



**National Security
and Intelligence
Review Agency**

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

Review of Operational Collaboration between the Communications Security Establishment and the Canadian Security Intelligence Service

NSIRA // Review 21-16

TOP SECRET//SI/[REDACTED]//CEO

Table of Contents

List of Acronyms	iii
Glossary of Terms	iv
EXECUTIVE SUMMARY	vii
1. INTRODUCTION	1
Authority	1
Scope of the Review	1
Methodology	2
Review Statements	2
2. BACKGROUND	2
3. FINDINGS, ANALYSIS, AND RECOMMENDATIONS	3
Collaboration in Operations	3
Requests for Assistance	3
Joint Operations	9
Collaboration in Information Sharing	14
Lead Information Messages	14
Exceptional Reporting Loop	22
Protected Entity Tool	24
Collaboration in Threat Reduction Measures	25
CSIS Consultation with CSE	25
TRM Coordination with CSE Active Cyber Operation	26
Status of CSE-CSIS Collaboration	27
4. CONCLUSION	30
Annex A: Operations	31
16(1)(c) [REDACTED] Warranted Section 12 Investigation	31
[REDACTED] Warranted Section 16 Operation	31
[REDACTED] Operation	33

TOP SECRET//SI/[REDACTED]//CEO

15(1)

Annex B: Section 35 Reports 34

15(1)(f)	Non-compliance with the Law – CSE Analyzes [REDACTED] of a Canadian's Device	34
	Non-compliance with the Law – CSE Receives and Utilizes Entire Exceptional Reports	38

Annex C: Findings and Recommendations..... 40

Collaboration in Operations: Requests for Assistance	40
Collaboration in Operations: Joint Operations.....	41
Collaboration in Information Sharing: CSIS Lead Information	42
Collaboration in Information Sharing: Exceptional Reporting Loop	43
Collaboration in Information Sharing: Protected Entity Tool.....	43
Collaboration in Threat Reduction Measures	43
CSE-CSIS Relationship	44

15(1)

TOP SECRET//SI/[REDACTED]//CEO

List of Acronyms

ACO – Active Cyber Operation

CLI – CSIS Lead Information

CSE – Communications Security Establishment

CSE Act – *Communications Security Establishment Act*

CSIS – Canadian Security Intelligence Service

CSIS Act – *Canadian Security Intelligence Service Act*

DoJ – Department of Justice

FILGI – Foreign Intelligence Lead Generation Information

GC – Government of Canada

HUMINT – Human Intelligence

[REDACTED]

IP – Internet Protocol

IRD – Intelligence Requirement Disclosure

[REDACTED]

16(1)(c) **NDA** – *National Defence Act*

[REDACTED]

OCSEC – Office of the Communications Security Establishment Commissioner

[REDACTED]

RFA – Request for Assistance

SIGINT – Signals Intelligence

Glossary of Terms

Active Cyber Operation. Activities conducted on or through the Global Information Infrastructure that degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization, or terrorist group as they relate to international affairs, defence or security.

Canadian(s). A Canadian citizen, a permanent resident as defined in section 2(1) of the *Immigration and Refugee Protection Act*, or a corporation incorporated under the laws of Canada or a province.

[REDACTED]

16(1)(c)

Contact Chaining. The process of analyzing an identifier to determine the nature of the user's communications (e.g. contacts, duration and time of communications events); can be performed manually or through an automated process.

[REDACTED]

CSE's Assistance Mandate. Under section 20 of the *Communications Security Establishment Act* (CSE Act), CSE is authorized to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence. Under section 25(1) of the CSE Act, CSE has the same authority as the agency requesting assistance, and is subject to the same limitations imposed on the agency, including warrant conditions.

CSE Risk Assessment. An analysis of legal, reputational, partnership, and operational risks associated with an operation.

CSIS Risk Assessment. An analysis of legal, reputational, operational, and foreign policy risks associated with an operation.

CSIS's Threat Reduction Measures. Under section 12.1(1) of the *Canadian Security Intelligence Service Act* (CSIS Act), if there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, CSIS may take specific measures, within or outside of Canada, to reduce that threat.

Designated Service Employee. A CSIS employee belonging to a class of employees designated pursuant to CSIS policies to conduct assessments found in CSIS warrant

15(1)

TOP SECRET//SI//[REDACTED]//CEO

conditions, and for which a Regional Director General or a Director General is accountable for these employees' actions.

Exceptional Reporting. Intelligence reports produced by foreign SIGINT partners derived as a result of directly targeting Canadians.

Five Eyes. International intelligence-sharing partnership between the United States, the United Kingdom, Australia, New Zealand, and Canada.

Foreign Intelligence. Information about the capabilities, intentions or activities of a foreign individual, state, organization, or terrorist group, as they relate to international affairs, defence or security.

Foreignness Assessment. Analysis conducted by CSE personnel to establish that the user of the device at issue is not Canadian or located in Canada.

Infrastructure. Any functional component, physical or logical, of communication systems, information technology systems, and networks.

15(1)(f)

[REDACTED]
[REDACTED]
[REDACTED]

Incidental Collection. Acquisition of information that was not itself deliberately sought as part of an information acquisition activity and that was not directed at the Canadian or person in Canada.

Joint Operation. Operational activity undertaken by CSIS or CSE in conjunction with a domestic or foreign partner.

CSIS Lead Information. Messages from CSIS to CSE that include lead information that CSE can choose to further pursue under the foreign intelligence aspect of its mandate.

Operational Plans. A policy document that guides operational activity, generally includes all authorities and stakeholders, permissible activities, roles and responsibilities, and mandatory processes.

Protected Entity Tool. Tool within CSE's targeting database that helps to prevent CSE from targeting Canadians by flagging the identifiers as belonging to a Canadian and blocking any future querying or targeting requests against that selector.

Request for Assistance. A formal request made to CSE under section 20 of the CSE Act to obtain CSE expertise and assistance needed to carry out an operation.

Reverse Targeting. Where CSE performs investigative SIGINT activities on foreign targets for the purposes of obtaining information about a Canadian in contact with the foreign target.

Selectors. Unique identifiers associated with an entity, such as a phone number, email address, or social media account.

SLINGSHOT. CSE's intelligence reporting repository.

Target. Any entity (individual, corporation, organization, or foreign state) that is the subject of a national security investigation and related operational activity.

Targeting. Activities undertaken by CSE and CSIS to gain access to information related to a target.

Warranted Target. The subject of an investigation conducted by CSIS for which CSIS has obtained a warrant under section 21 of the CSIS Act.

EXECUTIVE SUMMARY

The Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS) are two core pillars of Canadian intelligence collection, meaning effective collaboration between the departments is critical to national security. The ability to consider both departments' activities in tandem is important given the tension between CSIS's mandate, which authorizes collection and sharing of information about Canadians, and CSE's core prohibition against directing its activities at Canadians.

NSIRA's predecessor agencies did not have mandates that allowed for review across multiple government departments. This is the first review of CSE and CSIS collaboration that was able to access information from both departments and examine a sample of CSE and CSIS collaborative operational activities and information sharing. This includes information concerning collaboration between CSIS and CSE further to CSIS's Threat Reduction Measures (TRMs). Through this review, NSIRA is satisfying its annual requirement under section 8(2) of the *National Security and Intelligence Review Agency Act* to review an aspect of CSIS's TRMs.

Operational Collaboration

CSIS Request for Assistance (RFAs)

CSE executes CSIS RFAs under the assistance aspect of its mandate provided by section 20 of the *Communications Security Establishment Act* (CSE Act). NSIRA found a lack of information sharing and proactive planning on behalf of CSE and CSIS and recommended some procedural changes to improve information flow, transparency, and accountability of CSE's execution of CSIS's authorities and powers.

Joint Operations

Joint operations are operations in which the departments work in parallel against common threats under their respective mandates and associated legislative authorities. However, a tension exists between CSIS's mandate, which authorizes collection of information about Canadians, and CSE's core prohibition against directing its activities at Canadians under section 22(1) of the CSE Act. NSIRA found that CSE failed to account for, and mitigate, the elevated risk of targeting Canadians when working with CSIS. Accordingly, NSIRA recommended that the two departments more comprehensively engage in joint operational planning and that CSE conduct risk and foreignness assessments that place a greater focus on ensuring they abide by their prohibition against targeting Canadians when collaborating with CSIS.

15(1)

TOP SECRET//SI//CEO

Information Sharing

CSIS Lead Information Messages (CLIs)

CSIS uses CLIs to share information that CSE may find relevant for its own foreign intelligence purposes. These messages contain a wide range of information, including information about Canadians, and sometimes CSIS will make requests for action further to the disclosure. NSIRA found the CLI process lacked governance and accountability structures and created a risk of CSE performing reverse targeting. That is, where CSE performs investigative SIGINT activities on foreign targets for the purposes of obtaining information about a Canadian in contact with the foreign target, which amounts to directing its activities at Canadians. NSIRA recommended that both departments establish policies, procedures, and analyst training to standardize the disclosure and receipt of CLIs. NSIRA also recommended that CSIS cease making requests pertaining to Canadians via the CLI process.

Furthermore, NSIRA found that CSE's application of incidental collection provisions may not be appropriate in situations where CSE knows there is a Canadian nexus to the foreign intelligence lead, and where it knows it is likely to collect Canadian information in pursuing the lead. NSIRA recommended that CSE reconsider how it manages the collection, retention, and reporting of specific Canadian information when it has advance knowledge of this information, given the protections of the *Canadian Charter of Rights and Freedoms*.

- 15(1)(f) NSIRA found one case of non-compliance with the law further to a CLI. In this case, CSIS sent CSE a CLI accompanied by [REDACTED] of a Canadian's device. CSE analyzed [REDACTED] of the device, with the intent to obtain foreign intelligence information from it. NSIRA found this contravened CSE's prohibition against directing its activities at Canadians and recommended that CSE clearly articulate in its policy that conducting analysis on Canadian information to identify information of foreign intelligence value is prohibited.

The Exceptional Reporting Loop

In the exceptional reporting loop, CSE acts as a conduit between foreign partners and CSIS for the delivery of foreign agency SIGINT reporting derived from directly targeting Canadians. Some of this reporting loops back to be ingested by CSE under its foreign intelligence mandate. CSE utilizes the entire report, as opposed to just the information of foreign intelligence value. NSIRA found this to be non-compliant with the law given CSE's prohibition on directing its activities at Canadians. NSIRA recommended that CSIS only disclose, and CSE only utilize, the foreign lead information extracted from the reports.

The Protected Entity Tool

Under both the CLI process and the exceptional reporting loop CSE possesses the protected entity tool within its targeting database that can be applied to Canadian identifiers. When used, this tool guards against subsequent targeting of the identifier. NSIRA found that this mechanism is not consistently applied and recommended codifying its use into policy.

Threat Reduction Measures (TRMs)

CSIS regularly consults CSE prior to undertaking TRMs, as required by section 12.1(3) of the CSIS Act. This consultation occurs during the general planning and approval stages of a TRM. NSIRA found that CSE stated a preference for more granular consultation later in the TRM process which CSIS did not pursue; NSIRA recommended that CSIS do so.

NSIRA also reviewed one situation where a CSIS TRM was used to complement a CSE Active Cyber Operation (ACO). NSIRA found that CSE did not notify CSIS in a timely manner of a compliance incident under its ACO. NSIRA recommended that when CSE identifies compliance incidents in its own activity that overlap with TRM activity it share the details with CSIS.

CSE-CSIS Relationship

NSIRA found that in one operation CSE failed to cooperate effectively with CSIS, leading to a missed opportunity to advance Canadian intelligence objectives via domestic collaboration. CSE's lack of prioritization of domestic collaboration evidenced in this operation presented as a more general issue. As CSE has unique technical expertise, its willingness to work with domestic partners can be pivotal to Canadian success. If CSE does not readily consider the totality of potential operational yield for Canada realized through domestic collaboration opportunities, Canada risks losing opportunities to satisfy intelligence objectives.

1. INTRODUCTION

Authority

1. This review was conducted under the authority of section 8(1)(a) and section 8(2) of the *National Security and Intelligence Review Agency Act*. This review satisfies NSIRA's annual legislative requirement to review an aspect of CSIS's performance of its Threat Reduction Measures (TRMs).¹

Scope of the Review

2. This review considered operational collaboration between the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS). Unless otherwise specified, CSE's reviewed activities were conducted under the foreign intelligence authorities found at section 16 of the *Communications Security Establishment Act* (CSE Act) and associated Ministerial Authorizations.
3. NSIRA sought to understand how and under what circumstances CSE and CSIS collaborate. To do so, NSIRA reviewed two primary methods of collaboration in operations: collaboration under CSE's assistance mandate, and collaboration performed under each department's respective mandates. In addition, NSIRA reviewed two types of information sharing: CSIS lead information messages (CLIs) and the disclosure of exceptional reporting. NSIRA evaluated governance structures and legal compliance, among other considerations.
4. NSIRA also reviewed collaboration between the departments within the context of CSIS's execution of TRMs. NSIRA reviewed CSIS's consultation with CSE in the TRM regime, as well as one case where a CSIS TRM was used to complement an Active Cyber Operation (ACO) undertaken by CSE.
5. Finally, NSIRA used information gathered during this review to make comments about the working relationship between CSE and CSIS.
6. The period under review ranged from January 1, 2016 to September 30, 2021, although information outside this period was also considered as necessary.

¹ The statistics that are generally included in NSIRA's annual review of CSIS TRMs are not a part of this review but will be included in NSIRA's Public Annual Report.

Methodology

7. Throughout its review, NSIRA employed a wide range of methods, including document review, briefings and technical demonstrations, direct and proxy access to systems and repositories, and interviews with specific CSE and CSIS employees.

Review Statements

8. NSIRA found that overall, its expectations for responsiveness from CSE during this review were **not met**. CSE delayed responding to NSIRA information requests and challenged NSIRA's access to information. CSE made improvements in the review's final stages including by facilitating candid and open participation of CSE operational staff.
9. NSIRA found that the requirements for the verification of requested CSE information for this review were **partially met**. CSE facilitated technical verification sessions for NSIRA staff, with the ability to test information and statements provided over the course of the review in certain CSE repositories and systems. While NSIRA was satisfied with CSE's facilitation of the verification exercise, some of the results of the queries performed by NSIRA did not align with the information provided by CSE.
10. NSIRA found that overall, its expectations for responsiveness by CSIS during this review were **met**. While there were some delays with CSIS's provision of information, CSIS liaison representatives and all operational staff with whom NSIRA engaged were professional, candid, and transparent. CSIS often proactively provided relevant information that allowed NSIRA to obtain the facts and contextual information it needed to support its review.
11. NSIRA found that the requirements for the verification of requested CSIS information for this review were **met**. NSIRA had direct access to CSIS systems and repositories, and, therefore, was able to corroborate information in real time. As well, documentation within repositories supported statements made to NSIRA by CSIS staff in briefings and interviews.

2. BACKGROUND

12. As NSIRA's predecessor agencies did not have mandates that allowed for review across multiple government departments, this is the first review of CSE and CSIS collaboration that was able to access information from both departments and examine collaboration from both perspectives. It is also the first review of CSE-CSIS

collaboration outside CSE's assistance mandate, examining collaboration in operations wherein CSE and CSIS work together under their respective mandates.

13. The ability to consider both departments' activities in tandem outside of the assistance mandate is important given the tension between CSIS's mandate, which authorizes collection and sharing of information about Canadians, and CSE's core prohibition against directing its activities at Canadians under section 22(1) of the CSE Act. When CSE is assisting CSIS under its assistance mandate, this distinction does not apply as it operates under CSIS's authorities. However, the distinction does matter in other instances of operational collaboration. As such, this review was the first to assess the significant compliance risks stemming from CSE and CSIS's differing powers and restrictions.

3. FINDINGS, ANALYSIS, AND RECOMMENDATIONS

Collaboration in Operations

14. CSE and CSIS collaborate under two main mechanisms: (1) CSIS requests for assistance (RFAs), and (2) what NSIRA will refer to as joint operations. NSIRA conducted a detailed review of two operations conducted under RFA and one joint operation.

Requests for Assistance

15. CSE's assistance mandate is outlined under section 20 of the CSE Act, which authorizes CSE to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Armed Forces, and the Department of National Defence. In undertaking this assistance, section 25(1) of the CSE Act provides CSE with the same authority as the agency requesting assistance and renders CSE subject to the same limitations imposed on the requesting agency, including those set out in warrants.
16. CSE policy governs the assistance aspect of CSE's mandate, including assistance to CSIS. This policy requires that CSIS complete RFA forms that include details of the lawful authorities under which the request is made, including warrants or other documents clarifying authorities, and the scope of activities being requested. CSE policy requires an operational plan be drafted to translate these requests into "feasible operational activities".

- 17. Finding 1: NSIRA found that CSE does not routinely share its operational plans and associated risk assessments with CSIS when operating under CSIS authorities. This may leave CSIS unable to fully assess CSE's activities for compliance.**
18. According to CSE policy, its operational plans drafted further to an RFA must consolidate all authorities and stakeholders, define the permissible activities, outline roles and responsibilities, and establish mandatory processes. In practice, these plans contain details of the precise actions CSE will undertake to satisfy the RFA, and the mechanism by which warrant conditions will be respected. Further, certain operational plans also articulate actions CSIS will take throughout the operation. As part of the planning process, CSE must also assess the risks of the requested activities.²
19. CSE does not routinely provide their operational plans or risk assessments to CSIS. Without access to these documents, CSIS may not be able to confirm whether CSE actions comply with CSIS authorities as it may not be privy to, or have a record of, the precise actions CSE plans to undertake under the RFA. Furthermore, when operational plans account for activities to be conducted by CSIS in support of the assistance, a failure to share this document could culminate in a misunderstanding of roles and responsibilities.
20. In September 2022, CSIS noted that the current RFA system is often plagued with delays as the departments struggle to determine whether the technology that CSE proposes to use is compatible with the enabling CSIS authority. Sharing proposed CSE operational plans at the outset would serve to bolster CSIS's understanding of CSE's technologies and allow CSIS to comment on the proposed technologies. This may further reduce delays by allowing CSIS to develop precedent on CSE technologies and their relationships to CSIS authorities.

Recommendation 1: NSIRA recommends that CSE share its operational plans and associated risk assessments with CSIS prior to operating under CSIS authorities.

² CSE's Assistance policy suite notes CSE must assess operational risk, feasibility, and resources, however it does not further define this assessment. As a comparison, CSE's Foreign Intelligence policy suite notes that CSE risk assessments assess legal, reputational, partnership, and operational risks. For its part, CSIS assesses four pillars of risk, they are: legal, operational, foreign policy, and reputational.

15(1)

TOP SECRET//SI//CEO

CASE STUDY: Operation [REDACTED] Warranted Section 12 Investigation

16(1)(c)

21. Operation [REDACTED] (see Annex A), carried out under sections 12 and 21 of the *Canadian Security Intelligence Service Act* (CSIS Act), was designed to collect intelligence on [REDACTED]. After obtaining a Federal Court warrant, CSIS submitted an RFA to CSE to conduct SIGINT collection on the target, [REDACTED].

15(1)(f)

22. **Finding 2: NSIRA found that close collaboration at the working level created the right conditions for CSIS to monitor CSE's assistance activities for compliance with warrant conditions.**

23. The warrants that authorized CSIS [REDACTED] required that CSIS verify [REDACTED] before a full collection of information could happen. To conduct [REDACTED] CSIS has a standard [REDACTED] collection procedure, [REDACTED].
[REDACTED] When CSIS has reasonable grounds to believe [REDACTED] [REDACTED] the full collection of information [REDACTED] can proceed. The warrant requires that this review be conducted by a "designated Service employee."

16(1)(b)

24. In this case, as CSIS's [REDACTED] procedure differed from CSE's standard approach to [REDACTED]³, CSE and CSIS engaged in detailed communications so that CSIS could confirm warrant conditions were respected. Further, to fulfill the "designated Service employee" requirement, a CSIS employee physically attended CSE premises to review collected [REDACTED] and confirm that there were reasonable grounds to believe that [REDACTED].

15(1)(f)
16(1)(b)

25. Additional in-depth communication and cooperation between operational teams that reinforced compliance was evident. For example, the RFA required that before [REDACTED] CSE had to obtain written permission from the CSIS designated employee. This practice compelled regular and consistent communication between the two departments that assisted in ensuring warrant conditions were respected.

16(1)(b)

³ [REDACTED]

15(1)

TOP SECRET//SI//CEO

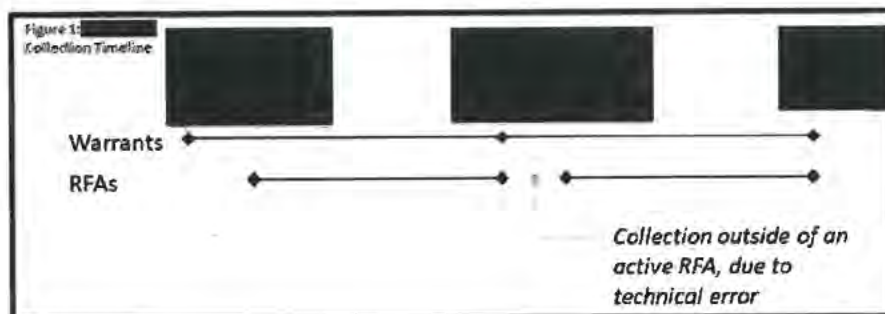
Recommendation 2: NSIRA recommends that when CSIS engages CSE for assistance with the execution of warranted powers, a CSIS employee be involved to ensure compliance in CSE's collection activities until the request for assistance has terminated.

26. **Finding 3:** NSIRA found that CSIS failed to submit an updated request for assistance to CSE in a timely manner when it sought new warrant powers.
27. **Finding 4:** NSIRA found that CSE and CSIS did not engage in any joint investigation, assessment, or tracking of a compliance incident.
28. A failure to ensure that a new RFA was approved when a new warrant was issued led to a compliance incident on CSE's part, and loss of intelligence collection on CSIS's part.

15(1)(d)

29. CSIS obtained warranted powers on the target valid from [REDACTED] to [REDACTED] and then subsequently from [REDACTED] to [REDACTED]. After receiving the initial set of warrants, CSIS submitted an RFA to CSE that was valid until the warrants' expiry on [REDACTED]. When CSIS obtained the second set of warrants, it failed to provide CSE with an updated RFA until [REDACTED]. This meant that while a warrant existed for collection on the target, CSE did not have an active RFA in place authorizing it to collect on the target between [REDACTED] and [REDACTED].
30. CSE experienced a compliance incident with respect to the initial RFA. The CSIS warrants allowed for requests to foreign partners to collect on the target while they were outside Canada. Such a request was made to [REDACTED] SIGINT collection agency, [REDACTED]. [REDACTED] CSE explained that despite having submitted a request to cease collection at the expiry of the first set of warrants, [REDACTED] tools used for this collection at the time were experiencing technical issues that it suspects caused the incident.

16(1)(c)



15(1)

TOP SECRET//SI//[REDACTED]//CEO

31. While a valid warrant existed at the time of [REDACTED] collection, as an RFA was not in place to cover these dates, CSE submitted a request to have the collected information purged from relevant systems, with a CSIS employee copied on the correspondence. According to CSE, this was the only means by which CSIS was informed of the incident and CSE's response. CSIS indicated that it had no record of any compliance incidents on the file and that no evidence exists that any investigation of the compliance incident took place independently by CSIS or concurrently between CSIS and CSE.

Recommendation 3: NSIRA recommends that CSIS develop a process to ensure that necessary requests for assistance are submitted to CSE in a timely manner subsequent to obtaining warrant powers.

Recommendation 4: NSIRA recommends that when working under a request for assistance CSIS and CSE develop a framework for joint investigation of potential compliance incidents.

16(1)(c)

15(1)(d)

CASE STUDY: Operation [REDACTED] Warranted Section 16 Operation

32. Operation [REDACTED] (see Annex A) was carried out under section 16 of the CSIS Act. After obtaining a Federal Court warrant, CSIS submitted an RFA to CSE,

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

33. **Finding 5:** NSIRA found that CSE and CSIS failed to implement an effective operational framework for their collection activity. This contributed to two instances of non-compliance with the Federal Court's direction.

34. The Federal Court authorized [REDACTED] [REDACTED] warrant [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] the Federal Court authorized the operation with the direction that [REDACTED] [REDACTED]

15(1)

TOP SECRET//SI//CEO

15(1)(d)

[REDACTED]
[REDACTED]
[REDACTED] it was permitted to ask
permission [REDACTED] . However, [REDACTED] not
permitted [REDACTED]
[REDACTED]

35. However, on two occasions, [REDACTED] leading to compliance incidents with the CSIS warrant. These incidents can largely be attributed to a disconnect in CSE and CSIS's understanding of the authority granted by the Federal Court. These compliance incidents have been briefed to the Federal Court.

36. The issues underpinning the compliance incidents began in [REDACTED]. CSIS informed the Court [REDACTED] CSE misunderstood this to mean [REDACTED] now permitted to [REDACTED] for its own [REDACTED] intelligence purposes. CSE communicated this [REDACTED] without CSIS's knowledge. CSIS understood correctly that this new process had no impact on [REDACTED] for its own [REDACTED] intelligence mandate.

15(1)

37. This difference in interpretation went unnoticed by the departments for almost [REDACTED]. It was not until [REDACTED], when CSE shared with CSIS a summary of [REDACTED] that CSIS realized CSE was operating under a false understanding of the authorities.

16(1)(c)
15(1)(d)

38. During the period under review, the only materials to govern [REDACTED] were the initial RFA seeking CSE's assistance, a [REDACTED] CSE operational plan, [REDACTED] CSE's operational plan was not shared with CSIS and CSIS did not draft any other policy instrument to guide the operation. Further, there was no formal agreement in place between CSE, CSIS, [REDACTED] setting out the procedures to govern the execution of [REDACTED]

15(1)(d)

39. Absent a written agreement, all practical arrangements concerning this operation were made via correspondence at the working level. With the exception of initial communications in [REDACTED], working level communications with [REDACTED] excluded CSIS. CSE managed [REDACTED], which meant that CSIS was not privy to the majority of the practical conversations that guided exactly how its warrant powers would be executed. Reliance on this *ad hoc* working

15(1)

TOP SECRET//SI//CEO

level correspondence and decision making⁴ resulted in knowledge gaps and ultimately non-compliance caused by confusion as the operation evolved.

- 16(1)(c) 40. Given the complexity of this operation [REDACTED], a
15(1)(d) written [REDACTED] agreement coupled with CSIS's involvement in day-to-day communications [REDACTED] [REDACTED] may have provided an early awareness of, and ultimately guarded against, non-compliance with CSIS's warranted authorities.
41. Since the end of the period under review, an agreement between CSE, CSIS, [REDACTED] [REDACTED] to govern [REDACTED] [REDACTED] was in development.

Recommendation 5: NSIRA recommends that CSIS ensure roles and responsibilities are clearly agreed to prior to allowing partners to execute warrant powers. Where appropriate, these agreements should be shared with the Federal Court.

Recommendation 6: NSIRA recommends that CSIS ensure it is directly involved in all substantive communications with any partner actively executing its warrant powers.

Recommendation 7: NSIRA recommends that CSIS share paragraphs 32 through 41 of this review, along with associated recommendations, with the Federal Court.

Joint Operations

42. CSE and CSIS carry out joint operations wherein both departments work in parallel against common threats under their respective mandates and associated legislative authorities. Circumstances surrounding joint operations often involve interdependencies that make operations possible only through collaborative activity.

⁴ CSE staff partially attributed their error in understanding of the reporting requirements to an employee turnover; those responsible for running the operation were different from those involved in planning an obtaining initial warrant powers.

15(1)

TOP SECRET//SI//CEO

CASE STUDY: Operation [REDACTED] Operation

- 16(1)(c) 43. In operation [REDACTED] (see Annex A), CSIS wanted to identify [REDACTED]
15(1) [REDACTED] To do so, it [REDACTED]
[REDACTED]
[REDACTED]
- 15(1)(d) 44. CSE leveraged the CSIS operation and, using its own foreign intelligence powers,
15(1)(f) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
45. **Finding 6: NSIRA found that CSE and CSIS identified an effective opportunity to collaborate under their respective mandates and carried out an operation that proved beneficial for both Canada and its allies.**
- 16(1)(c) 46. Operation [REDACTED] proved beneficial for both CSE and CSIS, and represents an example of the departments appropriately identifying an opportunity, and executing an operation, that addressed a common threat actor by applying their own legislative powers in a complementary way. This operation contributed to CSIS's ability to
15(1)(d) identify [REDACTED] and enabled CSE to publish [REDACTED] intelligence reports concerning the threat. CSE authorized CSIS to undertake [REDACTED] actions stemming from their intelligence reports, largely consisting of information sharing with foreign partners, further demonstrating the value of the intelligence acquired.
47. **Finding 7: NSIRA found that, while CSIS's operational framework was sufficient, CSE's operational framework did not assess legal and policy risk specific to the operation.**
- 16(1)(c) 48. CSIS had a robust governance structure supporting [REDACTED] For each round of activity, CSIS had an approved operational plan accompanied by a risk assessment that reflected the specific facts. [REDACTED]
15(1) [REDACTED]
[REDACTED]
- 16(1)(c) 49. Conversely, CSE used a combination of instruments to govern its participation in
15(1)(d) [REDACTED] Governing the operation was a [REDACTED] Intelligence Requirement Disclosure (IRD) provided to CSIS, which highlighted CSE's intent to [REDACTED]
[REDACTED]
The IRD did not identify specific targets of interest, but noted that "it is understood

TOP SECRET//SI//CEO

15(1)

that operational plans for each new target(s) would be drafted according to the applicable policies/procedures.”⁵

- 16(1)(c) 50. CSE did not draft new operational plans specific to the activities being performed as
15(1)(d) part of [REDACTED] Rather it relied on an umbrella operational project approval for [REDACTED]

While CSE developed technical risk mitigation measure for a subset of the rounds it was involved in, it did not have a governing document that assessed overall risk and compliance. No risk assessments were performed and no legal advice was obtained specific to this operation.

- 16(1)(c) 51. While the use of umbrella approvals may be appropriate in some circumstances, in [REDACTED] it did not allow CSE to properly consider the elevated risk specific to this operation. CSE’s umbrella approval also did not identify mitigation measures to reduce the risk of targeting Canadians, and simply noted “target pursuit will be located outside of Canada,” without specifying measures to ensure this.

- 15(1)(d) 52. CSIS clearly articulated the presence of Canadians in the operation as part of its proposal for the activity to CSE, stating that “the Service is closely monitoring the activities of [REDACTED] Canadians [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] With this information, it is clear that there was an elevated risk of CSE targeting a Canadian contrary to its prohibition on directing its activities at Canadians, solely through its participation in this operation. Therefore, a specific operational plan and risk assessment would have been appropriate. Instead, the use of its umbrella approval in this case meant that CSE participated in an operation initially designed to identify Canadian threat actors without seeking specific legal or policy advice.

Recommendation 8: NSIRA recommends that when CSE engages in joint operations with CSIS it should perform risk assessments for each operational activity. These should specifically consider the risk of targeting Canadians and implement proactive measures to mitigate this risk.

⁵ CSE policy does not identify the intended or required use of the IRD. A caveat found on the IRD itself notes that the information is being disclosed as contextual knowledge pertaining to a national intelligence priority under CSE’s mandate, and as such this document appears to be simply used to flag an intelligence gap CSE believes CSIS may be able to assist with.

15(1)

TOP SECRET//SI//CEO

53. Finding 8: NSIRA found that CSE and CSIS did not draft joint terms of engagement, a joint operational plan, or engage in joint risk assessments.

54. CSIS does not have policies or procedures specific to collaboration with CSE or other departments that guide its operational planning or risk assessment requirements.

55. For its part, CSE policy requires it to develop written terms of engagement when it conducts joint operational activities with partner organizations. These must include an assessment of the overall risk of the operation, an outline of roles and responsibilities, and an overview of mechanisms to protect, share, and legally disclose sensitive information. CSE policy also recommends that CSE and the partnering department create collaborative rather than concurrent operational plans and risk assessments. When this is not feasible, it recommends that the departments exchange their respective assessments and operational plans.

16(1)(c) 56. There is no evidence that any of the operational procedural documents utilized for [REDACTED] were exchanged between the two departments, nor any evidence of the terms of engagement required by CSE policy.

15(1)(d) 57. The lack of document exchange created a situation that could have resulted in knowledge and awareness gaps. For example, CSE's technical risk mitigation charts allocated full responsibility to CSIS for [REDACTED] of the [REDACTED] measures involved in the operation, and partial responsibility for another [REDACTED]. No written record exists that CSE informed CSIS of these responsibilities, or confirmed CSIS was willing or capable of undertaking the relevant measures.

58. Joint planning and risk assessment, or at minimum, sharing these planning documents, is important when CSE and CSIS are cooperating under their respective mandates. Given the potential for increased cumulative risk of operations involving multiple departments with different authorities, restrictions, and operational practices, it is key the departments are planning collaboratively and adequately communicating with each other.

Recommendation 9: NSIRA recommends that when participating in joint operations, CSE and CSIS either jointly develop or share written terms of engagement, operational plans, and risk assessments.

59. Finding 9: NSIRA found that CSE's foreignness assessment did not account for the increased risk of targeting Canadians when working with CSIS.

15(1)

TOP SECRET//SI//CEO

- 15(1)(f) 60. CSE's policy requires that a foreignness assessment be conducted to determine that the user of the device at issue is not Canadian or located in Canada. The foreignness assessment must be conducted by CSE personnel responsible for querying or targeting as close to commencing the operation as possible and as required once the activity has been approved. It also notes that the foreignness assessment must meet the threshold of reasonable grounds to believe and must consider the fact that [REDACTED] may not reflect the foreign status of a target.
- 16(1)(c) 61. When conducting a foreignness assessment against a group of persons, CSE policy
15(1)(d) notes that assessments should attempt to ensure that each individual in the group is not a Canadian or a person in Canada.
- 16(1)(c) 62. For its foreignness assessment in [REDACTED] CSE explained that it primarily relied
15(1)(d) on CSIS's verbal briefing that [REDACTED] contained a large proportion of [REDACTED], despite CSIS having advised that Canadians were likely to be found in [REDACTED]. Beyond this, CSE explained that to assess foreignness, it built filters into [REDACTED].
- As a final step, CSE noted that it monitored collection [REDACTED] to ensure they were only [REDACTED] foreign individuals.
- 16(1)(c) 63. This foreignness assessment performed by CSE in [REDACTED] cannot be
15(1)(d) considered to meet its policy requirements. The [REDACTED] filters applied by CSE, [REDACTED] do not necessarily reflect nationality or location as noted in CSE's policy. Further, CSE's reliance on CSIS's statement about the composition of [REDACTED] does not meet the requirement that CSE personnel conduct the assessment to determine that each [REDACTED] is not Canadian.
- 15(1)(f) 64. The only means of truly assessing foreignness in this operation occurred [REDACTED] in the final step where CSE reviewed collected information. CSE cannot rely on after the fact foreignness assessments to satisfy its proactive policy obligations.

Recommendation 10: NSIRA recommends that CSE perform foreignness assessments that account for the increased risk of targeting Canadians when working with CSIS.

Collaboration in Information Sharing

65. This review focused on two methods of information sharing: (1) lead information messages and (2) the exceptional reporting loop. This review also considered steps taken by CSE to protect Canadian information shared by CSIS within these two processes.

Lead Information Messages

16(1)(b)

66. CSIS Lead Information messages (CLIs) and Foreign Intelligence Lead Generation Information (FILGIs) are the means by which CSIS shares intelligence it believes may be of value to CSE's foreign intelligence mandate. In addition to providing lead information, CSIS uses these messages to request information from and/or action by CSE. CLIs are generally sent in a [REDACTED] and FILGIs in [REDACTED] files. For ease of reference, NSIRA will refer to both kinds of messages as CLIs.

67. CLIs are emailed from CSIS analysts directly to CSE analysts. Upon receipt, CSE chooses how to act on the intelligence, including whether to pursue any further action based on the lead information. At CSIS, CLIs are saved in a single corporate repository, however, at CSE they are not.

68. NSIRA assessed a sample of 25 CLIs and has viewed a wide range of others to confirm the routine nature of this exchange. The content of CLIs varied widely. Some CLIs exclusively contained foreign intelligence leads with no Canadian nexus, while others exclusively contained information about Canadians or made requests for further information about Canadians.

69. Both the CSIS Act and the CSE Act govern the disclosure, acquisition, and use of the information contained in CLIs. CSIS shares this type of information pursuant to section 19(2) of the CSIS Act, which enables it to disclose information for the purposes of the performance of its duties and functions. Section 16 of the CSE Act permits CSE to collect foreign intelligence using a range of sources and methods, and it relies on this section to utilize the information contained in the CLIs.

70. While CSE is prohibited from directing its activities at Canadians, section 23(4) of the CSE Act does permit CSE, in certain circumstances, to incidentally acquire information about Canadians. Incidental collection occurs when information was not deliberately sought and the information-acquisition activity was not directed at the Canadian or person in Canada. By using this provision, CSE is able to acquire the information about Canadians shared by CSIS via the CLI process.

71. **Finding 10: NSIRA found that both CSE and CSIS lack policies, procedures, and accountability mechanisms to govern CSIS lead information messages and associated requests and actions.**
72. **Finding 11: NSIRA found that CSIS's use of lead information messages to share information and make requests about Canadians creates a high risk of potential for non-compliance for CSE.**
73. CSIS does not have policies, procedures, or any other type of guidance for analysts developing and sharing CLIs with CSE.
74. CSE policy provides high-level guidance for receiving disclosures from GC entities. However, this policy does not specifically outline parameters of how to deal with Canadian information received via CSIS disclosures, nor does it detail what actions CSE analysts can take with respect to this information, provide standardized structure to govern responses to CLIs, or require any record keeping of activity undertaken further to a CLI.
75. This is particularly problematic as the CLI process is sometimes used by CSIS for the purposes of sharing or gathering information about Canadians, placing CSE at a high risk of non-compliance depending on how it chooses to use the lead information.
76. Currently, individual CSE analysts are responsible for identifying what can and cannot be done with Canadian information. If they are unsure, they are responsible for taking the initiative to seek advice from CSE's policy unit, who themselves lack necessary policy to reference. This leads to inconsistency and risks incidents of non-compliance.
77. In two of the CLIs reviewed by NSIRA, CSIS provided CSE with foreign selectors and information about Canadians located abroad. In both cases, CSIS was interested in knowing whether CSE was aware of contacts between the foreign selectors and selectors believed to belong to the Canadians. In one, CSIS also asked CSE to confirm whether the suspected Canadian selectors actually belonged to or were being used by the Canadian.
78. In these cases, the CSE team correctly identified that to action CSIS's request could constitute reverse targeting activities, where CSE performs investigative SIGINT activities on foreign targets for the purposes of obtaining information about a Canadian in contact with the foreign target. CSE has acknowledged that such activities are equivalent to directing activities at Canadians and are, therefore, not compliant with its legislation.

79. The CSE team in these cases sought policy advice. The policy unit responded that the team would be permitted to perform contact chaining analysis⁶ on the foreign targets of interest as long as activities ceased if they led to a Canadian. This advice relied on the premise that "there is no real intent to gather information about the CDN contact; merely to gather more FI on the original valid target."
80. CSE did not articulate another legitimate foreign intelligence motive for conducting contact chaining on the foreign selectors. As such, the intent of the proposed activity appears to be to respond to the request in the CLI; namely, to determine contact between the foreign selectors and Canadian selectors. This would have constituted reverse targeting even if CSE stopped once a Canadian contact was identified.
81. Upon NSIRA's inquiry into the matter, CSE rescinded both pieces of policy advice, determining that it had been incorrect. CSE further confirmed that no activities were performed in relation to the CSIS requests.
82. These cases demonstrate the risk that currently exists with the lack of policies and procedures in place with respect to CLIs. Even when analysts properly identified issues and sought advice, the lack of policy and standard operating procedures for managing Canadian information found in CLIs could have resulted in non-compliance. CSE needs a policy framework in place with respect to CLIs. This framework should outline a structure to respond to CLIs that accounts for what CSE analysts can and cannot do with Canadian information, requires appropriate oversight, and properly safeguards against reverse targeting requests. Operating procedures should also require thorough reporting and tracking mechanisms to document exactly how CSE analysts act in response to CLIs, as well as their foreign intelligence intent for conducting any follow-on activities.

Recommendation 11: NSIRA recommends CSIS cease making requests for action and/or further information to CSE in relation to Canadians or people in Canada via CSIS lead information messages.

Recommendation 12: NSIRA recommends that CSIS develop policies, procedures, and analyst training to standardize the disclosure of CSIS lead information messages to CSE.

⁶ Contact chaining involves the analysis of a selector to determine the nature of the user's communications. Contact chaining does not yield the actual content of the communications, only contact identifiers, duration, and time of communication events.

Recommendation 13: NSIRA recommends that CSE develop policies, procedures, and analyst training to standardize the use of CSIS lead information messages.

83. Finding 12: NSIRA found that CSE's application of incidental collection provisions may not be appropriate in situations where CSE knows there is a Canadian nexus to a CSIS foreign intelligence lead, and where it knows it is likely to collect Canadian information in pursuing the lead.

16(1)(c)

84. In a third CLI reviewed by NSIRA, the CSE analyst receiving the CLI did not obtain legal or policy advice prior to taking action on the information disclosed by CSIS. In this case, CSIS provided CSE with a CLI containing [REDACTED] [REDACTED] CSIS also noted that [REDACTED] believed to be in contact with Canadian [REDACTED] CSIS requested, via the same CLI, that CSE ask the foreign SIGINT partner to release a report with [REDACTED] Canadian [REDACTED] so that CSIS could make a request to obtain them.

85. Four days after receiving the disclosure, CSE generated an intelligence report in response to the CLI which noted that [REDACTED] in the CLI [REDACTED] in contact with [REDACTED] Canadian [REDACTED]. CSIS obtained [REDACTED] Canadian [REDACTED] by submitting a request for disclosure of Canadian identifying information. The report named [REDACTED] and identified [REDACTED] contact events. The report does not include the contents [REDACTED] Canadian [REDACTED] or [REDACTED]. This suggests that contact chaining was performed by CSE, potentially for the purposes of identifying [REDACTED] Canadian [REDACTED].

86. While directing activities against [REDACTED] would have been permissible under the foreign intelligence mandate, any attempts to specifically identify the Canadian [REDACTED] known to be in contact with would amount to reverse targeting, as discussed above. CSE advised that their activity pursuant to the CLI was entirely focused on [REDACTED] with the intent of [REDACTED] [REDACTED] that the discovery of the Canadian information was incidental. However, the report's focus on the Canadian contact events with no additional foreign intelligence calls this explanation into question and

15(1)

TOP SECRET//SI/[REDACTED]//CEO

suggests reverse targeting may have taken place. Absent a formal tracking system that documents CSE analyst actions and supporting rationale in response to CLIs, CSE cannot demonstrate no reverse targeting took place and NSIRA cannot confirm the rationale for the CSE activity.

87. CSE's incidental collection provisions may be insufficient to manage the collection, retention, and reporting of Canadian information in similar scenarios. Incidental collection occurs when the Canadian information was not deliberately sought and the information acquisition activity was not directed at the Canadian or person in Canada. These provisions are most often used by CSE when, in the process of conducting foreign intelligence activities, it discovers specific Canadian information or information about Canadians that was previously unknown. In some CLIs, CSIS shares a foreign intelligence lead with CSE and may highlight a distinct Canadian link. When CSE pursues this lead, the Canadian information may not be deliberately sought but CSE is aware of its existence. It is, therefore, insufficient to treat the use, retention, and reporting of this Canadian information in the same manner. This is particularly true when CSE is alerted to the existence of the Canadian information by CSIS, and reports the Canadian information back to CSIS, which would otherwise generally require a warrant to collect Canadian information of the same nature.
88. CSE requires a regime that allows it to conduct legitimate foreign intelligence activities in response to CLIs in a manner that protects previously known Canadian information. Without this, CSE and CSIS run the risk of collaborating to collect information not otherwise allowed by their respective mandates, and which is protected under the *Canadian Charter of Rights and Freedoms*.

Recommendation 14: NSIRA recommends that CSE develop a regime for collecting, retaining, and reporting to CSIS Canadian information it uncovers further to legitimate foreign intelligence activities where it has advance knowledge of the Canadian information.

15(1)(f) **CASE STUDY: Non-Compliance with the Law – CSE Analyzes [REDACTED] of a Canadian's Device**

15(1)(f) **89. Finding 13: NSIRA found that CSE did not comply with section 22(1) of the CSE Act when it analyzed [REDACTED] of a Canadian's device obtained through a CSIS lead information message.**

15(1)

TOP SECRET//SI//CEO

- 15(1)(d) 90. In one case reviewed by NSIRA, CSIS sent a CLI to CSE that contained [redacted] of the contents of a Canadian's [redacted] device. The Canadian was the subject of a CSIS warrant and had been [redacted] authorities due to involvement in [redacted] activities.
- 15(1)(f) [redacted] authorities [redacted] of the individual's [redacted] [device] and shared it with CSIS, which in turned shared it with CSE via a CLI.
- 15(1)(d) 91. The CLI indicated the individual's [redacted]
15(1)(f) [redacted] The CLI further explained how CSIS acquired [redacted] of the device, indicated that the individual was currently the subject of CSIS investigation, and stated that [redacted] of the individual's device was being provided for "analytic and lead generation purposes".
- 15(1)(f) 92. CSE relied on its foreign intelligence mandate to ingest the CLI and [redacted] of the Canadian's device and to analyze the information found within. The analysis did not yield anything of foreign intelligence value and CSE subsequently deleted the data.
- 15(1)(f) 93. As CSE's prohibition against directing its activities at Canadians applies in this case, CSE provided two arguments to NSIRA to justify analyzing the information despite [redacted] originating from a Canadian's device. First, it noted that [redacted] had been lawfully obtained by CSIS, stating that [redacted] ...it received [redacted] of the content of the device, that was legally obtained by CSIS and disclosed to CSE." Second, CSE stated that it analyzed [redacted] of the device in order to identify information of foreign intelligence interest and the Canadian information found in the device was incidental.
94. CSE's policy notes that to respect the "directed at" prohibition, foreign intelligence activities must be directed at foreign persons and entities outside of Canada. It indicates that both analysis and evaluation of data for foreign intelligence value are considered SIGINT production activities and further confirms that operational analysis must not be directed at Canadians or persons in Canada. The policy is clear that these provisions apply to information collected by CSE activities and to data or information disclosed to CSE by a GC department for use under the foreign intelligence aspect of CSE's mandate.
95. With respect to disclosures specifically, CSE's policy indicates "where a foreign nexus is not evident in disclosed information (e.g. when the information is that of a Canadian or of a person in Canada), CSE must ensure that the disclosing entity clearly explains the foreign intelligence value in writing". As noted above, in this case the CLI only indicated that the information was being provided for "lead generation and analytic purposes" and did not articulate a specific foreign intelligence value.

TOP SECRET//SI/[REDACTED]//CEO

NSIRA saw no evidence of CSE requesting this information from CSIS. Further, the general inclusion of "when the information is that of a Canadian or a person in Canada" contradicts the notion that operational analysis must not be directed at Canadians or persons in Canada. This example is inappropriate to include in this section of the CSE policy without requiring the information to fit into the narrow exceptions that allow CSE to retain Canadian information, as described below.

15(1)(f) 96. In this case, CSE conducted SIGINT production activities (specifically, operational analysis) [REDACTED] of the device. As this device belonged to a Canadian, CSE's actions were directed at a Canadian. It is irrelevant that the actions were intended to produce information of foreign intelligence interest, or that the information was initially legally obtained by CSIS.

97. There are two circumstances in which CSE is permitted to acquire and/or use Canadian information under their foreign intelligence mandate. In the first, CSE's policy, citing section 46 of the CSE Act, permits certain use, analysis, and disclosure of information relating to a Canadian or person in Canada in its possession in circumstances where there are reasonable grounds to believe that there is imminent danger of death or serious bodily harm to any individual and that the information will be relevant to the imminent danger. CSE did not provide any information to suggest such circumstances applied in this case.

15(1) 98. The second circumstance is incidental collection. However, information cannot be considered incidentally collected if it was collected by an activity that was directed at a Canadian. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

15(1)(d) 99. Although legal advice was not sought in relation to [REDACTED] of the Canadian's
15(1)(f) device, [REDACTED]
CSE was not permitted to use [REDACTED] Canadian's device as a starting point to identify information of foreign intelligence interest as [REDACTED] device could reasonably be expected to contain [REDACTED] information that could not be seen to be incidentally collected.

100. In response to NSIRA's concerns on this case, CSE stated the following:

TOP SECRET//SI//CEO

15(1)

Canada's national security legislation is intended to not leave knowledge gaps between Canada's security agencies and to ensure that foreign and domestic threats are dealt with by the appropriate agency and in a seamless way. The inability of CSE to acquire and use information of FI value that has been lawfully obtained by CSIS through lawful activities directed by that agency against a Canadian could create a gap with severe implications for Canada's national security.

101. This response fails to consider the context of this situation. CSE may acquire and use information of foreign intelligence value that has been lawfully obtained by CSIS, even if obtained by CSIS directing its activities at a Canadian, as CSE suggests in the above. The compliance issue in this case was that CSE itself conducted the analysis on Canadian information (i.e. directing its activities at a Canadian) in order to identify information of foreign intelligence value and attempted to then justify this action as incidental collection. To render this compliant, the analysis of the Canadian information would have needed to be done by CSIS prior to disclosure as opposed to by CSE post-disclosure. This is an important distinction that differentiates this case from legitimate instances of CSE's analysis of CSIS disclosures.

15(1)(f)

102. As articulated in CSE policy, CSIS's (or other GC departments') legal authorities to disclose do not create corresponding authorities for CSE to analyze, and CSE's intent to discover foreign intelligence information does not relieve it of its responsibility to not direct its activities at Canadians. When operating under its foreign intelligence mandate, CSE's actions further to all CLIs must be consistent with its own authorities and applicable restrictions. In this case, CSE's analysis of [REDACTED] of the Canadian's device contravened section 22(1) of the CSE Act.

15(1)(f)

103. Further to the above, CSE stated that it "acknowledges the perception of this anomalous activity of receiving a file containing [REDACTED] of the content of a Canadian's device [and] has since made a policy decision to not look into this particular kind of file." CSE did not provide any policy documentation to support this statement.

Recommendation 15: NSIRA recommends that CSE update its policies to prohibit the analysis of information relating to a Canadian or person in Canada for the purposes of identifying foreign intelligence.

Exceptional Reporting Loop

104. NSIRA reviewed the process by which CSIS receives and shares exceptional reporting with CSE. NSIRA will refer to this process as the exceptional reporting loop.
105. When foreign SIGINT partners produce reporting derived from directly targeting Canadians, CSE and CSIS refer to the resulting reports as exceptional reports. The Five Eyes partnership involves a long-standing unwritten agreement that members will not target one another's citizens using SIGINT activities. However, as each country remains a sovereign nation, it is understood that they may, on an exceptional basis, target members' citizens if needed to respond to urgent threats.⁷ The resulting exceptional reporting is of interest to CSIS given that a Canadian is involved and therefore a nexus to the security of Canada likely exists.
106. Prior to 2014, SIGINT partners shared exceptional reporting directly with CSIS. However, due to [REDACTED] at CSIS it was determined that under RFA, CSE could act as a conduit between foreign SIGINT partners and CSIS. Under this RFA, known as [REDACTED] SIGINT partners provide exceptional reports directly to CSE either through CSE's intelligence reporting software, SLINGSHOT, or via other secure communications methods. CSE then grants CSIS staff access to the exceptional reports within SLINGSHOT. After [REDACTED] deemed success by the departments, [REDACTED]
107. Under the RFAs, CSE has also been provided the authority to review the reports for foreign intelligence value. CSE may then request that CSIS disclose the reports containing information of foreign intelligence value back to CSE. At this point in the process, CSIS acts under section 19(2) of the CSIS Act to review the request and decide whether to disclose the exceptional report in its entirety to CSE. CSE, no longer operating under RFA, then receives the disclosure and utilizes the exceptional reporting for foreign intelligence purposes using the powers in section 16 of the CSE Act.
108. Of note, the Office of the Communications Security Establishment Commissioner reviewed the initial implementation of [REDACTED] in 2015 and found the procedure to be compliant with the law. However, the report noted that while CSE analysts were reviewing the exceptional reporting to identify foreign lead information,

15(1)(f) ⁷ [REDACTED] Five Eyes partners target Canadians on an exceptional basis, and subsequently produce exceptional reporting, [REDACTED]
[REDACTED]
[REDACTED]

15(1)

TOP SECRET//SI//CEO

CSIS did not disclose any foreign lead information until after the period under review, so the "reporting loop" was not reviewed at that time.

CASE STUDY: Non-Compliance with the Law – CSE Receives and Utilizes Entire Exceptional Reports

- 15(1)(d) 109. Finding 14: NSIRA found that CSE did not comply with either section 22(1) of the CSE Act or section 273.64(2)(a) of the *National Defence Act* (NDA) when it used [REDACTED] complete exceptional reports for foreign intelligence purposes.
- 16(1)(c) 110. The review period began prior to the enactment of the CSE Act, as such, some of CSE's activities under [REDACTED] were conducted under the authorities of the NDA. Section 273.64(2)(a) of the NDA is the mirror provision to section 22(1) of the CSE Act, which prohibits CSE from directing its activities at Canadians or persons in Canada.
- 15(1)(d) 111. During the period under review, [REDACTED] exceptional reports were transmitted from CSE to CSIS using [REDACTED]. Of these [REDACTED] CSE requested the disclosure of [REDACTED] and received and analyzed all [REDACTED] in their entirety. Some foreign selectors were targeted further to the reports. However, CSE indicated that the exceptional reports primarily "added context" to CSE [REDACTED] investigations.
- 16(1)(c)
- 15(1)(d) 112. CSE stated generally that "Canadian information [found in the exceptional reports] is not used in connection with any SIGINT FI activity." However, it provided no specific confirmation concerning the [REDACTED] reports in question, nor did it detail any mitigating measures used with respect to the Canadian information contained in these reports.
113. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- 15(1)
114. CSE cannot indirectly (via CSIS) obtain reporting that it could not directly obtain from its SIGINT partners, nor can it use this Canadian information as a starting point to advance its foreign intelligence mandate, as noted above. As CSE is not interested in, nor is it authorized to use, the Canadian information contained in the reporting, a more nuanced approach must be taken to enable CSE to obtain information to further its foreign intelligence mandate without violating the prohibition in section 22(1) of the CSE Act. A refined CLI process with necessary protections for any

15(1)

TOP SECRET//SI/[REDACTED]//CEO

Canadian information, as recommended above, would serve as an appropriate means to do so.

Recommendation 16: NSIRA recommends that if CSIS decides to disclose exceptional reporting to CSE, it should extract the relevant foreign intelligence for disclosure as opposed to sending the entire report.

Recommendation 17: NSIRA recommends that CSE cease using complete exceptional reports from CSIS under its foreign intelligence mandate.

Protected Entity Tool

115. For both lead information messages and exceptional reporting, CSE stated that Canadian information it receives can be proactively entered as a "protected entity" within CSE's targeting database. The protected entity tool within the targeting database helps to prevent CSE from targeting Canadians by flagging the identifiers as belonging to a Canadian and blocking any future querying or targeting requests against that identifier.
116. **Finding 15: NSIRA found that CSE does not consistently utilize its protected entity tool to prevent targeting Canadian identifiers it receives from CSIS.**
- 15(1)(f) 117. Canadian information sent by CSIS to CSE via CLIs and exceptional reports was inconsistently entered as a protected entity in CSE's targeting database. [REDACTED] out of [REDACTED] Canadian identifiers provided by CSIS to CSE within NSIRA's sample were either not found within the database, or were not marked as protected entities.
118. CSE policy notes that information relating to Canadians can be used, analyzed, or retained by CSE in certain circumstances, one of which is so that information can be entered into the protected entity database to prevent inadvertent targeting. It further stipulates that queries and targeting actions must be run against the protected entities database to minimize the risk of incidentally collecting Canadian communications. However, there is no explicit policy requirement for Canadian information obtained via disclosure or discovered directly by CSE SIGINT activity to be flagged using the protected entity tool.

15(1)

TOP SECRET//SI//CEO

Recommendation 18: NSIRA recommends that CSE introduce a requirement to always apply the protected entity tool to all Canadian identifiers.

Collaboration in Threat Reduction Measures

119. As part of this review, NSIRA satisfied its annual requirement to review an aspect of CSIS's Threat Reduction Measures (TRMs) carried out under section 12.1 of the CSIS Act.

CSIS Consultation with CSE

120. Under the TRM regime, when CSIS has reasonable grounds to believe that an activity constitutes a threat to the security of Canada, it may take measures to reduce that threat. Section 12.1(3) of the CSIS Act requires that CSIS consult with other federal departments and agencies as appropriate to determine if they are in a position to reduce the threat in question prior to taking action.

121. **Finding 16: NSIRA found that while CSIS performs an initial consultation, it does not routinely pursue further engagement with CSE during Threat Reduction Measure activities that could overlap with CSE activities.**

122. In accordance with the legislative consultation requirement of the TRM regime, which is also codified in CSIS operational policies, CSIS regularly consults and de-conflicts with CSE prior to undertaking TRMs. Multiple measures may be implemented under a single TRM authority. Despite CSE requesting more routine engagement, CSIS's consultation with CSE normally only occurs during the planning and approval stages of a TRM authority. This limits the usefulness of the consultation. NSIRA reviewed three cases that demonstrate this.

16(1)(c)

123. In one case concerning a TRM meant to address [REDACTED], CSE highlighted that certain teams could benefit from a consultation prior to the execution of specific measures. In another case, CSE requested that, prior to implementing a TRM in relation to [REDACTED], CSIS inform CSE of the

15(1)(f)

[REDACTED]
[REDACTED]
[REDACTED] Finally, in a TRM that allowed CSIS [REDACTED]
[REDACTED] against [REDACTED], CSE identified that they had several teams focusing on the same target set and noted it

15(1)

TOP SECRET//SI//[REDACTED]//CEO

would be helpful for them to have advance notice of any potential TRM activity. CSE further noted they may be able to provide validation or other assistance.

124. In the first two cases, CSIS did not pursue any further consultation with CSE, deeming CSE's overall concurrence with the TRM authority to be sufficient. In relation to the [REDACTED] TRM, CSIS did document consultation with CSE in relation to [REDACTED] specific measures, which CSE supported.

125. In order for CSIS to meet their legislative requirement to consult, CSE may need to be aware of specific measures to confirm whether or not they are in a position to reduce the threat. In instances where CSE identified overlaps in both departments' activities, further consultation may also serve to identify opportunities for additional collaboration or assistance, as well as consistency of GC messaging to external partners.

Recommendation 19: NSIRA recommends that CSIS pursue routine engagement with CSE during the implementation of its Threat Reduction Measures when the potential for operational overlap exists.

TRM Coordination with CSE Active Cyber Operation

126. NSIRA examined one instance where a CSIS TRM was used to complement an Active Cyber Operation (ACO) being conducted by CSE under its own mandate.

16(1)(c) **CASE STUDY: Operation [REDACTED]**

127. [REDACTED] CSE undertook an ACO wherein [REDACTED]

15(1)(d)

15(1)(f)

[REDACTED] CSIS conducted a measure under a previously approved TRM authority aimed at [REDACTED]

[REDACTED] CSE and CSIS were both part of [REDACTED] in which this operation was discussed.

128. **Finding 17:** NSIRA found that CSE did not notify CSIS in a timely manner of a compliance incident in its Active Cyber Operation, which was connected to a CSIS Threat Reduction Measure.

129. CSE and CSIS collaborated closely both in setting up CSIS's TRM to complement CSE's ACO, as well as in the lead-up to the TRM's execution. This included

15(1)

TOP SECRET//SI//CEO

16(1)(b) communication regarding the logistics and timelines of CSE's activity and the associated logistics of CSIS's [REDACTED]. Once the TRM was implemented, CSIS advised CSE, at which point the collaboration ceased.

15(1)(d) 130. [REDACTED] CSE discovered via open source research that [REDACTED].
[REDACTED]
[REDACTED] The next day, CSE sent an email to some individuals from [REDACTED] of this incident, however, no CSIS employees were copied on the email. CSE noted that CSIS was informed verbally, but did not specify when this happened or what information was shared. According to CSIS, it was not until after a [REDACTED] bilateral meeting between CSIS and CSE management where the operation was discussed that it was fully briefed on CSE's compliance incident.

16(1)(b) 131. Initially, CSE had advised CSIS that the operation would not [REDACTED]. As such, CSE's discovery [REDACTED] changed a key parameter of the operation upon which CSIS planned its TRM.

132. While this compliance incident did not create a knock-on compliance incident for CSIS, under different conditions it could have. CSE's delay in effectively communicating the compliance incident to CSIS increases that risk. Given that the TRM and ACO regimes both enable their respective departments to actively take measures, albeit of a different nature, to counter threats, there is potential for this scenario to repeat under different circumstances and the departments should be alive to this potential as they run similar concurrent operations.

Recommendation 20: NSIRA recommends that CSE share details of potential compliance incidents with CSIS when an overlap may exist with a CSIS Threat Reduction Measure.

Status of CSE-CSIS Collaboration

133. Finding 18: NSIRA found that CSE failed to cooperate effectively with CSIS, leading to a missed opportunity to advance Canadian intelligence objectives via domestic collaboration.

15(1)

TOP SECRET//SI//[REDACTED]//CEO

16(1)(c) 134. In operation [REDACTED]⁸ CSIS sought to collect information within Canada on a foreign target under sections 12 and 21 of the CSIS Act. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

15(1)(d) 135. In [REDACTED] CSIS submitted an RFA to CSE to [REDACTED]
15(1)(f) [REDACTED] CSE accepted and
16(1)(c) committed to [REDACTED] In [REDACTED] CSE advised CSIS
that it was [REDACTED]
In [REDACTED], CSE formally terminated the RFA noting that [REDACTED]
[REDACTED] it
was no longer in a position to resource [REDACTED] At this point, CSE had not
provided CSIS with [REDACTED] under the RFA. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

15(1)(f) 136. CSE began a separate operation against the same target under section 16 of the
16(1)(c) CSE Act, as it had advised CSIS in [REDACTED] that it planned to do. This
operation utilized CSE's [REDACTED]
[REDACTED] This opportunity was derived from
CSIS efforts under the [REDACTED] initiative. Despite requests from CSIS to also
explore this new operation under RFA focusing on the communications of other CSIS
warranted targets [REDACTED] CSE opted to execute the
operation under their own foreign intelligence mandate. CSE reasoned that this was
the better option given the potential for collection of high value foreign intelligence
concerning targets [REDACTED] and that an RFA for CSIS warranted targets
could be implemented once the operation was running. While this RFA was later
actioned, during the period under review, [REDACTED]
[REDACTED]
[REDACTED]

137. Throughout [REDACTED] CSE failed to consider the impact of its choices on
CSIS's ability to discharge its mandate and detracted from Canada's overall ability to

16(1)(c) ⁸ [REDACTED] NSIRA did not review this operation from a technical or legal compliance perspective, but merely to observe how CSE and CSIS work together.

15(1)

TOP SECRET//SI//CEO

16(1)(c)
15(1)(d)

successfully progress the [REDACTED] operation as [REDACTED] effort against the target. CSE initially committed to assisting CSIS, [REDACTED], but later terminated the RFA without providing CSIS the requested assistance. CSE then utilized information it obtained from the CSIS operation to develop its own initiative, failing to promote a collaborative approach [REDACTED]

16(1)(c)

138. This lack of prioritization of domestic collaboration presents as a more general issue, not only isolated to the [REDACTED] operation.

139. A Memorandum of Understanding between CSE and CSIS, in place since 2011, states that the departments will "provide operational support to each other, when appropriate, in relation to their respective mandates." Further, the two shall "cooperate to avoid duplication of technology development and technology initiatives related to operations by relying, as appropriate, on the technical expertise of CSE to advance both CSE and CSIS interests."

140. Despite the emphasis of CSE tools being used to advance both departments' initiatives, CSE's policy fails to promote this kind of cooperation. Under the assistance aspect of its mandate, CSE is not obliged to action RFAs and can deny a request based on operational resourcing or prioritization considerations. However, there is no corresponding requirement for CSE to analyze the impact of the activity requested on the requesting department's initiative or GC strategic priorities when making its decision. Outside of its assistance mandate, CSE's policy repeatedly stipulates that consideration be paid to Five Eyes partner activities, and the impacts of CSE activity on its partners, but lacks similar considerations for domestic cooperation.

141. Conversely, CSIS's new Ministerial Direction (MD) for Operations prioritizes domestic collaboration as a fundamental principle, indicating "the Service will consider and seek to mitigate any potential significant adverse effects of its activities on the fulfilment of the mandates of other government departments and agencies, including by sharing information and collaborating with them, as appropriate." While this MD was not in force during the period under review, it emphasizes the importance of domestic collaboration. CSE does not have similar specific guidance in any MDs issued by the Minister of National Defence.

142. CSE has unique technical expertise within the GC. Its willingness to work with domestic partners can be pivotal to Canadian success. When CSE focuses primarily on its own goals or those of its Five Eyes partners and does not equally consider the totality of the potential operational yield for Canada realized through domestic collaboration, Canada risks losing opportunities to satisfy intelligence objectives.

4. CONCLUSION

143. As CSE and CSIS are two core pillars of the Canadian security and intelligence community, their effective collaboration is critical to protecting national security and advancing Canada's interests. CSE and CSIS should focus on combining their respective capabilities and expertise towards satisfying GC intelligence priorities.
144. In light of their differing mandates and legal frameworks, it is incumbent on CSE and CSIS to carefully plan their collaboration and establish guardrails. Structures for governance, clear understandings of roles and responsibilities, and sufficient information sharing must be paramount in each instance of operational collaboration. When this is done, the results of CSE and CSIS collaboration can be broad, deep, and have significant impact.

15(1)
15(1)(d)
15(1)(f)
16(1)(c)

TOP SECRET//SI//CEO

Annex A: Operations

Warranted Section 12 Investigation

1. In this operation, CSE and CSIS both targeted selectors associated with a CSIS section 12 warranted target. CSIS obtained a [REDACTED] warrant, amongst others, which allowed them to [REDACTED]. The target had also demonstrated [REDACTED] increasing the difficulty and risk associated with [REDACTED]. As such, CSIS submitted an RFA to CSE to assist with [REDACTED] as well as to conduct SIGINT collection. Regardless of which entity was responsible for the collection, the warrant required that a CSIS "designated employee" review the results of a limited initial collection and confirm that [REDACTED].
[REDACTED]
2. The operation was structured such that CSIS was responsible for [REDACTED] and CSE was responsible [REDACTED] outside of Canada. Both CSE and CSIS successfully [REDACTED] and produced intelligence products as a result of the operation. CSE's collection was enabled by [REDACTED] and CSIS collection was enabled using a combination of their own tools and CSE tools.

Warranted Section 16 Operation

3. In this operation, CSIS submitted an RFA to CSE, [REDACTED] in order to [REDACTED] and [REDACTED] under section 16 CSIS warranted authorities. This operation [REDACTED].
[REDACTED] The operation was structured such that [REDACTED].
[REDACTED] CSE was responsible for analyzing the data and reporting on it. The operation took place in [REDACTED].
[REDACTED]

TOP SECRET//SI//[REDACTED]//CEO

4. The Federal Court approved warrants in Canada on the condition that [REDACTED]
5. Throughout the course of the operation there were two compliance incidents wherein [REDACTED] for [REDACTED] intelligence purposes.
6. In the first instance, a CSE analyst looking through the [REDACTED] identified that [REDACTED] reporting that was not [REDACTED]. Upon further investigation it was identified that [REDACTED] used [REDACTED] without seeking CSIS's approval. [REDACTED] reported that in this instance the analyst who released the relevant report failed to recognize that [REDACTED] utilized this information in error.
7. In the second incident, [REDACTED] CSIS provided a list of questions [REDACTED] to answer concerning [REDACTED] responded, [REDACTED]. This was again discovered by a CSE analyst [REDACTED] reported that they thought providing the responses to the questions encompassed the required authorization.
8. In addition to the human error involved in violating the reporting requirements of the warrant in these cases, both non-compliance incidents also involved [REDACTED] for [REDACTED] intelligence purposes, contrary to the warrant.
9. These instances have both been reported to the Federal Court. At present, CSE has received written confirmation from [REDACTED]

TOP SECRET//SI//CEO

15(1)
15(1)(d)
15(1)(f)
16(1)(c)

[REDACTED] for [REDACTED] intelligence
purposes.

Operation

10. In this operation, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
11. CSE and CSIS discovered that this operation could also be used in order to support collection under section 16 of the CSE Act. As such, CSE [REDACTED]
[REDACTED]
[REDACTED] the CSE infrastructure ran a number of checks [REDACTED] in an attempt to filter out Canadians or those located in Canada. These checks included identifying [REDACTED]
[REDACTED]
- Once CSE did successfully [REDACTED] it would then also conducted further analysis on the collection in order to ascertain if the user of the device was Canadian or located in Canada. When CSE successfully [REDACTED]
[REDACTED] they produced reports, which were released to CSIS. Should CSIS be interested in using the reporting, either to further their own investigation or to share with partners, it was able to seek permission from CSE to do so.
12. The departments conducted this operation entirely under their own mandates, CSIS Act section 12 and CSE Act section 16. While CSIS collection would have been possible without CSE's involvement in the operation, CSE did require CSIS in order to gain access to [REDACTED]

Annex B: Section 35 Reports

- 15(1)(f) **Non-compliance with the Law – CSE Analyzes [REDACTED] of a Canadian's Device**
1. CSIS Lead Information messages (CLIs) and Foreign Intelligence Lead Generation Information (FILGIs) are the means by which CSIS shares intelligence it believes may be of value to CSE's foreign intelligence mandate. In addition to providing lead information, CSIS uses these messages to request information from and/or action by CSE.
 - 15(1)(d) 2. CLIs are generally sent in a [REDACTED] context and are emailed from CSIS analysts directly to CSE analysts. Upon receipt, CSE chooses how to act on the intelligence, including whether to pursue any further action based on the lead information. At CSIS, CLIs are saved in a single corporate repository, however, at CSE they are not.
 3. Both the *Canadian Security Intelligence Services Act* (CSIS Act) and the *Communications Security Establishment Act* (CSE Act) govern the disclosure and acquisition of the information contained in CLIs. CSIS shares this type of information pursuant to section 19(2) of the CSIS Act, which enables it to disclose information for the purposes of the performance of its duties and functions. Section 16 of the CSE Act permits CSE to collect foreign intelligence using a range of sources and methods, and it relies on this section to acquire the information contained in the CLIs.
 4. While CSE is prohibited from directing its activities at Canadians under section 22(1) of the CSE Act, section 23(4) of the CSE Act does permit CSE, in certain circumstances, to incidentally acquire information about Canadians. Incidental collection occurs when information was not deliberately sought and the information-acquisition activity was not directed at the Canadian or person in Canada. It is using this provision that CSE is able to acquire the information about Canadians shared by CSIS via the CLI process.
 - 15(1)(f) 5. **NSIRA found that CSE did not comply with section 22(1) of the CSE Act when it analyzed [REDACTED] of a Canadian's device obtained through a CSIS lead information message.**
 - 15(1)(d) 6. In one case reviewed by NSIRA, CSIS sent a CLI to CSE that contained [REDACTED] of
15(1)(f) the contents of a Canadian's [REDACTED] device. The Canadian was the subject of a CSIS warrant and had been [REDACTED] authorities due to [REDACTED] involvement in [REDACTED] activities. [REDACTED]

15(1)

TOP SECRET//SI//CEO

15(1)(f)

_____ authorities _____ of the individual's _____ and shared it with CSIS, which in turned shared it with CSE via a CLI.

15(1)(d)

15(1)(f)

7. The CLI indicated the individual's _____
_____ The CLI further explained how CSIS acquired _____ of the device, indicated that the _____ and stated that _____ of the individual's device was being provided for "analytic and lead generation purposes".

15(1)(f)

8. CSE relied on its foreign intelligence mandate to ingest the CLI and _____ of the Canadian's device and to analyze the information found within. The analysis did not yield anything of foreign intelligence value and CSE subsequently deleted the data.

15(1)(f)

9. As CSE's prohibition against directing its activities at Canadians applies in this case, CSE provided two arguments to NSIRA to justify analyzing the information despite _____ originating from a Canadian's device. First, it noted that _____ had been lawfully obtained by CSIS, stating that _____ it received _____ of the content of the device, that was legally obtained by CSIS and disclosed to CSE." Second, CSE stated that it analyzed _____ of the device in order to identify information of foreign intelligence interest and the Canadian information found in the device was incidental.

10. CSE's policy notes that to respect the "directed at" prohibition, foreign intelligence activities must be directed at foreign persons and entities outside of Canada. It indicates that both analysis and evaluation of data for foreign intelligence value are considered SIGINT production activities and further confirms that operational analysis must not be directed at Canadians or persons in Canada. The policy is clear that these provisions apply to information collected by CSE activities and to data or information disclosed to CSE by a GC department for use under the foreign intelligence aspect of CSE's mandate.

11. With respect to disclosures specifically, CSE's policy indicates "where a foreign nexus is not evident in disclosed information (e.g. when the information is that of a Canadian or of a person in Canada), CSE must ensure that the disclosing entity clearly explains the foreign intelligence value in writing". As noted above, in this case the CLI only indicated that the information was being provided for "lead generation and analytic purposes" and did not articulate a specific foreign intelligence value. NSIRA saw no evidence of CSE requesting this information from CSIS. Further, the general inclusion of "when the information is that of a Canadian or a person in Canada" contradicts the notion that operational analysis must not be directed at Canadians or persons in Canada. This example is inappropriate to include in this

15(1)

TOP SECRET//SI//[REDACTED]//CEO

section of the CSE policy without requiring the information to fit into the narrow exceptions that allow CSE to retain Canadian information, as described below.

15(1)(f) 12. In this case, CSE conducted SIGINT production activities (specifically, operational analysis) [REDACTED] of the device. As this device belonged to a Canadian, CSE's actions were directed at a Canadian. It is irrelevant that the actions were intended to produce information of foreign intelligence interest, or that the information was initially legally obtained by CSIS.

13. There are two circumstances in which CSE is permitted to acquire and/or use Canadian information under their foreign intelligence mandate. In the first, CSE's policy, citing section 46 of the CSE Act, permits certain use, analysis, and disclosure of Canadian information in its possession in circumstances where there are reasonable grounds to believe that there is imminent danger of death or serious bodily harm to any individual and that the information will be relevant to the imminent danger. CSE did not provide any information to suggest such circumstances applied in this case.

15(1) 14. The second circumstance is incidental collection. However, information cannot be considered incidentally collected if it was collected by an activity that was directed at a Canadian. [REDACTED]

15(1)(d) 15. Although legal advice was not sought in relation to [REDACTED] of the Canadian's
15(1)(f) device, [REDACTED]
CSE was not permitted to use [REDACTED] Canadian's device as a starting point to identify information of foreign intelligence interest as [REDACTED] device could reasonably be expected to contain [REDACTED] that could not be seen to be incidentally collected.

16. In response to NSIRA's concerns on this case, CSE stated the following:

Canada's national security legislation is intended to not leave knowledge gaps between Canada's security agencies and to ensure that foreign and domestic threats are dealt with by the appropriate agency and in a seamless way. The inability of CSE to acquire and use information of FI value that has been lawfully obtained by CSIS through lawful activities directed by that agency against a

15(1)

TOP SECRET//SI//CEO

Canadian could create a gap with severe implications for Canada's national security.

17. This response fails to consider the context of this situation. CSE may acquire and use information of foreign intelligence value that has been lawfully obtained by CSIS, even if obtained by CSIS directing its activities at Canadian, as CSE suggests in the above. The compliance issue in this case was that CSE itself conducted the analysis on Canadian information (i.e. directing its activities at a Canadian) in order to identify information of foreign intelligence value and attempted to then justify this action as incidental collection. To render this compliant, the analysis of the Canadian information would have needed to be done by CSIS prior to disclosure as opposed to by CSE post-disclosure. This is an important distinction that differentiates this case from legitimate instances of CSE's analysis of CSIS disclosures.

18. As articulated in CSE policy, CSIS's (or other GC departments') legal authorities to disclose do not create corresponding authorities for CSE to analyze, and CSE's intent to discover foreign intelligence information does not relieve it of its responsibility to not direct its activities at Canadians. When operating under its foreign intelligence mandate, CSE's actions further to all CLIs must be consistent with its own authorities and applicable restrictions. In this case, CSE's analysis of [REDACTED] of the Canadian's device contravened section 22(1) of the CSE Act.

15(1)(f)

19. Further to the above, CSE stated that it "acknowledges the perception of this anomalous activity of receiving a file containing [REDACTED] of the content of a Canadian's device [and] has since made a policy decision to not look into this particular kind of file." CSE did not provide any policy documentation to support this statement.

15(1)(f)

15(1)

TOP SECRET//SI//CEO

Non-compliance with the Law – CSE Receives and Utilizes Entire Exceptional Reports

1. When foreign SIGINT partners produce reporting derived from directly targeting Canadians, CSE and CSIS refer to the resulting reports as “exceptional reports”. The Five Eyes partnership involves a long-standing unwritten agreement that members will not target one another’s citizens via signals intelligence. However, as each country remains a sovereign nation, it is understood that they may, on an exceptional basis, target member’s citizens if needed to respond to urgent threats.⁹ The resulting exceptional reporting is of interest to CSIS given that a Canadian is involved and therefore a nexus to the security of Canada likely exists.

15(1)(d)
15(1)(f)
16(1)(c)

2. Prior to 2014, SIGINT partners shared exceptional reporting directly with CSIS. However, due to [REDACTED] at CSIS it was determined that under RFA, CSE could act as a conduit between foreign SIGINT partners and CSIS. Under this RFA, known as [REDACTED] SIGINT partners provide exceptional reports directly to CSE either through CSE’s intelligence reporting software, SLINGSHOT, or via other secure communications methods. CSE then grants CSIS staff access to the exceptional reports within SLINGSHOT. After [REDACTED] deemed success by the departments, [REDACTED]

3. Under the RFAs, CSE has also been provided the authority to review the reports for foreign intelligence value. CSE may then request that CSIS disclose the reports containing information of foreign intelligence value back to CSE. At this point in the process, CSIS acts under section 19(2) of the CSIS Act to review the request and decide whether to disclose the exceptional report in its entirety to CSE. CSE, no longer operating under RFA, then receives the disclosure and utilizes the exceptional reporting for foreign intelligence purposes using the powers in section 16 of the CSE Act.

16(1)(c)

4. Of note, the Office of the Communications Security Establishment Commissioner reviewed the initial implementation of [REDACTED] in 2015 and found the procedure to be compliant with the law. However, the report noted that while CSE analysts were reviewing the exceptional reporting to identify foreign lead information, CSIS did not disclose any foreign lead information until after the review period, so this part of the process was not reviewed at that time.

⁹ [REDACTED] Five Eyes partners target Canadians on an exceptional basis, and subsequently produce exceptional reporting, [REDACTED]
[REDACTED]
[REDACTED]

TOP SECRET//SI//CEO

15(1)
15(1)(d)
15(1)(f)

5. NSIRA found that CSE did not comply with either section 22(1) of the CSE Act or section 273.64(2)(a) of the National Defence Act (NDA) when it used [REDACTED] complete exceptional reports for foreign intelligence purposes.
- 16(1)(c) 6. The review period began prior to the enactment of the CSE Act, as such, some of CSE's activities under [REDACTED] were conducted under the authorities of the NDA. Section 273.64(2)(a) of the NDA is the mirror provision to section 22(1) of the CSE Act, which prohibits CSE from directing its activities at Canadians or persons in Canada.
- 16(1)(c) 7. During the period under review, [REDACTED] exceptional reports were transmitted from CSE to CSIS using both [REDACTED]. Of these [REDACTED] CSE requested the disclosure of [REDACTED] and received and analyzed all [REDACTED] in their entirety. Some foreign selectors were targeted further to the reports. However, CSE indicated that the exceptional reports primarily "added context" to CSE [REDACTED] investigations.
- 15(1)(d) 8. CSE stated generally that "Canadian information [found in the exceptional reports] is not used in connection with any SIGINT FI activity." However, it provided no specific confirmation concerning the [REDACTED] reports in question, nor did it detail any mitigating measures used with respect to the Canadian information contained in these reports.
- 15(1) 9. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
10. CSE cannot indirectly (via CSIS) obtain reporting that it could not directly obtain from its SIGINT partners, nor can it use this Canadian information as a starting point to advance its foreign intelligence mandate.¹⁰ As CSE is not interested in, nor is it authorized to use, the Canadian information contained in the reporting, a more nuanced approach must be taken to enable CSE to obtain information to further its foreign intelligence mandate without violating the prohibition in section 22(1) of the CSE Act. A refined CLI process with necessary protections for any Canadian information, as recommended above, would serve as an appropriate means to do so.

15(1)(f)

¹⁰ Refer to NSIRA's section 35 report entitled "Non-compliance with the Law - CSE Analyzes [REDACTED] of a Canadian's Device" also drafted further to its Review of CSE-CSIS Operational Collaboration (review #21-16).

Annex C: Findings and Recommendations

Collaboration in Operations: Requests for Assistance

Finding 1: NSIRA found that CSE does not routinely share its operational plans and associated risk assessments with CSIS when operating under CSIS authorities. This may leave CSIS unable to fully assess CSE's activities for compliance.

Recommendation 1: NSIRA recommends that CSE share its operational plans and associated risk assessments with CSIS prior to operating under CSIS authorities.

Finding 2: NSIRA found that close collaboration at the working level created the right conditions for CSIS to monitor CSE's assistance activities for compliance with warrant conditions.

Recommendation 2: NSIRA recommends that when CSIS engages CSE for assistance with the execution of warranted powers, a CSIS employee be involved to ensure compliance in CSE's collection activities until the request for assistance has terminated.

Finding 3: NSIRA found that CSIS failed to submit an updated request for assistance to CSE in a timely manner when it sought new warrant powers.

Recommendation 3: NSIRA recommends that CSIS develop a process to ensure that necessary requests for assistance are submitted to CSE in a timely manner subsequent to obtaining warrant powers.

Finding 4: NSIRA found that CSE and CSIS did not engage in any joint investigation, assessment, or tracking of a compliance incident.

Recommendation 4: NSIRA recommends when working under a request for assistance CSIS and CSE develop a framework for joint investigation of potential compliance incidents.

Finding 5: NSIRA found that CSE and CSIS failed to implement an effective operational framework for their collection activity. This contributed to two instances of non-compliance with the Federal Court's direction.

Recommendation 5: NSIRA recommends that CSIS ensure roles and responsibilities are clearly agreed to prior to allowing partners to execute warrant powers. Where appropriate, these agreements should be shared with the Federal Court.

Recommendation 6: NSIRA recommends that CSIS ensure it is directly involved in all substantive communications with any partner actively executing its warrant powers.

Recommendation 7: NSIRA recommends that CSIS share paragraphs 32 through 41 of this review, along with associated recommendations, with the Federal Court.

Collaboration in Operations: Joint Operations

Finding 6: NSIRA found that CSE and CSIS identified an effective opportunity to collaborate under their respective mandates and carried out an operation that proved beneficial for both Canada and its allies.

Finding 7: NSIRA found that, while CSIS's operational framework was sufficient, CSE's operational framework did not assess legal and policy risk specific to the operation.

Recommendation 8: NSIRA recommends that when CSE engages in joint operations with CSIS it should perform risk assessments for each operational activity. These should specifically consider the risk of targeting Canadians and implement proactive measures to mitigate this risk.

Finding 8: NSIRA found that CSE and CSIS did not draft joint terms of engagement, a joint operational plan, or engage in joint risk assessments.

Recommendation 9: NSIRA recommends that when participating in joint operations, CSE and CSIS either jointly develop or share written terms of engagement, operational plans, and risk assessments.

Finding 9: NSIRA found that CSE's foreignness assessment did not account for the increased risk of targeting Canadians when working with CSIS.

Recommendation 10: NSIRA recommends that CSE perform foreignness assessments that account for the increased risk of targeting Canadians when working with CSIS.

Collaboration in Information Sharing: CSIS Lead Information

Finding 10: NSIRA found that both CSE and CSIS lack policies, procedures, and accountability mechanisms to govern CSIS lead information messages and associated requests and actions.

Recommendation 12: NSIRA recommends that CSIS develop policies, procedures, and analyst training to standardize the disclosure of CSIS lead information messages to CSE.

Recommendation 13: NSIRA recommends that CSE develop policies, procedures, and analyst training to standardize the use of CSIS lead information messages.

Finding 11: NSIRA found that CSIS's use of lead information messages to share information and make requests about Canadians creates a high risk of potential for non-compliance for CSE.

Recommendation 11: NSIRA recommends CSIS cease making requests for action and/or further information to CSE in relation to Canadians or people in Canada via CSIS lead information messages.

Finding 12: NSIRA found that CSE's application of incidental collection provisions may not be appropriate in situations where CSE knows there is a Canadian nexus to a CSIS foreign intelligence lead, and where it knows it is likely to collect Canadian information in pursuing the lead.

Recommendation 14: NSIRA recommends that CSE develop a regime for collecting, retaining, and reporting to CSIS Canadian information it uncovers further to legitimate foreign intelligence activities where it has advance knowledge of the Canadian information.

15(1)(f) **Finding 13:** NSIRA found that CSE did not comply with section 22(1) of the CSE Act when it analyzed [REDACTED] of a Canadian's device obtained through a CSIS lead information message.

Recommendation 15: NSIRA recommends that CSE update its policies to prohibit the analysis of information relating to a Canadian or person in Canada for the purposes of identifying foreign intelligence.

Collaboration in Information Sharing: Exceptional Reporting Loop

15(1)(d) **Finding 14:** NSIRA found that CSE did not comply with either section 22(1) of the CSE Act or section 273.64(2)(a) of the *National Defence Act* (NDA) when it used ■ complete exceptional reports for foreign intelligence purposes.

Recommendation 16: NSIRA recommends that if CSIS decides to disclose exceptional reporting to CSE, it should extract the relevant foreign intelligence for disclosure as opposed to sending the entire report.

Recommendation 17: NSIRA recommends that CSE cease using complete exceptional reports from CSIS under its foreign intelligence mandate.

Collaboration in Information Sharing: Protected Entity Tool

Finding 15: NSIRA found that CSE does not consistently utilize its protected entity tool to prevent targeting Canadian identifiers it receives from CSIS.

Recommendation 18: NSIRA recommends that CSE introduce a requirement to always apply the protected entity tool to all Canadian identifiers.

Collaboration in Threat Reduction Measures

Finding 16: NSIRA found that while CSIS performs an initial consultation, it does not routinely pursue further engagement with CSE during Threat Reduction Measure activities that could overlap with CSE activities.

Recommendation 19: NSIRA recommends that CSIS pursue routine engagement with CSE during the implementation of its Threat Reduction Measures when the potential for operational overlap exists.

Finding 17: NSIRA found that CSE did not notify CSIS in a timely manner of a compliance incident in its Active Cyber Operation, which was connected to a CSIS Threat Reduction Measure.

Recommendation 20: NSIRA recommends that CSE share details of potential compliance incidents with CSIS when an overlap may exist with a CSIS Threat Reduction Measure.

15(1)

TOP SECRET//SI//[REDACTED]//CEO

CSE-CSIS Relationship

Finding 18: NSIRA found that CSE failed to cooperate effectively with CSIS, leading to a missed opportunity to advance Canadian intelligence objectives via domestic collaboration.