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 # 2200–102

March 23, 2016

The Honourable Harjit S. Sajjan, PC, OMM, MSM, CD, MP
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 the second part of my review of Communications Security Establishment (CSE) use of metadata in a foreign signals intelligence (SIGINT) context. 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) and in accordance with paragraph 10 of the 2011 Ministerial Directive on the Collection and Use of Metadata (Metadata MD).

This report builds on the 2015 *Review of CSE's Use of Metadata in a Signals Intelligence Context* (Part 1), which provided detailed background information on CSE collection, use and sharing of SIGINT metadata generally, and examined particular SIGINT metadata activities. This report examines additional SIGINT metadata activities not addressed in the 2015 report, including follow-up on past findings of Commissioners. A third report, to be completed in 2016, will examine CSE's use of metadata in an information technology security context.

The objectives of the review were to examine specific CSE SIGINT metadata activities, to assess whether the activities complied with the law, ministerial direction, and CSE operational policies and procedures, whether measures are in place to protect the privacy of Canadians, and to identify any areas for future in-depth review.

I examined three activities: (1) contact chaining activities [redacted] (2) follow-up on issues identified in my February 2014 report on the CSE Office of Counter-Terrorism (OCT) and in my March 2015 report on the 2014 Privacy Incident File (PIF) relating to the discovery of the targeting of a Canadian selector by a second party partner; and, (3) network analysis and prioritization.

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

I found that, during the period under review, contact chains [redacted] were authorized and generally conducted in a manner consistent with CSE operational policy. However, a small number of activities raised questions about CSE authorities, and CSE documentation and record-keeping practices were inconsistent. While I am not fully satisfied with CSE's approach, nor with the documentation and record-keeping practices for all of the activities examined, I found no instances of non-compliance with the law or with ministerial direction. I did not make any recommendations to address the issues and irregularities identified in this report because, subsequent to the period under review, CSE suspended indefinitely contact chaining activities [redacted] It is positive that CSE tracked and responded to case law developments that had implications for these metadata activities.

Prior to its decision to suspend these activities, CSE did not meet its commitments to address my recommendation to amend OPS-1-10 to reflect current practices and enhance record keeping. This can be explained by the short period of time between my OCT report and the suspension of the activities.

While CSE has updated policy guidance on metadata analysis for foreign intelligence purposes, policy on "chaining [redacted] remains vague and should be clarified.

CSE has made progress to address past recommendations to implement a process for the handling of instances involving the inadvertent targeting of a Canadian by a Second Party. I accept CSE's rationale for its response to the issues identified in previous reviews of OCT and PIF that this report followed up on. I believe it to be important that policy advice on this issue be provided to operational employees as soon as possible.

No questions were raised from my review of the authorities or policies governing CSE network analysis and prioritization metadata activities or of the conduct of those activities.

This review contains no recommendations.

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

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

Yours sincerely,

Jean-Pierre Plouffe

c.c. Ms. Greta, Bossenmaier, Chief, CSE

Enclosure

Office of the
Communications Security
Establishment Commissioner

CANADA

Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET // SI // CEO

Our File # 2200–102

Review of CSE's use of Metadata in a Signals Intelligence Context (Part 2)

March 23, 2016

P.O. Box/C.P. 1984, Station "B"/ Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax (613) 992-4096
info@ocsec bccst.gc.ca

TABLE OF CONTENTS

I. AUTHORITIES

The review was conducted under the authority of the Communications Security Establishment Commissioner as articulated in paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA), and in accordance with paragraph 10 of the 2011 *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata* (Metadata MD).

II. INTRODUCTION

The Communications Security Establishment (CSE) defines metadata as: "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content."[1]

CSE collects, uses and shares foreign signals intelligence (SIGINT) metadata from the global information infrastructure under the authority of paragraph 273.64(1)(*a*) of the NDA. SIGINT metadata activities are further guided and constrained by the Metadata MD,[2] as well as by CSE's operational policies.[3]

CSE collects, uses and shares SIGINT metadata for specific purposes in support of its foreign intelligence acquisition program, including to gain a better understanding of the global information infrastructure. CSE acquires SIGINT metadata from a variety of its own collection sources as well as those of its international partners, and sometimes receives disclosures of metadata from domestic partners.

---

[1] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata,* November 21, 2011, section 2(a).

[2] The November 21, 2011, MD to the Chief, CSE sets out the Minister of National Defence's expectations respecting CSE collection, use and sharing of metadata in the conduct of foreign intelligence activities. Included in the MD is a statement that activities undertaken pursuant to the MD are subject to review by the CSE Commissioner.

[3] Currently, CSE policy OPS-1-16, *Policy on Metadata Analysis for Foreign Intelligence Purposes*, January 7, 2016.

According to CSE policy, SIGINT may use metadata for the following purposes:[4]

- contact chaining;[5]
- network analysis and prioritization;[6]
- identifying new targets and selectors; and
- monitoring or identifying patterns of foreign malicious cyber activities.

Rationale for conducting this review

The collection, use and sharing of metadata are important activities for CSE. To ensure compliance with legal, ministerial and policy requirements, specific controls are placed on these activities, including the Metadata MD. Non-compliance while conducting these activities could have a significant impact on the privacy of Canadians.

Reviews by the Commissioner's office of CSE foreign intelligence activities generally include examination of CSE metadata activities and, since 2006, a number of reviews have focused in large part on CSE's collection, use and sharing of SIGINT metadata.

This report builds on the 2015 *Review of CSE's Use of Metadata in a Signals Intelligence Context* (Part 1) (our file # 2200-86), which provided detailed background information on CSE collection, use and sharing of SIGINT metadata generally, and examined particular SIGINT metadata activities. It examines additional SIGINT metadata activities not addressed in the 2015 report, including follow-up on past findings of Commissioners. A third report, to be completed in 2016, will examine CSE's use of metadata in an information technology (IT) security context.

---

[4] CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, December 1, 2012, section 3.6.

[5] "Contact chaining refers to the method developed to enable the analysis, from information derived from metadata, of communications activities or patterns to build a profile of communications contacts of various foreign entities of interest in relation to the foreign intelligence priorities of the Government of Canada, including the number of contacts to or from these entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period over which these contacts were attempted or made, as well as other activities aimed at mapping the communications of foreign entities and their networks." (*Ibid.* at section 8.4)

[6] "Network analysis and prioritization refers to the method developed to understand the global information infrastructure, from information derived from metadata, in order to identify and determine telecommunications links of interest to achieve Government of Canada foreign intelligence priorities. This method involves the acquisition of metadata, the identification of [redacted] the determination of the [redacted] the determination of the [redacted] (*Ibid.* at section 8.16)

III. OBJECTIVES

The objectives of the review were to examine specific CSE SIGINT metadata activities, to assess whether the activities complied with the law, ministerial direction and CSE operational policies and procedures, to assess whether measures are in place to protect the privacy of Canadians, and to identify any areas for future in-depth review.

IV. SCOPE

The Commissioner's office examined specific CSE SIGINT metadata activities, namely:

1. contact chaining activities [redacted]
2. issues identified in the Commissioner's reports on CSE's Office of Counter-Terrorism (OCT) (February 2014) and in the 2014 CSE Privacy Incidents File (March 2015) relating to the discovery of the targeting of a Canadian selector by a second party partner;[7] and
3. network analysis and prioritization.

V. CRITERIA

The Commissioner's office assessed whether CSE's use of metadata in a SIGINT context complied with the law and protected the privacy of Canadians in the context of the Commissioner's standard review criteria.

A) Legal Requirements

The Commissioner expects CSE to conduct its activities in accordance with the NDA, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code* and any other relevant legislation. The Commissioner examined Department of Justice Canada legal advice received by CSE in order to inform his assessment of whether CSE conducted its activities in compliance with the law.[8]

---

[7] The Second Parties are CSE's four SIGINT partners: the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Signals Directorate, and the New Zealand Government Communications Security Bureau. Collectively with CSE, they are referred to as the Five Eyes.

[8] If legal advice given to CSE is shared with the Commissioner's office, this is done on the understanding that the sharing by CSE of information that is subject to solicitor-client privilege does not constitute a waiver by CSE of its privilege.

B) Ministerial Requirements

The Commissioner expects CSE to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

C) Policies and Procedures

The Commissioner expects CSE:

i) to establish appropriate policies and procedures to guide its activities and to provide sufficient direction on legal and ministerial requirements, including the protection of the privacy of Canadians;

ii) to ensure its employees are knowledgeable about and comply with the policies and procedures; and

iii) to maintain the integrity of the operational activities by applying an effective policy compliance monitoring framework to its activities, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

The Commissioner's office reviewed relevant CSE records, conducted interviews with CSE employees, and received briefings on specific CSE activities in order to assess compliance with legal and ministerial requirements, as well as associated policies and procedures. The Commissioner's office also reviewed written responses provided by CSE to questions raised during the course of the review. This included the examination of documents such as CSE policies and procedures, administrative records, and legal advice from the Department of Justice Canada.

VII. BACKGROUND

In the summer of 2013, the Commissioner's office started a comprehensive review of CSE's use of metadata in the context of both its SIGINT and its IT security activities. This review was planned prior to the unauthorized disclosures of classified information initiated by former U.S. National Security Agency (NSA) contractor Edward Snowden. Subsequent to the disclosures, the high public profile of metadata activities underscored the utility of such a review.

During the course of the review, it became clear that, to be timely, the volume and depth of information to be examined and assessed required the Commissioner's office to prepare more than one report. Initially, we decided to prepare two reports on CSE

SIGINT and IT security metadata activities, respectively. However, after being informed by CSE that it did not properly minimize Canadian identity information contained in certain metadata prior to it being shared with second party partners, we decided to further divide the SIGINT component into two reports. The Commissioner's *Review of CSE's Use of Metadata in a Signals Intelligence Context* (Part 1) — provided to the Minister of National Defence in March 2015 and summarized in the Commissioner's 2014–2015 public annual report — examined CSE SIGINT architecture relating to metadata and minimization deficiencies in shared metadata. It contains detailed background information, including on: what is metadata; how CSE uses it in a SIGINT context; how CSE collects metadata; where it is stored; how it is accessed; how it is shared; related tools, systems and databases; and measures in place to protect the privacy of Canadians. Much of this background is applicable to the activities described below, but will not be repeated in whole in this report.

This second report on CSE SIGINT metadata activities addresses elements that were set aside during the first review in order to fully explore the incidents relating to metadata minimization.

Contact Chaining

CSE operational policy OPS-1 provides that, in accordance with the Metadata MD, CSE may search metadata for the purpose of providing any information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization, terrorist group or other such entity as they relate to international affairs, defence or security. Contact chaining is one technique that a SIGINT analyst may use to identify and document the communications activities or patterns of an entity of potential foreign intelligence interest.

Analysts conduct contact chaining activities primarily through a tool called [redacted]

[redacted] Contact chaining is normally conducted [redacted] in which case an analyst does not need to seek approval prior to undertaking the activity.

During the period under review, CSE policy OPS-1-10, *Procedures for Metadata Analysis* [redacted] (June 25, 2010), provided direction on the process for analysts to conduct metadata analysis — in pursuit of foreign intelligence — [redacted] According to OPS-1-10, analysts could seek approval for [redacted] a contact chain [redacted] if: there were reasonable grounds to believe that the analysis would provide information or intelligence about the capabilities, intentions or actions of foreign actors; the expected foreign intelligence would correspond to a Government of Canada intelligence requirement; and other avenues of foreign intelligence target development had been considered. Authorization required a form to be approved by five different supervisors and managers responsible for operations, policy and internal oversight, and culminating in sign-off by the Director General, Intelligence (DGI). The form was to include: the foreign intelligence priority the analysis is expected to satisfy; [redacted] and a detailed rationale outlining why the requester had reasonable grounds to believe that the activity would lead to foreign intelligence. With approval, an analyst could conduct such contact chains for up to [redacted] using metadata that had been collected at any time prior to the date of approval. OPS-1-10 permitted [redacted] and, if a second [redacted] The Commissioner's December 2010 *Review of CSEC's Contact Chaining Activities* [redacted] provides detailed background information on this activity.

Solicitor-Client Privilege

[redacted]

[9] If the metadata analysis directly led to another [redacted]

Network Analysis and Prioritization

The [redacted] conducts network analysis and prioritization activities to identify and characterize telecommunication links of most value to meet Government of Canada foreign intelligence priorities.[10] Network analysis and prioritization activities are governed by OPS-1 and the Metadata MD, including associated requirements to protect the privacy of Canadians.

[redacted] Activities

[redacted]

[10] The Commissioner's March 2009 *Review of Recommendation No. 1 from the January 2008 Review Report Respecting CSEC's Ministerial Directive on the Collection and Use of Metadata — CSEC's* [redacted] *Network Analysis and Prioritization* [redacted] *Activities* provides detailed background information on these activities.

[11] CSE also acquires SIGINT [redacted] data through the targeting of foreign telecommunications [redacted] This results in [redacted] each of which assist CSE in [redacted] for SIGINT purposes. CSE SIGINT Program Instruction SPI-2-14 (March 2014), provides specific guidance on these activities. It defines [redacted] data as information that details the [redacted]

[redacted]

VIII. FINDINGS

1. Contact Chaining [redacted]

Finding no. 1: Contact Chaining [redacted]

During the period under review, contact chains [redacted] were authorized and generally conducted in a manner consistent with CSE operational policy; however, a small number of activities raised questions about CSE authorities, and CSE documentation and record-keeping practices were inconsistent.

The Commissioner's office examined all of the [redacted] contact chains [redacted] that were conducted from November 1, 2012, to October 31, 2013. The activities pertained to a number of different foreign intelligence target sets and were carried out by analysts from several different operational areas under CSE's DGI.

The Commissioner's office found that the contact chains [redacted] were authorized and generally conducted in a manner consistent with OPS-1-10.

It is positive that forms and other records demonstrated that CSE managers within the Directorate General of Policy and Communications (DGPC) exercised a robust challenge function relating to the approval process for requests for contact chaining activities [redacted] For example, DGPC rejected a number of requests because of concerns that, among other things, CSE might be perceived to be directing an activity at a Canadian. In other cases, DGPC required a stronger rationale to be provided prior to approval.

However, the Commissioner's office questioned CSE authorities relating to two of the activities conducted during the period under review.

In the first case, CSE records were unclear respecting whether the [redacted]

[redacted] — pursuant to CSE's authority under paragraph 273.64(1)(*a*) of the NDA (part (a) of CSE's mandate) or under paragraph 273.64(1)(*c*) of the NDA (part (c) of CSE's mandate).[12] CSE records contained [redacted] both pertaining to the same [redacted] network. [redacted] One record was a disclosure under part (a) of CSE's mandate relating to the acquisition and use of foreign intelligence. IRRELEVANT

IRRELEVANT

The Commissioner's office also observed two other irregularities that occurred in exigent circumstances.

In the first case, CSE undertook a contact chain [redacted] at [redacted][16] When the Commissioner's office asked whether the contain chain was conducted under part (c) of CSE's mandate, CSE indicated that it was done under part (a), [redacted] According to CSE "this information was not used by CSE to find information on the individual himself" and "if this was not such an urgent situation, the OCT probably would have rejected the message [redacted][17]

[12] A number of reports of the Commissioner have directly addressed CSE authorities under parts (a) and (c) of its mandate and contact chaining, namely: *Support to Law Enforcement (RCMP) — Phase II* (June 2006), *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005* (January 2008), [redacted] — *Phase I: CSE Mandate (a)* (January 2008), and *A Review of CSE's Contact Chaining Activities* [redacted] (December 2010). Subsequent to Commissioners' questions, in April 2007, a former Chief of CSE suspended all contact chaining activities [redacted] In October 2008, CSE resumed these activities after making significant changes to the conduct of the activities, and to the associated policy and accountability framework. During the period under review, OPS-1-10 prohibited [redacted] for contact chaining activities [redacted] IRRELEVANT

IRRELEVANT

[13] May 22, 2015, e-mail from CSE External Review.

[14] The Commissioner's February 2014 *Review of the Activities of the Office of Counter-Terrorism* identified similar violations.

[15] This deficiency is described in detail in the Commissioner's February 2014 OCT report.

[16] The appropriate process to follow to meet information needs is described in detail in the Commissioner's February 2014 *Review of the Activities of the Office of Counter-Terrorism*.

[17] May 22, 2015, e-mail from CSE External Review.

In another case, an analyst sought permission to query [redacted] In the absence of specific policy for such a query, the analyst sought guidance from the SIGINT Programs Oversight and Compliance section (now called SIGINT Policy and Review), which recommended following the approval and tracking process in OPS-1-10.

In addition, the Commissioner's office found that documentation and record-keeping practices relating to contact chaining activities [redacted] were inconsistent.

Several files contained no record of the results of the activities, contrary to OPS-1-10. When asked about this, CSE responded that, in some cases, no results were obtained. In such cases, however, CSE policy requires analysts to record a "nil" response in the file.

While the Commissioner's office is not fully satisfied with CSE's approach, and documentation and record-keeping practices for all of the contact chaining activities [redacted] examined, we found no instances of non-compliance with the law or with ministerial direction. The Commissioner's office is not making any recommendations to address the issues and irregularities identified in this report because, subsequent to the period under review, CSE suspended indefinitely its contact chaining activities [redacted] It is positive that CSE tracked and responded to case law developments that had implications for these metadata activities.

Prior to its decision to suspend the activities, CSE did not meet its commitments to address the Commissioner's recommendation to amend OPS-1-10 to reflect current practices and enhance record keeping.[18] This can be explained by the short period of time between the Commissioner's OCT report and the suspension of the activities. CSE also did not finish implementing all of the recommendations of its Directorate of Audit, Evaluation and Ethics audit of contact chaining [redacted] (July 2011).

Finding no. 2: Contact Chaining [redacted]

Subsequent to the indefinite suspension of contact chaining activities [redacted] formal policy guidance regarding "chaining [redacted] remains vague and should be clarified.

In 2011, CSE's Directorate of Audit, Evaluation and Ethics' audit of contact chaining [redacted] noted that "instructions on 'chaining [redacted] should be clearly articulated in a policy instrument in order to ensure policy compliance,"[19] and recommended that CSE clarify the policy on "chaining [redacted]"[20]

---

[18] Commissioner's February 2014 *Review of the Activities of the Office of Counter-Terrorism*.
[19] CSE Directorate of Audit, Evaluation and Ethics, *Audit of Contact Chaining* [redacted] July 7, 2011, page 9, paragraph 3.2.1.
[20] *Ibid.* at 15.

Although CSE accepted the recommendation from the audit, it cancelled OPS-1-10 when it stopped contact chaining activities [redacted] CSE worked on a new policy document, OPS-1-16, to provide updated guidance to analysts. OPS-1-16 was promulgated in January 2016. Therefore, during the period under review, there was insufficient policy guidance regarding "chaining [redacted] Formal guidance is now available, but would benefit from further clarification.

In response to a question about what impact the legal opinions cited above[21] had on activities other than contact chaining [redacted] CSE noted:

[redacted]

During the period under review, CSE practices relating to "chaining [redacted] were varied and guidance was informal and provisional.

CSE provided the Commissioner's office with internal CSE correspondence regarding this practice. In one e-mail, an OCT manager notified his team to cease all manual contact chaining [redacted][23] Another e-mail between two directors outlined ambiguities around distinctions between an analyst manually [redacted] and a machine automatically doing so.[24]

With the cancellation of contact chaining activities [redacted] there is a need for clear policy guidance on whether and when "chaining [redacted] remains permissible. Section 3.7 of operational policy OPS-1-16 places emphasis on the prohibition against initiating chaining activities [redacted] and on the principle that analysts are not to construct an automated tradecraft in such a way as to deliberately return information [redacted] OPS-1-16 does not prohibit an [redacted] contact chain tradecraft from chaining [redacted] CSE indicated that it will provide training on this subject and on the requirements of the new policy. It also noted that, like with other policies, interpretation assistance is readily available to analysts through consultation with internal policy compliance groups.

Subsequent to discussion with CSE, the Commissioner's office remains of the view that policy guidance regarding "chaining [redacted] is vague and should be clarified. OPS-1-16 would benefit from additional detail about what is and isn't permissible; including details contained in the written explanations provided to the

---

[21] *Supra*, p.6.
[22] May 22, 2015, e-mail from CSE External Review in response to RFI 10.2
[23] August 1, 2014, e-mail from Manager, CT Operations to staff.
[24] July 14, 2014, e-mail from Director, SIGINT Program Requirements to Director, [redacted]

Commissioner's office in the conduct of this review[25] would strengthen OPS-1-16. The Commissioner's office will examine the conduct of these activities involving Canadians as part of future activity-based reviews.

2. Issues related to the discovery of the targeting of a Canadian selector by a second party partner

Finding no. 3: Targeting of a Canadian Selector by a Second Party Partner

> CSE is making progress to address past recommendations of the Commissioner and to implement a process for the handling of instances of inadvertent targeting of a Canadian by a Second Party.

During the research phase of the OCT review, the Commissioner's office observed a screenshot in the [redacted] database indicating that a Canadian telephone number was being targeted [redacted][26] Follow-up investigation revealed that CSE had no specific policy in place for an analyst to follow if the analyst discovers that a Canadian is being targeted by a Second Party. The Commissioner recommended that CSE should promulgate guidance to codify its practices to address such cases, including notification to the Second Party to desist from such targeting and keeping a record of such cases. The Commissioner indicated that he would monitor developments. Similarly, in his March 2014 review of CSE's Privacy Incident File (PIF) for calendar year 2013, the Commissioner recommended that:

> Because of the enhanced potential of the violation of the privacy of a Canadian if a Second Party targets that Canadian... CSE [should] request second party partners to confirm de-targeting of Canadians, and indicate in the PIF whether the Second Party has confirmed that it stopped targeting that Canadian. This measure will enhance the protection of the privacy of Canadians and support you as Minister of National Defence in your accountability for CSE.

CSE is making progress to address these recommendations.

In May 2014, CSE issued SPI-6-14, *Responding to Inadvertent Targeting Incidents*, a SIGINT Program Instruction. According to CSE, while it is focused on incidents of inadvertent targeting by CSE, the same principles generally apply to cases involving inadvertent targeting of a Canadian by a Second Party.[27] SPI-6-14 requires CSE [redacted] to investigate whether a second party partner has targeted a Canadian selector originally discovered to have been inadvertently targeted by CSE, and to ask the partner(s) to stop targeting the selector, if required. CSE indicated that it has no plans to

---

[25] February 12, 2016, e-mail from CSE External Review entitled "Review of CSE's Use of Metadata in SIGINT Context (Part 2) – preliminary comments on draft report dated 4 February 2016."
[26] Although the Second Parties pledge not to direct activities at each other's citizens, they are sovereign nations and may derogate from their agreements, if it is judged necessary for their respective national interests.
[27] July 22, 2015, e-mail from CSE External Review in response to RFI 14.2.

revise operational policy to specifically address this subject. It will, however, communicate policy advice to operational staff through training, and may provide further direct guidance to employees, as needed. The Commissioner's Office believes it to be important that this policy advice be provided to operational staff as soon as possible. Also, in May 2015, CSE's Director of Disclosure, Policy and Review sent letters to liaison officers from each of the second party partner agencies, informing them of CSE's new approach to cases involving inadvertent targeting of a Canadian by a Second Party. The letters outlined CSE's existing practice of requesting de-targeting of Canadians or persons in Canada when inadvertent targeting is discovered, and stated that CSE would begin to also request confirmation by the Second Parties that, subsequent to a request, they had in fact ceased any inadvertent targeting.[28]

The Commissioner's office conducted a further investigation of the specific case discovered during the OCT review involving the targeting of a Canadian person [redacted] Contrary to the Commissioner's recommendation, in this case, CSE did not advise its second party partners to desist from targeting the Canadian. CSE indicated it had not done so because of the amount of time that had elapsed and that the risk to the privacy of the Canadian may be greater if it was to draw attention to the matter.[29] The Commissioner's office accepts this rationale in this particular situation.

In response to a request by the Commissioner's office, CSE determined that the Canadian was referenced in [redacted] reports produced between December 2010 and July 2013, [redacted] reports produced between 2010 and 2012, [redacted] report from 2011, and [redacted] report from 2012. Following an internal investigation, CSE retroactively included this detail in its PIF for calendar year 2014.

One of the PIF entries related to these incidents explains that the foreign cell phone number of this Canadian was inadvertently targeted by CSE from October 22 to November 3, 2010. When CSE discovered that the cell phone was being used by a Canadian, the same OCT analyst who originally had targeted the number then de-targeted it, and made a note in [redacted][30] not to target that number. CSE assessed that it is unlikely that any of the second party reports relating to the Canadian were based on communications of the Canadian intercepted by CSE, since the reports appear to be based on communications intercepted outside the brief period of time when CSE was

IRRELEVANT

[29] *Supra*, note 22.

[30] [redacted] is the cover name for CSE's target knowledge database. It contains information — from a variety of sources — populated by DGI analysts respecting foreign entities of foreign intelligence interest to the Government of Canada and associated selectors. [redacted] links CSE's target knowledge with selectors. In addition to containing a target knowledge database, [redacted] provides a targeting tool, that DGI analysts use to submit selectors [redacted] for validation and targeting. [redacted] permits DGI analysts to monitor the status of any selector for which they are responsible (targeted or not).

inadvertently targeting the Canadian. The Commissioner's office reviewed all [redacted] reports and agrees with CSE's assessment. In addition, the Canadian's identity information was supressed in all of the reports in a manner consistent with CSE and second party policies.

[redacted]

3. Network Analysis and Prioritization

Finding no. 4: Network Analysis and Prioritization

Network analysis and prioritization activities remain critical to the execution of CSE's foreign signals intelligence mandate.

Last year's first report on CSE's use of metadata in a SIGINT context outlined in detail the Commissioner's investigation into a particular set of activities that fall within network analysis and prioritization. The Commissioner concluded that these IP profiling and behavioural analytics activities were conducted in compliance with the law.

In the context of this review, the Commissioner's office further examined the activities of CSE's [redacted] The [redacted] section of CSE collaborates with the DGI to analyze gaps in CSE's ability to extract intelligence from the global information infrastructure. The [redacted] is then tasked with [redacted] which coordinates follow-on activity with DGI.

The Commissioner's office was satisfied with the information provided by CSE. We have no questions about the authorities or policies governing network analysis and prioritization activities described in the background section of this report.

IX. CONCLUSION

This report builds on the 2015 *Review of CSE's Use of Metadata in a Signals Intelligence Context* (Part 1), which provided detailed background information on CSE collection, use and sharing of SIGINT metadata generally, and examined particular SIGINT metadata activities. This report examines additional SIGINT metadata activities not addressed in the

[31] In 2016–2017, the Commissioner's office plans to [redacted] and reporting.

[redacted]

2015 report, including follow-up on past findings of Commissioners. A third report, to be completed in 2016, will examine CSE's use of metadata in an IT security context.

The objectives of the review were to examine specific CSE SIGINT metadata activities, to assess whether the activities complied with the law, ministerial direction, and CSE operational policies and procedures, whether measures are in place to protect the privacy of Canadians, and to identify any areas for future in-depth review.

The Commissioner's office examined three activities, namely:

1. contact chaining activities [redacted]
2. issues identified in the Commissioner's reports on CSE's OCT (February 2014) and in the 2014 CSE PIF (March 2015) relating to the discovery of the targeting of a Canadian selector by a second party partner; and
3. network analysis and prioritization.

The Commissioner's office found that, during the period under review, contact chains [redacted] were authorized and generally conducted in a manner consistent with CSE operational policy. However, a small number of activities raised questions about CSE authorities, and CSE documentation and record-keeping practices were inconsistent. While the Commissioner's office is not fully satisfied with CSE's approach, nor with the documentation and record-keeping practices for all of the contact chaining activities [redacted] examined, we found no instances of non-compliance with the law or with ministerial direction. The Commissioner's office does not make any recommendations to address the issues and irregularities identified in this report because, subsequent to the period under review, CSE suspended indefinitely contact chaining activities [redacted] It is positive that CSE tracked and responded to case law developments that had implications for these metadata activities.

Subsequent to the indefinite suspension of contact chaining activities [redacted] policy guidance regarding "chaining [redacted] remains vague and should be clarified.

The Commissioner's office found that CSE is making progress to address past recommendations of the Commissioner and to implement a process for the handling of instances of inadvertent targeting of a Canadian by a Second Party. The Commissioner's office accepts CSE's rationale for its response to the issues identified in previous reviews of CSE's OCT and PIF that this report followed up on. The Commissioner's Office believes it to be important that policy advice on this issue be provided to operational staff as soon as possible.

The Commissioner's office has no questions about the authorities or policies governing CSE's network analysis and prioritization metadata activities or about the conduct of those activities.

This review contains no recommendations.

Annex A is a list of findings. Annex B is a list of interviewees.

Jean-Pierre Plouffe, Commissioner

ANNEX A — Findings

Finding no. 1: Contact Chaining [redacted]

During the period under review, contact chains [redacted] were authorized and generally conducted in a manner consistent with CSE operational policy; however, a small number of activities raised questions about CSE authorities, and CSE documentation and record-keeping practices were inconsistent.

Finding no. 2: Contact Chaining [redacted]

Subsequent to the indefinite suspension of contact chaining activities [redacted] policy guidance regarding "chaining [redacted] remains vague and should be clarified.

Finding no. 3: Targeting of a Canadian Selector by a Second Party Partner

CSE is making progress to address past recommendations of the Commissioner and to implement a process for the handling of instances of inadvertent targeting of a Canadian by a Second Party.

Finding no. 4: Network Analysis and Prioritization

Network analysis and prioritization activities remain critical to the execution of CSE's foreign signals intelligence mandate.

ANNEX B — Interviewees

The following CSE employees provided information or facilitated the review:

Manager, External Review
Senior Review Advisor, External Review

Access Analyst, Office of Counter-Terrorism ([redacted]

Team Leader, [redacted]
Analyst, [redacted]

Manager, [redacted]