality of the individual whose personal

information is being shared; it is based on the country with whom it is intended to be shared. CSEC relies on open source information, SIGINT, Department of Foreign Affairs, Trade and Development analysis and may include other classified information such as CSIS Arrangement Profiles, when available, to complete its assessment of the non-five eyes partner's human rights record. If a GC client wants to disclose CII suppressed in a CSEC report with a non-five eyes partner, it is the GC client's responsibility to conduct the MRA. This year, CSEC disclosed CII from SIGINT reports to GC clients and second party partners, who subsequently shared the information with the following non-five eyes recipients: [REDACTED]
[REDACTED]

Denials

In the sample selected by the Commissioner's office, CSEC denied over a [REDACTED] of GC requests for the disclosure of CII from SIGINT reports, [REDACTED] of second party requests, and [REDACTED] requests to disclose CII [REDACTED]
[REDACTED]

VIII. FINDINGS

Compliance with the law

Finding no. 1: Compliance with the Law

Based on the information reviewed and the interviews conducted, CSEC's disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients complied with the law.

In accordance with the *NDA* and *Privacy Act*, CSEC effectively applied satisfactory measures to protect personal information and the privacy of Canadians in its disclosures of CII from SIGINT reports to GC clients, second party partners and non-five eyes recipients.

The Commissioners' disclosure review reports of November 19, 2008, and February 16, 2010, provide detailed background information on the legal authorities and requirements respecting CSEC disclosures of CII from SIGINT reports. CSEC advised that it did not receive any new advice from Justice Canada related to the subject of this review.

The Commissioner's office reviewed all of the approximately [REDACTED] SIGINT reports relating to the disclosures of CII from SIGINT reports made by CSEC during the period under review. With the exception of two privacy incidents (discussed under Potential Privacy Incidents, below), in accordance with CSEC policy and the agreements in place with its second party partners, CSEC and its second party partners suppressed all personal or identifying information of a Canadian in their reports.

CSEC records of the requests by GC clients, second party partners and disclosures to non-five eyes recipients generally contained clear and comprehensive descriptions of the partners' authorities and operational justifications for obtaining the CII from CSEC SIGINT reports. The number of denials is one demonstration of the rigour and due diligence applied by CSEC in its verification that partners have and document the authority and operational justification for obtaining CII from SIGINT reports. In a number of instances, D2 requested additional information before determining whether or not to disclose the CII.

The Commissioner's office did not have concerns with any of CSEC's decisions to disclose CII from SIGINT reports to its second party partners. However, the Commissioner's office observed that CSEC records of a number of the NSA requests [REDACTED] [REDACTED] contained the same basic and general statement about the agency's authority and operational justification for obtaining the CII, regardless of the client and particular situation. Notwithstanding the records, D2 was able to provide detailed descriptions of these requests and of its assessment. Conversely, the CSEC records of requests by other Second Parties generally contained more precise justifications relating to more specific operational requirements than the NSA requests. CSEC included in all disclosures the standard caveat restricting the further dissemination of CII by the Second Parties without further approval from CSEC. The Commissioner's office will monitor this issue in future annual reviews and encourages CSEC to make certain that records of all second party requests include comprehensive information on the parties' authorities and operational justification for obtaining CII from CSEC SIGINT reports.

Although CSEC does not currently have specific written guidance on disclosure of CII from SIGINT reports to non-five eyes recipients, D2 was able to demonstrate in all cases that it applied the same rigorous process as it does for second party partners. CSEC included in all disclosures the standard caveat restricting the further dissemination of CII without further approval from CSEC.

The Commissioner's office identified and discussed with CSEC a number of minor instances where records of the disclosures were not in accordance with best practices. For example, the use by D2 of "assumption" in some of its recommendations could raise questions about whether certain disclosures were based on clear information and compelling justifications. CSEC agreed that these records could have been better. The Commissioner's office also observed gaps in the supporting documentation for some of D2's recommendations and management's decisions to approve or deny disclosures. In these cases, evidence of the final approval or denial was only found in e-mails sent by CSEC to the requesting party and saved in a shared inbox. CSEC agreed that it should develop a better way to manage this information to ensure that all decisions are properly documented. The Commissioner's office will monitor these issues as part of future annual reviews.

Potential privacy incidents

In its review of the SIGINT reports relating to the sample of disclosure requests, the Commissioner's office identified what it believed could be six or more potential privacy incidents. According to CSEC policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities* (revised effective December 1, 2012), 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 CSEC policy. CSEC confirmed that two privacy incidents occurred pertaining to two Canadians mentioned in four reports. It appears that a second party partner included CII in the SIGINT reports, that is, CII was not initially suppressed in those reports as required by CSEC and second party policies. It is possible that CII may have also been included in other related reports on the same subjects. This is not to suggest that there was any deliberate non-compliance on the part of CSEC or any of its partners. CSEC will record the incidents in its Privacy Incidents File (PIF). The Commissioner's office will examine CSEC's responses to the incidents as part of next year's annual review of a sample of disclosures or annual review of the PIF.

Ministerial requirements

Finding no. 2: Ministerial Direction

Based on the information reviewed and the interviews conducted, CSEC's disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients complied with ministerial direction concerning the protection of the privacy of Canadians.

There is no specific ministerial direction respecting the disclosure of CII from SIGINT reports and the Commissioner's office did not identify any issues that would suggest a requirement for specific ministerial direction on this subject.

All CSEC activities, including disclosures, must respect general ministerial direction concerning the protection of the privacy of Canadians set out in the ministerial directives on *Privacy of Canadians* (revised effective November 20, 2012) and on *Accountability Framework* (revised effective November 20, 2012). As noted above, CSEC effectively applied satisfactory measures to protect personal information and the privacy of Canadians in its disclosures of CII from SIGINT reports to GC clients, second party partners and non-five eyes recipients.

In addition, the Ministerial Directive on *Framework for Addressing Risks in Sharing Information with Foreign Entities* (revised effective November 21, 2011) requires CSEC to consider the risk that sharing information [REDACTED] — such as the disclosure of CII — may result in the mistreatment of an individual. The Commissioner's office had no concerns about the one instance of a disclosure to a non-five eyes recipient through a second party partner requiring CSEC to prepare an MRA. CSEC's Directorate of

Audit, Evaluation and Ethics is currently conducting an internal review of its MRA process. The Commissioner plans to conduct an in-depth review of CSEC information sharing [REDACTED]

Policies and procedures

Finding no. 3: Appropriateness of policies and procedures

CSEC has comprehensive policies and procedures that guide its disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, and it is a positive development that CSEC is amending its policy guidance to encompass disclosures to second party partners, and through Government of Canada clients and second party partners to non-five eyes recipients.

CSEC's handling of requests for the disclosure of CII from SIGINT reports is governed by a number of policies and procedures that provide detailed direction on compliance with legal requirements and ministerial direction concerning the protection of the privacy of Canadians.

The Commissioner's office examined the most recent versions of these policies and procedures:

1. OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* (revised effective December 1, 2012)

This cornerstone policy establishes baseline measures to help ensure that CSEC only undertakes activities that are within its mandate, that are consistent with legal requirements and ministerial direction, and in a way that protects the privacy of Canadians in the use and retention of information intercepted by CSEC. Detailed requirements for compliance and privacy protection are found in CSEC activity-specific policy instruments.

2. OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports* (revised effective September 28, 2012)

This is the principal and long-standing policy (CSEC promulgated the first OPS-1-1 in 2002) applicable to the activities under review. It provides direction to CSEC employees involved in requests for, disclosures of and storing of CII suppressed from SIGINT reports, including guidance on authorities, responsibilities and accountability.

It is a positive development that CSEC is in the process of updating OPS-1-1 to reflect delegated authorities for the disclosure of CII from SIGINT reports to second party partners and non-five eyes recipients (the authorities contained in the briefing note of February 13, 2013, referred to below). In addition, the new version of

OPS-1-1 will better reflect the new automated processes, that is, [REDACTED] and [REDACTED]. CSEC anticipates that the new version of OPS-1-1 will be promulgated in the first quarter of the 2014–2015 fiscal year. CSEC has also committed to update its working aid (referred to below) to include disclosures to non-five eyes recipients through GC clients and second party partners.

3. OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians* (revised effective December 5, 2012)

These procedures describe CSEC's policy compliance monitoring program, which is intended to demonstrate that CSEC activities complied with the law and protected the privacy of Canadians. Specifically, the procedures describe at a high level what SIGINT and IT Security activities must be monitored, and assign responsibility for the program's management and oversight. In January 2014, the Commissioner completed an in-depth study of this program.

4. Operational Policy Section Action Primer (procedure) related to the Suppressed Identity Requests (received by Commissioner's office September 4, 2013)

This working aid provides detailed instructions to D2 analysts on the conduct of disclosures of CII from SIGINT reports to both GC clients and second party partners. It is maintained by D2 and kept "evergreen" to reflect best practices and address any situations that may arise.

5. Briefing note for the CSEC Director General Policy and Communications on delegated authorities related to *Repetitive Release of Canadian Identities Outside Canada (Note 2)* (dated February 13, 2013)

This document explains the delegated authorities for the disclosure of CII from SIGINT reports to second party partners and non-five eyes recipients. In addition, CSEC indicated that it is currently drafting an operational policy on mistreatment risk management (OPS-6). According to CSEC, these procedures will codify the mistreatment risk assessment and approval protocols in CSEC's direct and indirect information sharing activities [REDACTED] CSEC's five-eyes partners. In response to questions of the Commissioner's office, CSEC also acknowledged that there is a need to strengthen information management practices for the handling of requests from GC and second party partners to release CII to non-five eyes recipients as part of an information sharing request. The Commissioner will examine OPS-6 as part of the planned in-depth review of CSEC information sharing with [REDACTED]

Finding no. 4: Awareness of Personnel

CSEC employees interviewed were fully knowledgeable about and complied with policies and procedures for the disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients.

The Commissioner's office's review of records and interviews demonstrated that D2 managers and employees have an acute awareness of legislative requirements, ministerial direction, and CSEC policies and procedures, and that this is top of mind in the conduct of their work. The Commissioner's office did not identify any significant instances where the actions of D2 employees were inconsistent with CSEC policy and procedures for disclosures.

Finding no. 5: Management Control Framework

CSEC managers routinely and closely monitored disclosures of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients to ensure compliance and privacy protection.

In accordance with OPS-1-8, D2 is responsible for conducting policy compliance monitoring and validation of its disclosure activities. Once a month, the Supervisor of the Privacy and Interests Protection Team in D2 reviews a sample of disclosures for compliance with policy and procedures and informs the Manager, Corporate and Operational Policy (COP) of this review. In turn, the Manager COP provides regular updates to the Director, Disclosure, Policy and Review identifying any issues of concern. D2 employees are informed of any changes to policy or process and of new or changed clients and any specific client requirements. In addition, D2 meets at least every few months to discuss any issues and best practices.

Finding no. 6: Technology

It is a positive development that CSEC continues to give priority to the completion of the full automation of its process for the disclosure of Canadian identity information from foreign signals intelligence reports and that it plans to include second party partners in its automated systems.

To date, [REDACTED] is only available for GC clients; however, CSEC indicated that automation of second party requests for the disclosure of CII in SIGINT reports is a priority. It is also a priority for CSEC to implement updates to [REDACTED] for all requests, for example: to add certain additional fields that were part of the paper form (released by, release date, previously released, approved by); enhanced search functionality; improvements to enable the production of metrics on disclosures; and removal of bugs in the system that may cause certain information to appear in the wrong fields. It is a positive development

that these updates to [REDACTED] which are important for accountability and to demonstrate compliance, appear to be proceeding on a priority basis.

IX. CONCLUSION

This review encompassed a sample of approximately 20% of requests for the disclosure of CII from SIGINT reports for the period of July 1, 2012, to June 30, 2013, including a sample of such requests and subsequent disclosures to GC partners and all requests and disclosures to second party partners and non-five eyes recipients.

Based on the information reviewed and the interviews conducted, CSEC's disclosure of CII from SIGINT reports to GC clients, second party partners, and through GC clients and second party partners to non-five eyes recipients, complied with the law and with ministerial direction concerning the protection of the privacy of Canadians. In accordance with the *NDA* and *Privacy Act*, CSEC effectively applied satisfactory measures to protect personal information and the privacy of Canadians in its disclosures.


CSEC confirmed that two privacy incidents occurred pertaining to two Canadians mentioned in four reports. It appears that a second party partner included CII in the SIGINT reports, that is, CII was not initially suppressed in those reports as required by CSEC and second party policies. It is possible that CII may have also been included in other related reports on the same subjects. This is not to suggest that there was any deliberate non-compliance on the part of CSEC or any of its partners. CSEC will record the incidents in its Privacy Incidents File (PIF). The Commissioner's office will examine any such incidents as part of next year's annual review of a sample of disclosures or annual review of the PIF.

The Commissioner's office also identified and discussed with CSEC a number of minor instances where records of the disclosures were not in accordance with best practices. The Commissioner's office will monitor these issues as part of future annual reviews.

CSEC has comprehensive policies and procedures that guide its disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, and it is a positive development that CSEC is amending its policy guidance to encompass disclosures to second party partners and to non-five eyes recipients through GC clients and second party partners.

It is also positive development that CSEC continues to give priority to the completion of the full automation of its process for the disclosure of CII from SIGINT reports and that it plans to include second party partners in its automated systems.

This review contains no recommendations. A list of findings is enclosed at Annex A.


Jean-Pierre Plouffe, Commissioner

ANNEX A — Findings

Finding no. 1: Compliance with the Law

Based on the information reviewed and the interviews conducted, CSEC's disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients complied with the law.

Finding no. 2: Ministerial Direction

Based on the information reviewed and the interviews conducted, CSEC's disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients complied with ministerial direction concerning the protection of the privacy of Canadians.

Finding no. 3: Appropriateness of policies and procedures

CSEC has comprehensive policies and procedures that guide its disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, and it is a positive development that CSEC is amending its policy guidance to encompass disclosures to second party partners, and through Government of Canada clients and second party partners to non-five eyes recipients.

Finding no. 4: Awareness of Personnel

CSEC employees interviewed were fully knowledgeable about and complied with policies and procedures for the disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients.

Finding no. 5: Management Control Framework

CSEC managers routinely and closely monitored disclosures of Canadian identity information from foreign signals intelligence reports to Government of Canada clients, second party partners and non-five eyes recipients to ensure compliance and privacy protection.

Finding no. 6: Technology

It is a positive development that CSEC continues to give priority to the completion of the full automation of its process for the disclosure of Canadian identity information from foreign signals intelligence reports and that it plans to include second party partners in its automated systems.

ANNEX B — Interviewees

The following CSEC employees provided information or facilitated the review:

Special Advisor, D2

Supervisor, D2A

Team Leader, [REDACTED]

[REDACTED] Analyst, [REDACTED]

Analyst, SIGINT Oversight and Compliance

Analyst, SIGINT Oversight and Compliance

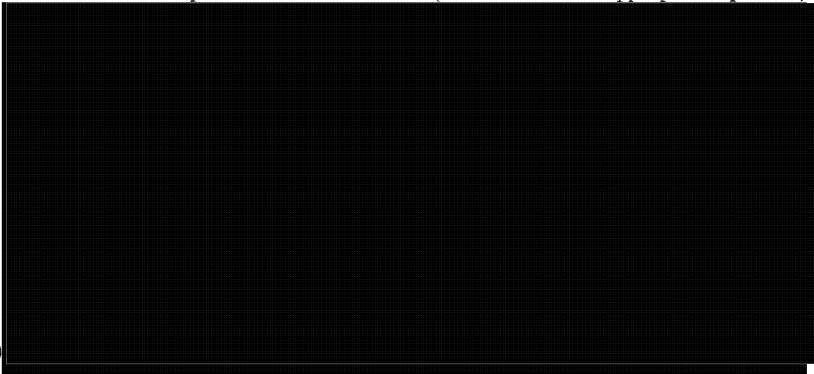
ANNEX C — Request for Release of Suppressed Information

Suppressed Identity Request Form

TOP SECRET//SI//Canadian Eyes Only

REQUEST FOR RELEASE OF SUPPRESSED INFORMATION

*Instructions: Sections A - G to be completed by Requester
Section H to be completed by CSE Operational Policy or CRO*

A. Requesting Client's Name	B. Client Title and Department
C. Report Serial Number	D. Date of Request
E. Information Requested	
F. Rationale for Request (<i>please complete all three questions</i>)	
<p>1) This information is required because it relates to (<i>mark an 'X' in the appropriate space(s)</i>):</p> <p>___ a) </p> <p>___ b)</p> <p>___ c)</p> <p>___ d)</p> <p>___ e)</p> <p>___ f)</p> <p>___ g)</p> <p>___ h)</p> <p>___ i)</p> <p>___ j)</p> <p>___ k)</p> <p>___ l)</p> <p>___ m)</p> <p>2) If the request relates to a potential or actual violation of a Canadian law, please cite the law.</p> <p>3) Explain how this information relates directly to an operating program or activity of your department.</p>	
G. Please indicate what action, if any, is being contemplated based on this information. (<i>Note that some actions require prior CSE approval.</i>)	
<p>Suppressed Information</p> <p><i>Released by:</i></p> <p><i>Reviewed by:</i></p> <p><i>Comments:</i></p> <p>This information is provided on the understanding that the requesting department requires the information to perform its lawful duties, and that this information will be handled in accordance with the <i>Access to Information</i></p>	

CERRID #

On-line Request System for GC Clients

Request Number	Date: 2/27/2014
----------------	-----------------

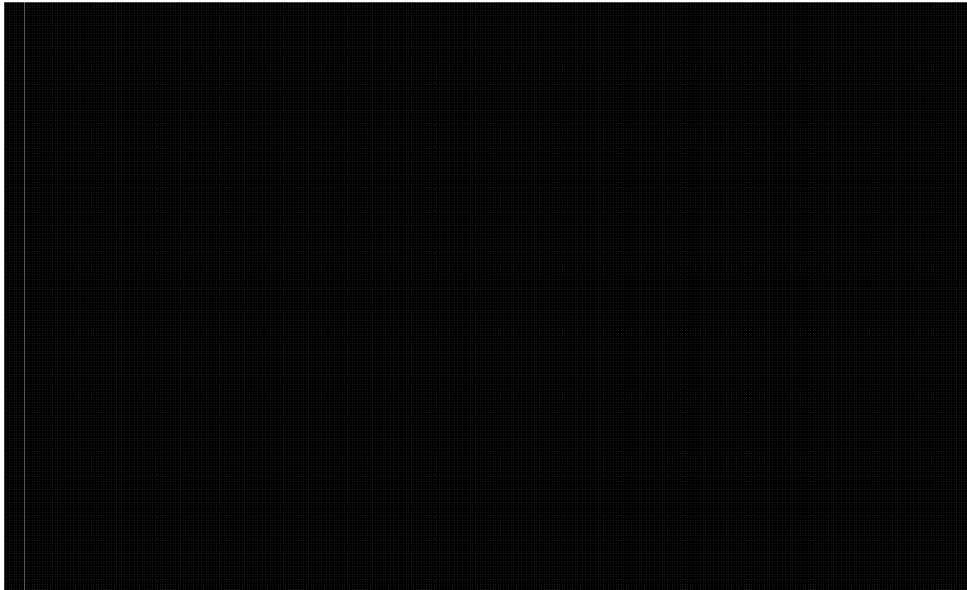
Request for Release of Suppressed Information

<u>A. Request Priority</u>	
Priority	Select... <input type="button" value="v"/>
Threat to Life?	<input type="checkbox"/>
Priority Justification	<div><div></div><div></div><div></div></div>

<u>B. Client Information</u>			
Name	<div><div></div><div></div><div></div></div>	Title	<div><div></div><div></div><div></div></div>
Department	Select... <input type="button" value="v"/>	Team	<div><div></div><div></div><div></div></div>
Email Address	<div><div></div><div></div><div></div></div>	Report Serial	<div><div></div><div></div><div></div></div>
If different from above	<div><div></div><div></div><div></div></div>	GAMMA:	<input type="checkbox"/>
Intended Recipients	<div><div></div><div></div><div></div></div>		

<u>C. Requested Suppressed Information</u>
Suppressed Alias
Please enter each alias on a separate line
<div><div></div><div></div><div></div></div>

<u>D. Request Rationale</u>
D-1. This information is required because it relates to (Check all that apply):



D-2. If the request relates to a potential or actual violation of a Canadian law or an international agreement to which a Canadian is a party, please cite it below:

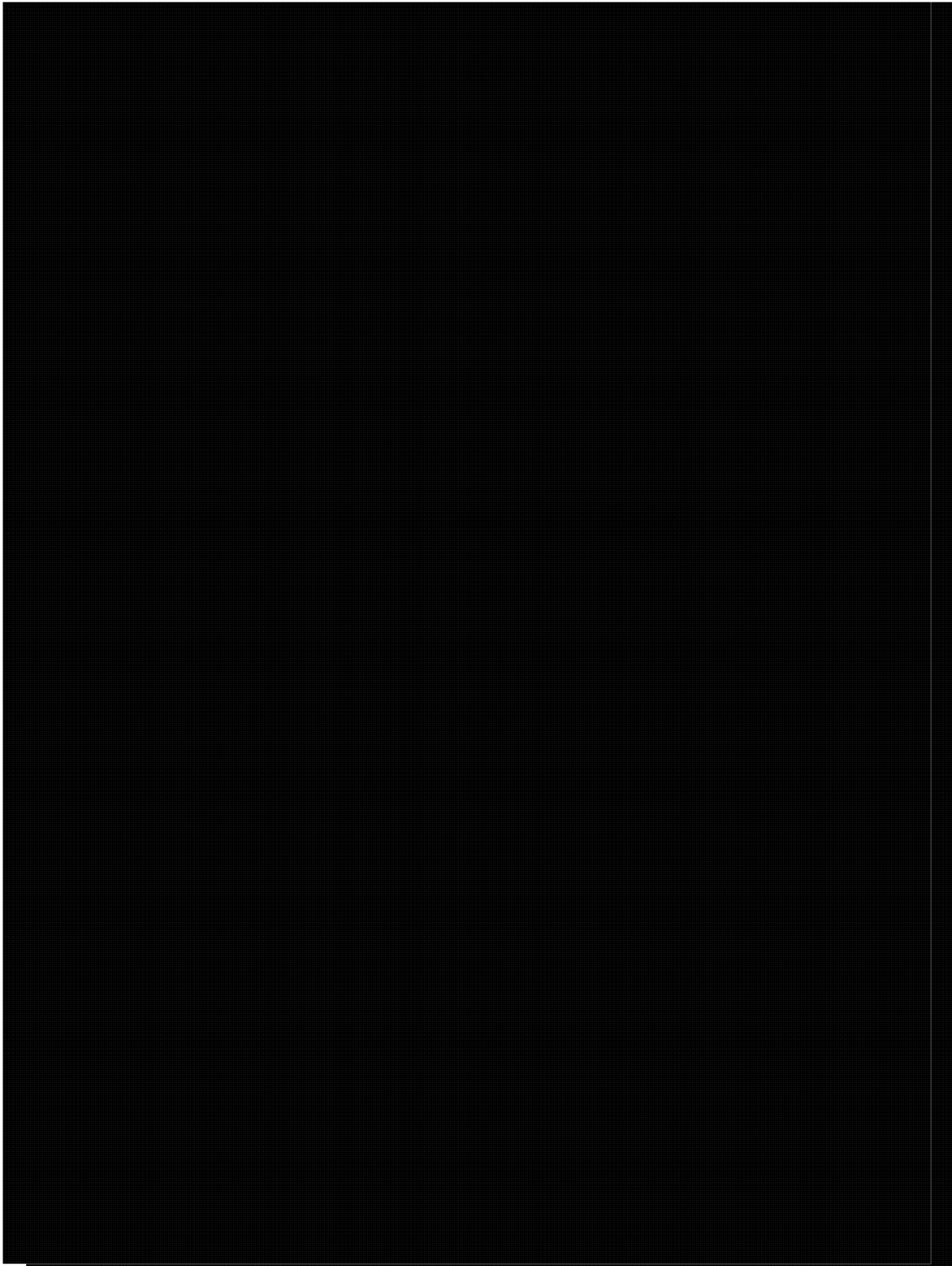
--	--

D-3. With reference to the content of the report, explain how the suppressed information will support your operating area's mandated functions:

--	--

E. Action-on

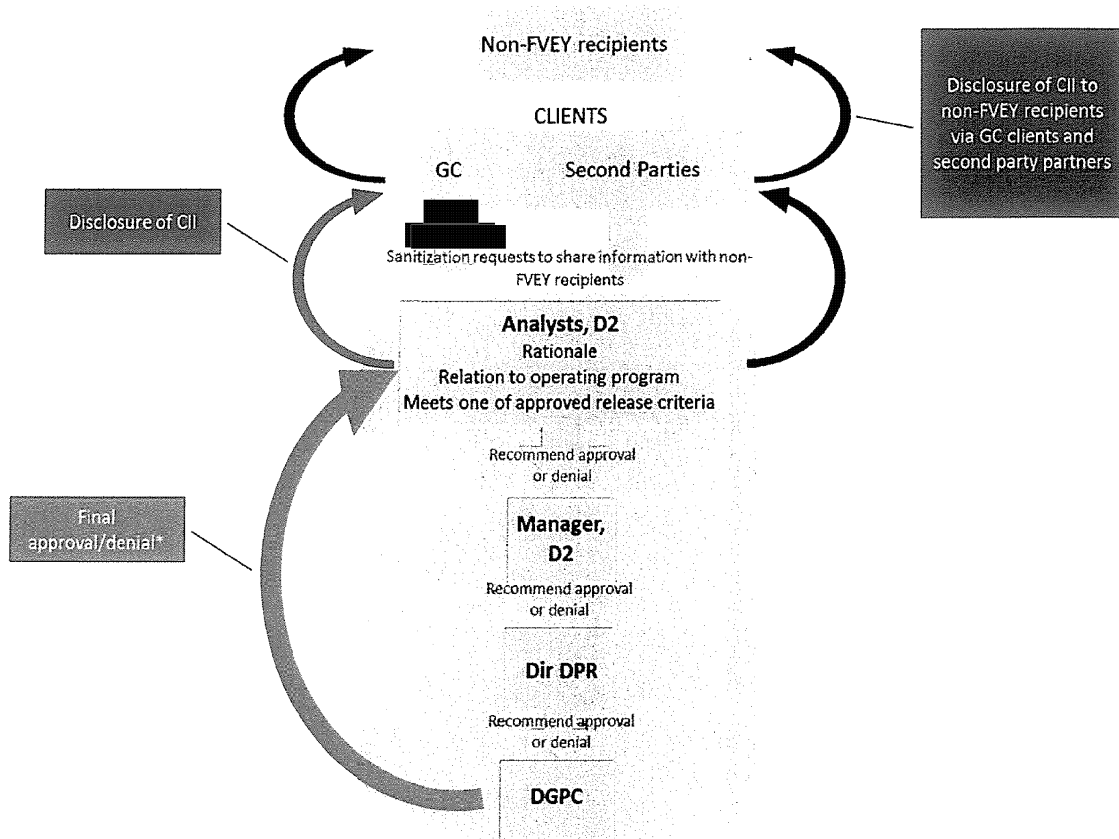
--	--



ANNEX D — Metrics for GC Agencies

Requesting Departments and Agencies	# Requests (in sample selected)	# CII (in requests)	Comments
Aboriginal Affairs and Northern Development Canada			
CBSA			
Canadian Cyber Incident Response Centre			
Canadian Nuclear Safety Commission			
Canada Revenue Agency			
CSEC			
CSIS			
Department of Foreign Affairs, Trade and Development			
Department of National Defence			
Finance			
Financial Transactions and Reports Analysis Canada			
Natural Resources Canada			
Privy Council Office			
Public Safety Canada			
RCMP			
TOTALS			

ANNEX E — Disclosure of CII in SIGINT Infographic



*Unless otherwise indicated as per delegated approval authority document