National Security and Intelligence Review Agency | Office de surveillance des activités en matière de sécurité nationale et de renseignement

REVIEW OF A SPECIALIZED [redacted] PROGRAM UNDER THE FOREIGN INTELLIGENCE ASPECT OF CSE'S MANDATE

NSIRA // Review 2021 - 06

TOP SECRET // SI // CEO

Table of Contents

I. EXECUTIVE SUMMARY

1. (TS) CSE carries out its [redacted] program under the foreign intelligence aspect of its mandate. As one of [redacted] authorized under the [redacted] Ministerial Authorization, the [redacted] program is uniquely positioned as both a user of traditional foreign intelligence and as a facilitator for foreign intelligence collection. The program involves [redacted]

2. (TS) The [redacted] program is multi-faceted and incorporates multiple functional pillars. For example, to support [redacted] the program encompasses target development activities that leverage existing SIGINT tools and tradecraft, as well as capability development [redacted] The program also collaborates with domestic or foreign partner agencies [redacted]

3. (TS) NSIRA assessed the entire lifecycle of the [redacted] program to assess for compliance with the law, Ministerial Authorizations, and internal policies. NSIRA's analysis extended beyond [redacted] and incorporated initial target development activities, as well as CSE's testing and validation of its tools [redacted]. In all, NSIRA reviewed [redacted] operations within the review period, encompassing over 1,600 documents and attending several briefings by CSE personnel. Each operation contained unique operational elements that enabled NSIRA to assess different aspects of the [redacted] program.

4. (TS) NSIRA's observations and findings highlighted systemic issues within the governance of the [redacted] program and concerns regarding how CSE describes its activities to the Minister of National Defence. During the review period, NSIRA found that CSE did not adequately inform the Minister of the testing and evaluation of its tools, nor did it sufficiently describe its activities conducted [redacted] NSIRA also found that CSE should have provided an update to the Minister on [redacted] its relationship with a foreign partner.

5. (TS) NSIRA's concern regarding CSE's relationship with a foreign partner is compounded by an inconsistent application of internal policies in the conduct of [redacted] activities. In the context of sharing with a [redacted] partner, NSIRA found that CSE did not always comply with its policies related to analytic exchanges, nor did CSE appropriately apply its Mistreatment Risk Assessment process prior to sharing information.

6. (TS) NSIRA also identified concerns related to the governance of the [redacted] program. First, CSE lacks written agreements with [redacted] partners implicated in [redacted]

[redacted] activities. Further, CSE has not developed policies and procedures to govern [redacted] Lastly, CSE's contributions to [redacted] operations led by a [redacted] partner were not accompanied with the operational planning and risk assessments as described by CSE to the Minister.

7. (U) Finally, NSIRA has identified an important area for further examination related to CSE's targeting regime, with an emphasis on the foreignness assessment process. Given that CSE's activities must not be directed at Canadians or at persons in Canada, the implementation of its targeting regime has sweeping implications across the majority of CSE's mandated activities. NSIRA observed a situation in which the foreignness assessment process pertaining [redacted] individuals had raised questions about the possibility of their Canadian status, yet CSE continued to perform intelligence collection and reporting activities [redacted] while the answers to these questions were outstanding.

8. (U) Throughout this review, NSIRA experienced significant challenges with CSE's provision of information and the quality of its responses. Substantial amounts of relevant material were provided only at the conclusion of the review, and some were not provided at all. As a result, NSIRA has limited confidence in the completeness of information provided by CSE, and is dissatisfied with CSE's responsiveness.

List of Acronyms

[redacted]

ACA – *Avoiding Complicity in Mistreatment by Foreign Entities Act*

[redacted]

CSE Act – *Communications Security Establishment Act*

CSIS – Canadian Security Intelligence Service

DND/CAF – Department of National Defence / Canadian Armed Forces

DOJ – Department of Justice

[redacted]

GAC – Global Affairs Canada

GC – Government of Canada

[redacted]

GII – Global Information Infrastructure

[redacted]

IRCC – Immigration, Refugees, and Citizenship Canada

[redacted]

MA – Ministerial Authorization

[redacted]

MFA – Minister of Foreign Affairs

MND – Minister of National Defence

[redacted]

MPS – Mission Policy Suite

MRA – Mistreatment Risk Assessment

[redacted]

RCMP – Royal Canadian Mounted Police

RSP – Releasable SIGINT Product

SCIDA – *Security of Canada Information Disclosure Act*

[redacted]

SIGINT – Signals Intelligence

SORAF – SIGINT Operational Risk Acceptance Form

[redacted]

[redacted]

Glossary of Terms

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

[redacted]

CSE-controlled environment. An area where specific parameters are controlled, regulated, or known.

[redacted]

II. AUTHORITIES

1. (U) This review was conducted pursuant to paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency (NSIRA) Act*.

III. INTRODUCTION

Review Background and Methodology

2. (TS) A range of programs and activities contribute to the foreign intelligence aspect of the Communications Security Establishment's (CSE) mandate. The [redacted] Program ([redacted]) is one such program, enabling the collection of foreign intelligence [redacted] often through working closely with domestic and international partners. Despite its sensitivity, this program has never been subject to internal or external review. [redacted] the lack of previous review in this area formed part of the rationale to first review this [redacted] foreign intelligence program, prior to embarking on future planned reviews of [redacted] collection programs.

3. (TS) This report will be structured in the following manner. Section III introduces the legal and policy foundation for activities conducted under [redacted] as well as an overview of the types of activities that are conducted. Sections IV to VI detail NSIRA's observations, findings, and recommendations pertaining to the activities performed in support of this program in the review period of January 1, 2018 to February 28, 2021. These sections are divided into the following key themes. Section IV details NSIRA's observations of the key compliance and governance issues surrounding the [redacted] program's target development activities and activities supporting [redacted] Section V presents governance mechanisms, such as [redacted] that are invoked when operations are deemed to reach the threshold of [redacted] operations. Section VI presents an overview of CSE's testing and evaluation activities in relation to the [redacted] program.[1] The report will conclude with a summary of CSE's overall responsiveness to this review.

---

[1] All of these themes relate to 'pre-operation' activities that are performed in the early stages before an operation is conducted, for reasons ranging from [redacted] operation. Testing activities also largely exist in the pre-operation space, as CSE seeks to ensure that its [redacted] tools will function [redacted] The structure of the report thus mirrors the sequence that each of these types of activities are performed in support of a [redacted] operation. Specifically, initial planning for [redacted] operations would begin with target development activities, and would encompass tools and techniques outside the [redacted] space. Once the operation is more

4. (TS) As part of its assessment, NSIRA reviewed a wide range of materials, including policies and procedures, Ministerial Authorizations, internal documents, technical documentation, as well as correspondence among CSE personnel and with partners in relation to specific operational activities. NSIRA requested all documentation pertaining to each of the [redacted] operations.[2] Additionally, CSE held several briefings to inform reviewers about different elements of the [redacted] program, and hosted a tour of the facilities [redacted]

5. (TS//SI) NSIRA reviewed the full lifecycle of those [redacted] activities that were carried out during the period of review, starting with the initial development of an operation to its conclusion or closure. This allowed NSIRA to understand the program's activities and how fits into CSE's broader foreign intelligence aperture. Each [redacted] operation tends to have unique operational elements, and as a result, NSIRA's findings pertain to the discrete issues observed in each operation. However, NSIRA's review also found that these discrete issues are illustrative of a number of systemic issues within the [redacted] program and in how its activities are described to the MND.

6. (TS//SI) [redacted] relies on and is interrelated with operational activities performed under the foreign intelligence aspect of CSE's mandate, which both facilitate and are facilitated by [redacted] activities. As a result, NSIRA's review included analysis of elements of [redacted] and intelligence analysis activities performed as part of the lifecycle of [redacted] programs, [redacted][3] The majority of these supporting activities are [redacted] which involve [redacted] program which in turn enables the collection of foreign intelligence. The same can be said, to a lesser degree, for CSE's other activities, such as [redacted][5] Rather than a standalone operating program, [redacted] is uniquely integrated into

---

finalized, governance structures more specific to the [redacted] environment would be applied. Finally, any tool developed [redacted] would be tested and evaluated [redacted]

[2] In all, NSIRA received and reviewed approximately 1,600 documents and CSE responses as part of this review.

[3] The program's activities [redacted] during the period of review, and [redacted] Further, NSIRA only assessed [redacted] and intelligence analysis activities in the context of the [redacted] operation to which they were linked. As such, NSIRA will not pronounce on the lawfulness, reasonableness, or necessity of these activities as part of this review, and intends to review them more holistically in the coming years.

[4] [redacted] (Refer to Mission Policy Suite, Foreign Intelligence Chapter, Section 14.1.)

[5] [redacted] (Refer to CSE Document, "End of Authorization Report for the Minister of National Defence: Foreign Intelligence Authorization [redacted] Activities," September 2020 to September 2021:)

different aspects of CSE's activities, both as a user of traditional foreign intelligence and in an enabling capacity.

What is the [redacted] Program?

7. (TS//SI) Housed under the foreign intelligence aspect of CSE's mandate, [redacted] is one of [redacted] authorized by the [redacted] Ministerial Authorization ([redacted] MA). The program enables CSE to acquire foreign intelligence [redacted] activities are comprised of several functional pillars [redacted]

8. (TS//SI) The [redacted] program is comprised of technologists, engineers, and analysts who contribute to the program by [redacted] As well, [redacted] analytical staff conduct target development activities to [redacted] using existing signals intelligence (SIGINT) tools and techniques. Finally, the program conducts [redacted]

[redacted]
Activities Budget
2020-2021

[redacted]

9. (TS//SI) To enable [redacted] activities involve a substantial investigative component in the form of research to [redacted][10] This process may encompass [redacted]

---

[6] Depending on the CSE's role in the operation, [redacted] personnel may be involved in each phase or may be more limited in their engagement by performing a specific role.

[7] CSE defines an operation in this context as: "An activity conducted [redacted] CSE Deck, "NSIRA Review of [redacted] Program," February 19, 2021, Slide 4.

[8] A [redacted] is an operation in which [redacted]

[9] CSE Deck, "NSIRA Review of [redacted] Program," February 19. 2021, Slide 9.

[10] Due to the varied nature of [redacted] activities, the term 'target' may encompass [redacted]

[redacted][11] To this end, CSE uses open-source information and/or leverages existing SIGINT tools, tradecraft, and information which, in some cases, may be authorized under separate Ministerial Authorizations or originate from the collection of CSE's Five Eyes partners.

10. (TS//SI) In addition to target development, [redacted] activities involve [redacted][2] During the review period, the program's operational activities were largely performed in collaboration with and/or alongside CSE's domestic and international partners, in which CSE's primary role has been to [redacted] The program's main international partners are [redacted][13] As described by CSE, collaborating with foreign partners carries the benefit of specialization and sharing of specific outputs, as well as achieving economies of scale through the partnership. For example, [redacted][4]

11. (TS//SI) Different mechanisms can enable [redacted][5]

Legal Foundation for [redacted] Activities

12. (TS) [redacted] activities are conducted under the authority of the *Communications Security Establishment (CSE) Act*. Specifically, section 16 of *the CSE Act* mandates CSE to acquire information from or through the global information infrastructure (GII) for the purpose of providing foreign intelligence in accordance with the Government of Canada's intelligence priorities.[16]

---

[11] CSE Deck. "[redacted] Operations", February 2021. Page 9 & 12.
[12] Application to the Minister of National Defence for Foreign Intelligence Authorization, [redacted] Activities, September 4, 2019, para. 11(c).
[13] Meeting with CSE stakeholders on [redacted] June 22, 2021.
[14] Please refer to Annex C for more information about [redacted]
[15] [redacted]
[16] *CSE Act*, section 16. "The foreign intelligence aspect of the Establishment's mandate is to acquire, covertly or otherwise, information from or through the global information infrastructure, including by engaging or interacting with

13. (TS//SI) As per subsection 26(1) of the *CSE Act*, the Minister of National Defence (MND) may issue a Foreign Intelligence Authorization that authorizes CSE to conduct the activities specified in s. 26(2) of the *CSE Act*. [redacted] activities are authorized under the Foreign Intelligence Authorization for [redacted] Activities, as a class of [redacted] activities authorized in furtherance of the foreign intelligence aspect of CSE's mandate.[17] Since the *CSE Act* came into force on August 1, 2019, there have been three annually-issued [redacted] MAs that have authorized CSE's [redacted] activities.[18]

14. (TS) A component of the [redacted] program involves the [redacted] Given the unique nature of [redacted] testing and evaluation activities may also be conducted pursuant to section 23(1)(c) of the *CSE Act*.[19] This section of the Act, [redacted] enables CSE to test and evaluate products, software, and systems, including evaluating them for vulnerabilities, despite the prohibition in subsection 22(1) of the *CSE Act* that CSE not direct any of its activities at Canadians or any person in Canada, or infringe the *Canadian Charter of Rights and Freedoms*.[20]

Policy Framework

15. (TS) CSE has not developed policy and procedural requirements that are specific to [redacted][21] Rather, CSE's principal policy document, the Mission Policy Suite (MPS), contains policies that generally guide [redacted] activities. For instance, the MPS provides overarching guidance for [redacted] that are transferable to the [redacted] operational context.[22] For instance, [redacted] activities must be directed at foreign networks and devices located outside Canada, [redacted][23] Further, CSE policies regarding targeting and the use of selected and unselected

---

foreign entities located outside Canada or by using any other method of acquiring information, and to use, analyse and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities."

[17] The other "classes" of [redacted] activities are [redacted] Note that "classes" of [redacted] activities, as described in the Chief's application, has a different meaning than the "classes of activities" listed in s. 26(2) of the *CSE Act*.

[18] The most recent Foreign Intelligence Authorization [redacted] Activities, 2021, issued by the MND on August 13, 2021 and approved by the Intelligence Commissioner on September 1, 2021, was beyond the scope of this review. CSE Foreign Intelligence Authorization [redacted] Activities, 2020, issued by the MND on August 25, 2020; Foreign Intelligence Authorization [redacted] Activities, 2019, issued by the MND on September 5, 2019.

[19] *CSE Act*, paragraph 23(1)(c).

[20] *CSE Act*, subsection 22(1).

[21] In NSIRA's review of the latest and previous versions of the MPS, [redacted] is simply named and described, without specific requirements, unlike [redacted] though [redacted] also are not subject to specific requirements.

[22] During the period of review, [redacted] were regularly executed in support of broader [redacted] objectives and goals.

[23] MPS, Foreign Intelligence Chapter, Section 14.1.

information[24] apply to [redacted] particularly in relation to research performed by [redacted] personnel in support, or in preparation for, [redacted] The MPS also contains important requirements for information sharing[25] and conducting joint operations with partners.[26]

IV. TARGET DEVELOPMENT

16. (TS//SI) Given the [redacted] program's [redacted] target development comprises [redacted] activities, and is usually the first step in planning a [redacted] operation. In CSE's application for the 2020-2021 [redacted] MA, CSE describes target development as an activity that [redacted] on foreign segments of the GII, [redacted] The application further explains that all target development activities are conducted under an [redacted] and that each target development request responds to GC intelligence priorities outlined in the National SIGINT Priorities List (NSPL).[27]

17. (TS//SI) In this context, NSIRA set out to assess how CSE's target development activities align with its legislative framework, the requirements of the [redacted] MA, and CSE's internal policies and procedures. NSIRA expected to find that, in preparation for [redacted] operations, CSE personnel conducted research on targets of interest in compliance with these requirements.

[redacted] Targets

18. (TS//SI) During the period of review, NSIRA observed [redacted] types of target development activities, with [redacted] comprising research into the [redacted] targets of an operation – in other words, those targets [redacted] target development pertained to researching [redacted] CSE employed a range of tools and techniques to

[24] CSE Mission Policy Suite, Foreign Intelligence Chapter, Section 11.
[25] CSE Mission Policy Suite, Foreign Intelligence Chapter, Para 25.8, Section 26, and Section 29.
[26] CSE Mission Policy Suite, Foreign Intelligence Chapter, Section 4.
[27] CSE Application for a Foreign Intelligence Authorization, [redacted] Activities 2020-2021, Para 38.
[28] These terms were defined by NSIRA for ease of reference and narrative throughout this report.

gather information on [redacted] targets, including both open-source and SIGINT tools.

19. (TS//SI) As part of its review, NSIRA requested all operational documentation, which included target development efforts. During the period of review, CSE performed target development as part of [redacted] in the review period: [redacted][29] Of [redacted], NSIRA selected [redacted] as the case study to assess CSE's target development activities as it was [redacted] and for which NSIRA had received substantially greater amounts of material in order to assess [redacted] CSE's targeting efforts.

Case study: Operation [redacted]

20. (TS//SI) A joint operation between CSE and [redacted][1] and involved [redacted] As part of this operation, CSE employed traditional SIGINT techniques such as [redacted] and open source research[34] [redacted]

Arrangement governing CSE's [redacted]

21. (TS) CSE's arrangement [redacted] was entered into prior to the *CSE Act*. Notably, the 2012 Ministerial Directive requires CSE [redacted]

---

[29] Target development was also assumed by NSIRA to have been performed as part of [redacted] However, NSIRA did not observe documentation pertaining to the target development for this operation, which could result from these activities having taken place prior to the review period.

[30] CSE's [redacted] is governed by the "Memorandum of Understanding between the Communications Security Establishment (CSE) and [redacted] which was signed in [redacted] and details the parameters of cooperation between CSE and [redacted]

[31] CSE Document, "CSE [redacted] Joint Operation Response," [redacted] See also: CSE Email, "RE: OP [redacted] approval request," [redacted]

[32] For example, see CSE Email, "RE: [redacted]

[33] For example, see CSE Email, "FW: JIRA : [redacted]

[34] CSE target summaries contain information gleaned from open sources [redacted]. For instance, refer to CSE Document, "[target name] [redacted]

[35] CSE Email, " [redacted] It is unclear to NSIRA whether [redacted]

[redacted][36] The coming into force of the *CSE Act* continued the existing arrangement in accordance with its terms.[37] Section 54 of the *CSE Act* does, however, impose new legislative requirements for CSE to abide by in entering into arrangements with entities with powers and duties similar to CSE's. Unlike the *National Defence Act,* the *CSE Act* legislates that the MND approve arrangements with institutions of foreign states, after the MND has consulted with the Minister of Foreign Affairs (MFA).[38] Under the *National Defence Act*, in accordance with the requirements of a Ministerial Directives [redacted] a briefing note on CSE's [redacted] was submitted to the Minister of National Defence on [redacted][40] after engaging with the Deputy Minister of Foreign Affairs [redacted][41]

22. (TS) In [redacted] CSE again engaged [redacted][42] and the Deputy Minister of Global Affairs Canada (GAC)[43] about the [redacted] Specifically, a CSE memo provided to the MND[44] clarified the [redacted] arrangement [redacted] However, CSE did not consider this [redacted] which would have required them to seek the updated approval of the MND, as required by the 2012 Ministerial Directive.[45]

23. (TS) However, personnel within CSE's [redacted] involved in managing CSE's [redacted] as part of this operation, noted that:

[redacted]

---

[36] Ministerial Directive, Communications Security Establishment, [redacted] 20 November 2012.
[37] Section 81 of the RELATED PROVISIONS of the *CSE Act* states: "Any arrangement entered into by the former department before the day on which section 76 comes into force continues in accordance with its terms."
[38] *CSE Act,* section 54(2), which states "However, the Establishment may enter into an arrangement with institutions of foreign states, international organizations of states or institutions of those organizations only with the Minister's approval, after the Minister has consulted with the Minister of Foreign Affairs."
[39] See the [redacted] Ministerial Directive, issued 18 August 2006.
[40] CSE letter to the Minister of National Defence, [redacted]
[41] CSE letter to the Minister of National Defence, [redacted]
[42] Chief of CSE letter to Director, [redacted] and letter from [redacted]
[43] CSE Letter to Deputy Minister of Global Affairs Canada, [redacted] However, NSIRA did not receive documentation from GAC.
[44] CSE Document, "Memorandum for the Minister of National Defence: CSE's [redacted]
[45] Ministerial Directive to CSE on [redacted] November 20, 2012.

[redacted][46]

24. (TS//SI) This assessment is supported by NSIRA's review of [redacted] as well as a number of other operational activities performed in the review period, including [redacted][47] Finally, CSE has stated that [redacted]

25. **(U) Finding no. 1: NSIRA finds that CSE has not updated the Minister of National Defence since [redacted] on [redacted] its relationship with a foreign partner ((S) [redacted]).**

(U) Recommendation no. 1: CSE should update the Minister of National Defence on [redacted] its relationship with a foreign partner ((S) [redacted]).

Analytic exchanges [redacted]

26. (TS//SI) [redacted]

[redacted]

[46] CSE Document, "Draft BN – [redacted] This was a draft document authored by CSE's [redacted] and was not circulated to the MND. (Refer to: CSE Email, "RE: Checking in – [redacted] and CSE Factual Accuracy Comments, May 20, 2022.)

[47] Refer to [redacted]

[48] CSE Factual Accuracy Comments, May 20, 2022.

[49] [redacted]

[redacted]

27. (TS//SI) [redacted] [51] In NSIRA's view, the information shared met the definition of analytic exchanges within CSE's MPS.[52]

28. (TS//SI) CSE's MPS requires that the exchange of such analytic information [redacted] must adhere to requirements pertaining to Releasable SIGINT Products (RSPs). Through the [redacted] MA, the MND has imposed a requirement that all RSPs meet the criteria outlined in the MPS prior to disclosure, meaning that following these parameters is a requirement of compliance with the MA.[53] In the MPS, this includes that the RSP must:

a. Include information that has been assessed to be of foreign intelligence value;
b. Be altered to protect the privacy of Canadians and persons in Canada;
c. Be sanitized to protect SIGINT equities, methods, and techniques;
d. Be serialized and traceable,[54]
e. Be caveated as appropriate; and
f. Be approved for release by the appropriate operational release authority, as well the appropriate authority for approving Mistreatment Risk Assessment (MRA) releases.[55]

29. (TS//SI) CSE's sharing of information [redacted] as part of this operation did not always comply with these policy requirements. [redacted]

---

[50] CSE Response to RFI-20, Q4, [redacted] Review, March 4, 2022.
[51] CSE Email, "Determining the need for an MRA for [redacted]
[52] CSE explains that it "conducts analytic exchanges with a variety of partners to [redacted] (Mission Policy Suite, Foreign Intelligence Chapter, Para. 26.15).
[53] CSE Foreign Intelligence Authorization, [redacted] 2020-21, Para. 53(e).
[54] CSE defines serialization and traceability as the assignment of an exclusive identifier to an RSP, [redacted] The nature of serialization is flexible so long as the product is uniquely identifiable, retrievable, and centrally-stored in an approved corporate repository.
[55] CSE Mission Policy Suite, Foreign Intelligence Chapter, Paras. 26.2 and 26.11.5
[56] [redacted] For example, refer to CSE Email, [redacted]
[57] CSE Document, "CSE Update [redacted] and CSE Email, "RE: [redacted] CSE explains that revealing information about its capabilities [redacted]

[redacted][59] As such, in NSIRA's view, CSE's analytical exchanges [redacted] did not always comply with its policies governing such exchanges.

30. **(U) Finding no. 2: NSIRA finds that in the context of a joint operation, CSE's analytic exchanges with a partner ((S) [redacted] did not comply with all of CSE's internal policy requirements relating to such exchanges with [redacted] partners.**

(U) Recommendation no. 2: CSE should comply with the Releasable SIGINT Products requirements pursuant to the Foreign Intelligence Mission Policy Suite when conducting analytic exchanges with [redacted] partners in the performance of all operational activities.

Extent of CSE's participation in [redacted]

31. (TS//SI) In assessing CSE's compliance with the RSP requirement concerning the foreign intelligence value of information collected for such exchanges, NSIRA encountered a matter with broader implications. [redacted]

[redacted] would constitute the revealing of a SIGINT equity, though it appears to have been approved by CSE management – however, the policy requirement is that equities are sanitized [redacted] (Refer to CSE Email, [redacted] CSE stated that in its view, this sharing of equities was in accordance with classification levels. Refer to CSE Factual Accuracy Responses, May 20, 2022.

[58] As part of the eventual risk assessment for this operation, CSE personnel explained to CSE's information sharing unit that caveats are identified in all shared reports, and included an example of a detailed caveat that is typically included in CSE's formal intelligence reporting. NSIRA did not find such caveats included in the materials [redacted] (Refer to: CSE Email, "RE: Determining the need for an MRA for Operation [redacted]

[59] For example, refer to: CSE, Documents, [redacted] "CSE Update [redacted]

[60] The information collected [redacted]

[61] CSE Email, "Determining the need for an MRA for Operation [redacted]

[62] CSE Email, "RE: SORAF activity summary," [redacted]

[63] CSE Factual Accuracy Comments, May 20, 2022.

[redacted]

32. (TS//SI) During the review, CSE took the position that [redacted] In addition, CSE ultimately contradicted the statements [redacted] personnel had made to CSE's information sharing unit, by [redacted]

33. (TS//SI) CSE's collection on [redacted] is not described to the MND within CSE's applications for Ministerial Authorizations authorizing [redacted] activities. In the 2020 and 2021 [redacted] applications to the Minister, the Chief of CSE explains that [redacted] The 2020 and 2021 applications also note that CSE [redacted] [6] The 2019 application provided less detail, noting that: [redacted] [67]

34. (TS//SI) During the review period, CSE explained that [redacted] [8] CSE further explained that [redacted]

---

[64] CSE Response to RFI-14, Q8, [redacted] Review, January 28, 2022.
During the factual accuracy stage, CSE again took the position that, contrary to the primary evidence (i.e. correspondence) NSIRA observed during this review, [redacted] (CSE Factual Accuracy Comments, May 20, 2022). However, NSIRA notes that these objectives pertain to [redacted]

[65] CSE Application for a Foreign Intelligence Authorization, [redacted] Activities 2020-2021, Para. 73(b); CSE Application for a Foreign Intelligence Authorization, [redacted] Activities 2021-2022, Para. 67(b).

[66] CSE Application for a Foreign Intelligence Authorization, [redacted] Activities 2020-2021, Para. 73(b). Note that the 2021-2022 application does not specify [redacted]

[67] Application to the Minister of National Defence for Foreign Intelligence Authorization [redacted] Activities, 2019-2020, page 12.

[68] CSE Response to RFI-20, Q3, [redacted] Review, March 4, 2022.

[redacted] [9] In NSIRA's view, relying on the support [redacted] program as authorized by the Minister.[70] For example, the 2021 application mentions an operation [redacted] to yield foreign intelligence. However, CSE's description of its involvement [redacted] to both the Minister and NSIRA do not mention CSE's collection and sharing [redacted]

35. **(TS) Finding no. 3: NSIRA finds that CSE's applications to the Minister of National Defence for Foreign Intelligence Authorizations for [redacted] Activities did not describe the full extent of CSE's involvement in activities [redacted]**

(TS) Recommendation no. 3: CSE should describe to the Minister of National Defence the full extent of its participation in [redacted] activities when applying for Foreign Intelligence Authorizations.

CSE's Mistreatment Risk Assessment Process

36. (TS//SI) Prior to sharing information with a foreign entity, CSE must conduct a Mistreatment Risk Assessment (MRA) in order to satisfy the requirements of the Ministerial Directions issued in relation to the *Avoiding Complicity in Mistreatment by Foreign Entities Act (ACA)*.[72] In relation to the disclosure of information to any foreign entity that would result in a substantial risk of mistreatment, the Directions require that the Chief must not disclose information unless that risk can be mitigated. CSE has developed MRAs as a mechanism to meet these requirements,[73] noting that this methodology is employed prior to sharing information with

---

[69] CSE Response to RFI-20, Q3, [redacted] Review, March 4, 2022. CSE Application for a Foreign Intelligence Authorization, [redacted] Activities 2020-2021, Para. 73(b).

[70] Such unspecified activities were authorized by the MND in the [redacted] MA, in accordance with s. 26(2)(e) of the CSE Act.

[71] During the factual accuracy stage, CSE agreed that [redacted] Refer to CSE Factual Accuracy Comments, May 20, 2022.

[72] Order in Council, Directions for Avoiding Complicity in Mistreatment by Foreign Entities (Chief of the Communications Security Establishment), September 4, 2019. These directions were issued pursuant to subsection 3(1) of the ACMFEA by the Governor in Council on the recommendation of the MND.

[73] CSE's MRA process seeks "to 1) identify and assess the mistreatment risk; 2) ensure that the approval authorities are commensurate with the mistreatment risk; and 3) not disclose information if the disclosure would result in a substantial risk of mistreatment of an individual." Further, "information must not be disclosed by CSE unless it is accurately and reliably reflective of the intelligence product from which it was obtained." (Refer to Mission Policy Suite, Foreign Intelligence Chapter, Para. 29.1)

foreign entities, and that CSE first establishes the risk level associated with exchanging a specific piece of information before proceeding with the sharing.[74] Further, CSE policy requires that an MRA be undertaken "when disclosing [information] (directly and indirectly) with foreign nations and entities not covered by an Annual MRA."[75] Indeed, to meet its obligations under ACA, an assessment of the risk posed by an information exchange would need to occur prior to the sharing, as stated by CSE's information sharing unit[76] and as CSE explained to the MND.[77]

37. (TS//SI) While the collection of information [redacted] and its sharing [redacted] the MRA process was initiated in [redacted] with some [redacted] personnel stating their belief that such a risk assessment was not necessary prior to any information sharing taking place. In response, the information sharing unit wrote that CSE has a "legal obligation to conduct an MRA for the activity if CSE is the point of exit [redacted] explaining further that:

> CSE must assess the risk of the mistreatment of an individual any time it shares (discloses or requests) information that could be used to identify someone with a foreign entity. [redacted] You have indicated that the information you would share [redacted] This type of information would need to be assessed for the risk of mistreatment prior to any sharing taking place.[79]

Information already shared when Mistreatment Risk Assessment was completed

38. (TS//SI) All of the information that was shared [redacted] as part of this operation was shared via the analytic exchanges described in the previous section, prior to the approval of the MRA on [redacted][80] CSE has explained that the operational team did not perform an MRA

---

[74] CSE Report, "Implementation of the Directions for Avoiding Complicity in Mistreatment by Foreign Entities: January 1, 2020 to December 31, 2020."
[75] Mission Policy Suite, Foreign Intelligence Chapter, Para. 29.6.
[76] CSE Email, "RE: Determining the need for an MRA for Operation [redacted]
[77] CSE Document, "Memorandum for the Minister of National Defence: CSE's [redacted] CSE explained to the Minister that [redacted]
[78] CSE Email, "RE: Determining the need for an MRA for Operation [redacted]
[79] CSE Email, "RE: Determining the need for an MRA for Operation [redacted] Emphasis by NSIRA.
[80] CSE Documents, "CSE Update Dashboard on [redacted] "CSE Update [redacted]

due to a narrow policy exception that lifts the requirement for an MRA [redacted] [1] NSIRA is not satisfied that this exception could have been invoked in the circumstances, given [redacted]

39. (TS//SI) Further, CSE reached an agreement in consultation with the MND, the Privy Council Office (PCO) and the Minister of Foreign Affairs (MFA) in 2017 that a case-by-case MRA would be conducted, as per CSE's internal processes, for sharing [redacted] – superseding any use of the policy exemption cited by CSE in this case.[82] By not completing an MRA prior to sharing the information, CSE did not consider whether there was a substantial risk that information shared could lead to likely mistreatment, thus not assuring itself that the requirements of the Directions and the ACA had been met. Further, CSE's approach did not align with what it had communicated to the MND, PCO and the MFA when describing [redacted]

40. (TS//SI) During the eventual MRA, it was not made clear to CSE personnel performing the risk assessment that substantial information had already been shared [redacted] by CSE. [redacted] personnel explained that the operation was intended to "[redacted] and that "any materials released [redacted] follow the approved equity check process and be issued as end product reports or RSPs where necessary,"[83] indicating that information would only be shared moving forward. Further, the MRA itself states that the information in question [redacted] and notes that [redacted] [84] NSIRA did not find any indication of information previously shared being acknowledged or retroactively assessed as part of the risk assessment process, and is concerned about the apparent lack of transparency about the previous sharing at this stage.

CSE Intelligence Reports, [redacted]
CSE Emails, [redacted] For context see also: CSE Email, "MRA Approval," [redacted] which states that the MRA approved on that date "identifies the approved scope of information sharing with [redacted]

[81] CSE Response to RFI-16, Q5, [redacted] Review, February 4, 2022.
[82] The consultations are referred to in CSE Email, "RE: Checking in – [redacted] and in CSE Document, "Draft BN – MRA and Normalization of [redacted]
[83] CSE Email, "RE: SORAF Help," [redacted] Emphasis by NSIRA.
[84] CSE Document, "MRA [redacted] Pages 3-4.

41. **(U) Finding no. 4: NSIRA finds that CSE did not appropriately apply its Mistreatment Risk Assessment process to information shared with a foreign partner, ((S) [redacted]). CSE conducted a mistreatment risk assessment only after having already shared substantial information with the partner.**

(S) Recommendation no. 4: CSE must perform a Mistreatment Risk Assessment prior to every instance of sharing information [redacted] in accordance with parameters established with the Minister of National Defence, Minister of Foreign Affairs, and the Privy Council Office in the development of CSE's working arrangement with this partner.

MRA not tailored to specific targeted individuals

42. (TS) In determining [redacted] rating for the MRA, CSE referenced the clause of the CSE-[redacted][5] The MRA also notes that [redacted][6] Finally, CSE's MRA assessment [redacted] focused primarily on [redacted] the MRA [redacted]

43. (U) In this context, NSIRA remains concerned about the inconsistencies within the supporting assessment of the MRA, which served as a foundation for [redacted] determined to be associated with this information sharing.

44. (TS//SI) [redacted]

---

[85] CSE Document, "MRA [redacted] See also CSE Response to RFI-16, Q5, February 4, 2022.
[86] CSE Document, "MRA [redacted] Page 2. CSE notes that [redacted]
[87] Indicators of mistreatment [redacted] and in relation to information previously shared [redacted]
[88] CSE Document, "MRA_[redacted] Pages 2-3.

[redacted] As such, NSIRA is concerned that CSE did not fulsomely assess the risk of mistreatment for [redacted] targets of this operation.

45. **(U) Finding no. 5: NSIRA finds that CSE did not appropriately justify [redacted] mistreatment risk for [redacted] targets of an operation.**

(U) Recommendation no. 5: When performing a Mistreatment Risk Assessment, CSE should specify why and how its risk rating applies to each individual implicated in the sharing of information with a foreign partner.

46. (U) Given that these findings directly relate to NSIRA's annual review of the implementation of directions issued under the ACA, this issue will be revisited in NSIRA's next planned review of these activities with a view to determining the compliance of this situation with the ACA and the Directions issues under this Act.

CSE's requirements for a foreignness assessment

47. (TS//SI) CSE is prohibited from directing its activities at Canadians, or persons in Canada.[92] To ensure that CSE is not directing any activities at Canadians, [93] CSE has developed policy requirements for a "foreignness assessment" to establish that the user of a selector is not a Canadian or a person in Canada. Among other things, the policy requires that the assessment

---

[89] CSE Document, "MRA_[redacted] Pages 3-4. Subsequent review of materials demonstrated that [redacted] CSE Email, [redacted]

[90] CSE Response to RFI-16, Q5, [redacted] Review, February 4, 2022. The MRA itself states that [redacted] without an explanation as to how [redacted] was reached. (CSE Document, "MRA_[redacted] Page 5.)

[91] CSE Response to RFI-15, Q5, [redacted] Review, January 28, 2022.

[92] CSE Act, s. 22(1).

[93] The *CSE Act* defines *Canadians* as a Canadian citizen, a permanent resident as defined in subsection 2(1) of the *Immigration and Refugee Protection Act* or a corporation incorporated or continued under the laws of Canada or a province.

meets the threshold of 'reasonable grounds to believe'[94] and be conducted as close as possible to the time of targeting and as required once the activity has been approved.[95]

48. (TS//SI) Through this review, NSIRA learned that CSE's assessment of the foreignness of its targets is primarily the responsibility of intelligence analysts, [redacted] [6] Intelligence analysts may employ certain SIGINT and open source research tools to validate the foreign nature of the selectors being targeted. For instance, the intelligence analyst may "[redacted]" The analyst may also request a formal citizenship status confirmation from Immigration, Refugees, and Citizenship Canada (IRCC) if they have reason to believe the individual could have ties to Canada.[97]

49. (TS//SI) In the context of [redacted] NSIRA learned that intelligence analysts confirmed that the target is not a Canadian [redacted] but that the assessment of foreignness upon which this decision is based is not formally tracked or reviewed by [redacted] management or by CSE's targeting personnel.[98] In NSIRA's view, this practice raises concerns about CSE's targeting procedures, including those related to internal communication and coordination, timeliness, and rigour of foreignness assessments, which NSIRA may examine in more detail as part of subsequent reviews.

CSE's foreignness check on [redacted] targets

50. (TS//SI) As part of its target development efforts, CSE collected information and reported [redacted]. In [redacted] CSE [redacted] initiated the process to confirm with Immigration, Refugees, and Citizenship Canada (IRCC) via the *Security of Canada Information Disclosure Act (SCIDA)* [redacted] Permanent Resident or citizenship status in Canada.[100] [redacted]

---

[94] However, the policy is not clear whether the threshold of "reasonable grounds to believe" is in relation to whether the target is, or is not, a Canadian or person in Canada.
[95] CSE Mission Policy Suite, Foreign Intelligence Chapter, Para. 11.6.
[96] Meeting with CSE personnel regarding targeting justifications, March 4, 2022.
[97] CSE Response to RFI-21, Q2, [redacted] Review, March 25, 2022.
[98] Meeting with CSE personnel regarding targeting justifications, March 4, 2022. CSE personnel communicated that [redacted]
[99] CSE units working on this operation were [redacted]
[100] CSE Email, "Request for SCIDA disclosure [redacted]. CSE Email, "RE: Request for Citizenship Checks," [redacted].

[redacted]

[redacted]

51. (TS//SI) [redacted] CSE further explained that it does not consider citizenship checks to be mandatory, and they are only undertaken when there exist indicators of an individual's ties to Canada.[107]

52. (TS) CSE later referenced [redacted][108] The core

---

[101] For example, see CSE Email, [redacted]
[102] CSE Intelligence Reports, [redacted]
[103] CSE Email, "RE: Request for Citizenship Checks," [redacted]. (See also: IRCC Email, "SCIDA Disclosure [redacted]. CSE could not explain why it took [redacted].)
[104] [redacted]
[105] CSE Response, [redacted] Review, RFI-16, Q1.
[106] [redacted]
[107] Meeting with CSE personnel regarding targeting justifications, March 4, 2022.
[108] CSE Factual Accuracy Comments, May 20, 2022.

materials forming NSIRA's review refuted that statement by [redacted]

53. (TS//SI) As previously noted, subsection 22(1) of the *CSE Act* prohibits CSE from directing its activities at Canadians or persons in Canada. In order to meet this requirement, NSIRA is of the opinion that CSE must conduct a foreignness assessment prior to conducting collection activities against a defined target, in order to meaningfully assess the likelihood that a target is a Canadian or a person in Canada. Indeed, such a requirement is reflected in CSE policy on foreign intelligence.[113] Additionally the [redacted] MA states that: "CSE relies on an assessment of the foreignness of the target before starting [redacted] operations. As a result, CSE has confidence that it is not directing its operations at a Canadian or any person in Canada."[114] Because the Minister's assessment of the proportionality of the authorized activities was partially premised on this statement, NSIRA expects that CSE always assess the foreignness of the target prior to starting activities in support of [redacted] – in line with CSE's statement to the Minister that it does so consistently.

54. (TS//SI) [redacted] as defined in the *CSE Act*, NSIRA questions how CSE [redacted] met its threshold of reasonable grounds to believe[116] – [redacted]

---

[109] CSE Email, "Update on [redacted]
[110] CSE Email, "GCRs," [redacted] CSE Email, "RE: Request for [redacted] This email demonstrates that [redacted]
[111] For example, refer to CSE Email, "Report for [redacted]
[112] CSE Email, "Update on [redacted] Also see CSE Response, [redacted] Review, RFI-15, Q9, February 4, 2022.
[113] Mission Policy Suite, Foreign Intelligence Chapter, Para. 11.6.
[114] CSE Foreign Intelligence Authorization, [redacted] Activities, September 5, 2019, Paras. 14, 25.
[115] Refer to CSE Email, "RE: [redacted]
[116] As required in CSE policy, the foreignness assessment must meet the threshold of reasonable grounds to believe. NSIRA notes that the threshold of reasonable grounds to believe is higher than the standard of reasonable grounds to suspect (*R. v. Mann*, 2004 SCC 52, at para 27).

[redacted]

55. (U) As part NSIRA's recent review of disclosures of information under SCIDA, NSIRA reviewed [redacted] requests for information by CSE to IRCC to confirm the citizenship status of individuals [redacted][117] This represented a [redacted] from [redacted] requests in the previous year,[119] potentially indicating CSE's [redacted] on IRCC's information to perform its activities. In this context, NSIRA has now observed that the long response times associated with SCIDA requests are unlikely to facilitate the timely collection of intelligence to satisfy GC requirements [redacted]

56. (U) At the same time, direct confirmation from the IRCC would achieve a higher degree of certainty as to an individual's *Canadian* status than CSE's internal foreignness assessment in order for CSE to verify that it is not directing its activities against Canadians, in accordance with s. 22(1) of the *CSE Act*. As such, NSIRA encourages CSE to develop an information sharing agreement with IRCC based on the two departments' respective legal authorities and the *Privacy Act,* or develop limited and controlled access to IRCC's databases for the purpose of obtaining timely and concrete confirmation of the citizenship or permanent resident status of its targets, to ensure that it does not direct its activities at Canadians.

57. **(U) Finding no. 6: NSIRA finds that CSE [redacted] collection and reporting activities on an individual, [redacted] before receiving confirmation from Immigration, Refugees, and Citizenship Canada [redacted]**

---

[117] NSIRA Report, "NSIRA and the OPC's review of federal institutions' disclosures of information under the *Security of Canada Information Disclosure Act* in 2020," 2021.

[118] [redacted] requests for citizenship checks in 2019 [redacted] made to IRCC [redacted] to the Canada Border Services Agency (CBSA). CSE then shifted to requesting information about Canadian status from IRCC exclusively rather than CBSA. Refer to CSE Factual Accuracy Comments, May 20, 2022.

[119] NSIRA Report, "NSIRA's 2019 annual report on the disclosure of information under the *Security of Canada Information Disclosure Act*," 2020.

[120] IRCC responded to [redacted]

58. **(U) Finding no. 7: NSIRA finds that CSE does not have a mechanism to obtain timely and concrete verification of a person's Canadian status in order to verify that it is not directing its activities at Canadians.**

(U) Recommendation no. 6: CSE should ensure that a foreignness assessment is completed prior to commencing collection and reporting on individuals. CSE should also develop policy requirements for the documentation, tracking, and management review of foreignness assessments.

(U) Recommendation no. 7: CSE should develop a mechanism with Immigration, Refugees, and Citizenship Canada, or other federal institutions as appropriate, to facilitate timely and concrete confirmation of the Canadian status of individuals implicated in CSE's operational activities.

V. GOVERNANCE AND RISK MANAGEMENT

59. (U) During the review period, CSE took part [redacted] operations led by a partner, in addition [redacted] operations jointly led by CSE and [redacted]

60. (TS//SI) As such, NSIRA set out to understand the governance parameters applied by CSE to each operation, to determine whether the associated activities were appropriately reflective of the risk factors of each operation and aligned with the requirements of the [redacted] MA.

Governance Mechanisms of [redacted] Operations: [redacted]

61. (TS//SI) [redacted]

62. (TS//SI) [redacted]

63. (TS//SI) CSE policy requires that a risk assessment be carried out prior to undertaking any new SIGINT activities that result in the acquisition of data from the GII, and for [redacted] that are [redacted][22] To that end, CSE explained that [redacted]

64. (TS//SI) [redacted]

---

[121] CSE Response, [redacted] Review, RFI-15, Q1, January 28, 2022. CSE explains: [redacted]

[122] Mission Policy Suite, Foreign Intelligence Chapter, Para 8.1. CSE calls this the SIGINT Operational Risk Assessment Framework (SORAF).

[123] CSE Response, [redacted] Review, RFI-15, Q1, January 28, 2022. CSE explains: [redacted]

[124] CSE Document, [redacted] SORAF," [redacted]

[125] [redacted] for example, refer to CSE Email, [redacted] for example, refer to CSE Email, "

[126] CSE Document, [redacted]

[127] CSE Document, [redacted]

[redacted]

65. (TS//SI) [redacted]

66. (TS//SI) In NSIRA's view, [redacted][134] warranted an overarching assessment of all aspects and potential techniques of the operation [redacted] as well as its objectives, implicated capabilities, and associated risks – especially when first approved by CSE in [redacted][135] Through this, CSE would have benefited from a fulsome evaluation of this [redacted] that would have set a clearer standard for [redacted] Further, a risk assessment

---

[128] [redacted] per the materials made available to NSIRA.
[129] CSE Document, [redacted]
[130] CSE Email, "Update on [redacted]
[131] [redacted]
[132] CSE Email, "RE: SORAF activity summary," [redacted]
[133] CSE Email, "RE: SORAF activity summary," [redacted]
[134] CSE Email, "RE: SORAF activity summary," [redacted]
[135] During the factual accuracy stage, CSE took the position that [redacted] In its view, an operational plan and risk assessment "can only be done once there is a strong idea of the direction that the operation will take [redacted] (CSE Factual Accuracy Comments, May 20, 2022). NSIRA is not satisfied with this explanation given [redacted] making it an important aspect of the operation to be assessed for risk.

specific to the [redacted] operation would have better aligned with CSE's policy requirement to conduct a risk assessment in support of [redacted][136] NSIRA believes that [redacted] contributed to the issues identified in the previous chapter in relation to this operation.

67. **(TS) Finding no. 8: NSIRA finds that CSE has not developed policies and procedures to govern its participation in [redacted] within the [redacted] program.**

(TS) Recommendation no. 8: CSE should develop policies and procedures to govern its participation in [redacted] within the [redacted] program.

Governance Mechanisms [redacted] Operations

68. (TS//SI) Certain operations in which the [redacted] program plays a part are managed by CSE's [redacted] partners. In these operations, CSE typically [redacted][137] In these cases, CSE does not conduct a risk assessment or apply any of its formal governance procedures to the operation, because in its view, this is solely the responsibility of the entity conducting the operation.[138] In essence, CSE explained its role is limited to [redacted] and that it is not privy to the risk assessments or other governance processes undertaken by the partner agency. Further, CSE has explained that its operational relationships [redacted]

Case studies in partner-led operations: [redacted]

69. (TS//SI) During the review period, CSE [redacted] partner-led operations: [redacted] operations,

[136] Cite the BN DC SIGINT, See also: CSE Document, [redacted]
[137] CSE Deck, "NSIRA Review of [redacted] Program," February 19, 2021, Slide 12.
[138] Meeting with CSE stakeholders on [redacted] June 22, 2021.
[139] Meeting with CSE stakeholders on [redacted] June 22, 2021.
[140] Meeting with CSE stakeholders on operational activities, July 19, 2021. [redacted]

CSE provided [redacted]

70. (TS//SI) [redacted] CSE did not conduct a risk assessment or apply any of its formal governance procedures to the operations, because in its view, this responsibility rests solely on the entity conducting the operation.[142] CSE also did not consult with its policy or legal units regarding its participation in these initiatives.[143] Accordingly, [redacted] CSE responded that it has "no [redacted] documentation. [redacted] In essence, CSE explained its role as [redacted] and that it was not privy to the risk assessments or other governance processes undertaken by the partner agency.

71. (TS) Further, CSE stated that it applies a policy exception that exempts it from conducting a risk assessment[145] when it is [redacted] This exemption is still subject to conditions, such as the completion of a risk assessment if requested by management, ensuring alignment with data sharing requirements, communication of conditions and caveats associated with the sharing, and ensuring [redacted] Finally, the rationale, conditions for sharing, and management approvals are required to be stored in a corporate repository.[146]

72. (TS//SI) Part of CSE's rationale for leaving the assessment of the risks of an operation to its partners is that it considers the [redacted]

[141] CSE Deck, "NSIRA Review of [redacted] Program," February 19, 2021, Slide 12.
[142] Meeting with CSE stakeholders on [redacted] June 22, 2021.
[143] CSE Response to RFI-01, Follow-up Q2, [redacted] Review, March 19, 2021.
[144] CSE Response to RFI-17, Q1, [redacted] Review, February 11, 2022.
[145] CSE Response to RFI-17, Q2, [redacted] Review, January 28, 2022.
[146] Mission Policy Suite, Foreign Intelligence Chapter, section 25.4.3. Emphasis by NSIRA.
[147] Meeting with CSE stakeholders on [redacted] June 22, 2021.
[148] CSE Response to RFI-15, Q8, [redacted] Review, January 28, 2022.
[149] CSE Email, [redacted] CSE Update [redacted]

[redacted]

73. (TS//SI) [redacted]

74. (TS//SI) NSIRA is not satisfied with CSE's invocation of the [redacted] exemption for not undertaking its governance processes for [redacted]-led operations. These operations, conducted without having undergone a risk assessment or operational plan and without having access to those of the [redacted] partner, [redacted] and in some cases required a substantial amount of dedicated resources. This included dedicating staff resources to [redacted]

---

150 [redacted] CSE Emails, [redacted]
CSE Email, "RE: [redacted]
151 CSE Email, [redacted]
152 [redacted] CSE Emails, [redacted]
153 [redacted] Examples in CSE Emails: [redacted]
"RE: [redacted]
154 CSE Meeting Records [redacted]
CSE Meeting Records [redacted]
CSE Meeting Records [redacted]
CSE Emails, [redacted]
155 Document, [redacted] Emails, [redacted]
156 [redacted] CSE Emails, [redacted]
157 CSE Email, "Draft Update," [redacted]

[redacted] and CSE's contribution to this effort was considered critical to its success.[159]

75. (TS) It is clear that [redacted] For these reasons, NSIRA does not believe the policy exemption for [redacted] nor indeed the nomenclature used by CSE to describe the activities, reflects their true nature [redacted]

76. (TS//SI) CSE has explained that these types of operations may lead to the sharing of foreign intelligence [redacted] if the partner decided to produce an intelligence report summarizing the obtained information and choosing to classify it for release [redacted][161] However, there is no requirement for the partner to route the resulting information back to CSE even if it may meet CSE's goals or intelligence requirements.[162] In fact, CSE explained that [redacted]

---

[158] CSE Email, "RE: Request for update – [redacted] Here, [redacted] personnel described [redacted] See also: CSE Email, [redacted]

[159] [redacted] CSE Email, "Draft Update," [redacted] During the factual accuracy stage, CSE took the position that [redacted] CSE Factual Accuracy Comments, May 20, 2022.) NSIRA is not satisfied with this response, as [redacted] Finally, when requested during the review, CSE did not produce any written record or agreement [redacted] relating to [redacted]

[160] [redacted] See Mission Policy Suite, Foreign Intelligence Chapter, Para 4.1. In NSIRA's view, CSE's participation in [redacted] led operations is reflective of [redacted] particularly given CSE's description of these operations [redacted] and the actual nature of CSE's participation in the operations outlined in this section.

[161] CSE Response to RFI-16, Q22, [redacted] Review, February 8, 2022.

[162] Meeting with CSE personnel on [redacted] June 22, 2021.

[163] CSE Response to RFI-07, Q5, [redacted] Review, September 16, 2021.

[164] CSE Response to RFI-07, Q1, Q2, [redacted] Review, August 13, 2021.

77. (TS//SI) In NSIRA's view, given the potential risks of [redacted] operations, it is prudent for CSE to formalize a governance agreement with partners to identify and manage any risks arising from [redacted] Furthermore, in the [redacted] MA, the MND requires that mutually agreed upon procedures consistent with the terms of the Authorization are in place when CSE provides [redacted][165] As such, NSIRA recommends that CSE create mutually agreed upon procedures with its partners, consistent the terms of any relevant Authorizations, and consult with the Department of Justice (DOJ) when creating such agreements. NSIRA will be interested in examining the role the DOJ plays in informing these types of collaborative CSE activities as part of future reviews.

78. (TS//SI) Additionally, CSE must conduct [redacted] operations "under an approved operational plan, following a rigorous and thorough risk assessment process," as stated to the MND in the [redacted] application.[166] In describing [redacted] to the Minister, CSE affirms that "each [redacted] regardless of duration, is conducted under an approved and tailored operational plan and risk assessment," with the level approval commensurate to the assessed level of risk.[167] CSE did not provide to NSIRA any approved operational plans or risk assessments for [redacted] operations led by its [redacted] partners during the period of review. In NSIRA's view, CSE's [redacted] – and thus must be conducted under an approved operational plan following a rigorous and thorough risk assessment process, considering the possible risks to CSE and its equities from participating in these activities.

79. **(TS) Finding no. 9: NSIRA finds that CSE's contributions to [redacted] operations with its [redacted] partners is not governed by any written arrangements with operational activities [redacted]**

80. **(TS) Finding no. 10: NSIRA finds that CSE's contributions to [redacted] operations led by a [redacted] partner have not been accompanied with the operational planning and risk assessment as described by CSE to the Minister of National Defence.**

---

[165] CSE Foreign Intelligence Authorization, [redacted] 2020-21, Para. 52.
[166] CSE Application for Foreign Intelligence Authorization, [redacted] 2020-21, Paras 74, 78, and 112. CSE further explains that "in instances where an operation involves coordination with international or domestic partners, CSE will also engage in a thorough consultation process." Here, CSE makes it clear to the MND that even for [redacted] operations that involve a domestic or international partner, a thorough consultation process is also to occur, in addition to an operational plan and risk assessment.
[167] CSE Application for Foreign Intelligence Authorization, [redacted] 2020-21, Para 16.

81. **(TS) Finding no. 11: NSIRA finds that CSE does not obtain operational plans or risk assessments developed by its [redacted] partners leading the [redacted] operations, nor contributes to the development of these plans or their associated parameters.**

(TS) Recommendation no. 9: CSE should develop written arrangements with its [redacted] partners implicated in [redacted] activities, to set the parameters for collaborating on these activities.

(TS) Recommendation no. 10: When collaborating on a [redacted] operation with a [redacted] partner, CSE should prepare an operational plan and conduct a risk assessment associated with the activity with a view to ensuring an operation's alignment with CSE's priorities and risk tolerance levels. CSE should also ensure that parameters and any caveats for the partner's [redacted] be outlined and acknowledged.

VI. TESTING TOOLS [redacted]

[redacted]

82. (TS//SI) CSE provided NSIRA personnel a comprehensive walkthrough of the [redacted] program's [redacted] all in support of CSE's foreign intelligence efforts, as well as for the purpose of assisting the RCMP, CSIS and CAF.[168] To ensure that its [redacted] tools are fit-for-purpose, CSE first conducts internal validation checks. Using CSE's internal capabilities, the tools are validated to ensure that they function appropriately, [redacted]

Testing and evaluation of CSE's products

83. (U) Upon learning that CSE tests tools [redacted] NSIRA set out to assess how CSE performed this testing in preparation for operational use [redacted] To that end, NSIRA received a briefing from CSE stakeholders related to the development, validation, and testing requirements

[168] Walkthrough of [redacted] facilities with CSE personnel, July 27, 2021.

conducted on tools prior to their use. NSIRA also requested all testing documentation, including supporting legal analyses, operational plans, as well as lessons learned and post-test reporting.

84. (U) NSIRA expected to find that CSE complied with internal policies and procedures in the performance of its testing and evaluation activities, appropriately assessed and considered the security, legal, and compliance aspects of these activities, and mitigated any associated risks prior to undertaking them.

85. (TS//SI) The MPS sets out a range of requirements pertaining to Testing & Training (T&T) activities, including that they:

a. are not directed at Canadians or any person in Canada, [redacted]

b. that pre-approval must be sought [redacted] where the activity may [redacted] and

c. that collection from testing [redacted] is to be limited to infrastructure information[169] and non-content.[170]

86. (TS//SI) Requirements are also set out for the segregation and retention of data collected from testing and training activities, as well as for the analysis of communications of consenting participants.[171]

87. (S) Following internal testing and validation within a CSE-controlled environment, CSE may choose to test its tools externally. [redacted]

[redacted] *testing case study:* [redacted]

88. (TS//SI) One of CSE's operational activities in the period of review pertained to the testing of [redacted] While not attached to a specific [redacted]

---

[169] Infrastructure information is information relating to any functional component of the Global Information Infrastructure (GII) or events that occur during the interaction of two or more devices that provide services on a network or between an individual and a machine (if the interaction is about only a functional component of the GII). Refer to Mission Policy Suite, Foreign Intelligence Chapter, Para. 12.3.

[170] Non-content is a category of data obtained by CSE that does not reveal purport, and includes both metadata and metadata-like features. Examples: [redacted] Refer to Mission Policy Suite, Foreign Intelligence Chapter Para. 10.5.

[171] MPS, Foreign Intelligence Chapter, Section 12.4.1.

[redacted]

89. (TS//SI) [redacted]

90. (TS//SI) [redacted]

---

[172] CSE Email. "FW: [redacted]
[173] CSE Email, "FOR APPROVAL: [redacted]
[174] CSE Document. "CSE [redacted]
[175] CSE Email, "FW: FOR CONSULTATION: [redacted]
[176] CSE Response to RFI-01, Follow-up Q2, [redacted] Review, March 19, 2021.
[177] CSE Email, "RE: [redacted] Nonetheless, NSIRA did not receive [redacted] that NSIRA received.
[178] [redacted]
[179] CSE Email, "RE: [redacted]
[180] CSE Document. "CSE [redacted]
[181] CSE Document. "CSE [redacted]

[redacted][182]

91. (TS//SI) One of the main features intended to be tested was [redacted]

[redacted][184]

92. (TS//SI) CSE conducted [redacted][185] Ahead of the tests, CSE developed operational plans delineating [redacted][186] Minor deviations from the plan were to be managed by the team lead, while any major or higher-risk departures from the plan would require further approvals.[187] While post-testing summaries of lessons learned were produced following [redacted] testing sessions,[188] this documentation did not enable NSIRA reviewers to assess the test's compliance with its operational plan.

93. (TS//SI) This is the first time that NSIRA has encountered CSE's interpretation and application of the paragraph 23(1)(c)[189] of the *CSE Act* since its coming into force on August 1,

---

[182] CSE Email, "FW: FOR CONSULTATION: [redacted] Data to be acquired during the testing included: [redacted][183]

[184] CSE Email, "FOR APPROVAL: [redacted] See also: CSE Response to RFI-08, Q5, [redacted] Review, August 23, 2021.

[185] CSE Response to RFI-07, Q10, [redacted] Review, September 1, 2021.

[186] CSE Document. [redacted]

[187] CSE Document. [redacted] Details or further specifics pertaining to the factors which would increase the risk are not mentioned, nor are the required approval authorities in these instances.

[188] CSE Document, [redacted]" and CSE Document, [redacted]

[189] Paragraph 23(1)(c) of the *CSE Act* provides that despite subsections 22(1) and (2), the Establishment may carry out any of the following activities in furtherance of its mandate: "testing or evaluating products, software and systems, including testing or evaluating them for vulnerabilities."

2019. As explained by CSE, CSE must dedicate time to capability development, and testing and evaluation is done to ensure CSE's capabilities are effective and compliant prior to operationalization.[190] NSIRA sought to clarify the legal authorities that apply to CSE's testing activities [redacted]

94. (TS//SI) Although not specified in the authorization request, [redacted] CSE explained that it relies on the issued [redacted] MA and paragraph 23(1)(c) of the *CSE Act*.[191] CSE explained that although paragraph 23(1)(c) provides a "narrow exception" to the 'directed at' prohibition in ss. 22(1) and (2) of the *CSE Act*, subsections 22(3) and 22(4) would still apply to testing activities.[192] However, if the testing in support of [redacted] is assessed as being at risk of contravening an Act of Parliament, or acquiring information from the GII that may interfere with a reasonable expectation of privacy of a Canadian or a person in Canada (reasonable expectation of privacy), it is conducted under the [redacted] Authorization.[193] Thus, it appears that CSE leverages both MAs and the exception in paragraph 23(1)(c) to cover [redacted] testing activities that risk amounting to a contravention of an Act of Parliament or interfering with a reasonable expectation of privacy.

95. (TS//SI) Due to the narrow exception provided for in paragraph 23(1)(c), and its novelty,[194] NSIRA considers it necessary for the Chief's applications to inform the Minister that [redacted] testing activities in support of the mandate might risk contravening ss. 22(1) and (2), an Act of Parliament, or interfere with a reasonable expectation of privacy, and therefore the authorization may be used to support such activities. NSIRA notes that while such testing activities may be reasonable in the circumstances and reasonably necessary to aid other authorized activities,[195] it is important for the Minister to be informed of these activities. This information can enable the Minister to include any terms, conditions or restrictions [redacted] to ensure the reasonableness and proportionality of an activity.[196]

---

[190] CSE Response to RFI-14, [redacted] Review, January 28, 2022.
[191] This section permits CSE to conduct the described activities[191] without contravening the prohibition on directing activities at Canadians or persons in Canada in s. 22(1) of the *CSE Act*.
[192] CSE Response to RFI-14, Q10, [redacted] Review, January 28, 2022. These subsections require a Ministerial Authorization for any activities performed in furtherance of the foreign intelligence or cybersecurity aspects of CSE's mandate that contravene an Act of Parliament or involve the acquisition of information on or through the GII that interfere with a reasonable expectation of privacy.
[193] CSE Response to RFI-14, Q3, [redacted] Review, January 28, 2022.
[194] A similar provision was not included in the *National Defence Act*.
[195] *CSE Act*, Para. 26(2)(e).
[196] *CSE Act*, Para. 35(d).

96. **(U) Finding no. 12: NSIRA finds that CSE's application for the [redacted] Authorization did not inform the Minister of National Defence that it intends to conduct testing and evaluation activities under the authority of the Authorization.**

(U) Recommendation no. 11: When applying for a Ministerial Authorization, CSE should disclose to the Minister any related testing or evaluation activities that it intends to undertake pursuant to paragraph 23(1)(c) of the *CSE Act*.

[redacted] *testing case study:* [redacted]

97. (TS//SI) During the review period, CSE also performed testing of [redacted]

98. (TS//SI) [redacted][2]

99. (TS//SI) [redacted]

---

197 [redacted]
198 CSE Draft Document, "Operation [redacted]
199 Please refer to Annex C for more information about [redacted]
200 CSE Email, "FW: [redacted] The testing was conducted [redacted]
201 The authority permitting CSE to conduct these testing activities was [redacted]
202 CSE Email, "RE: [For Approval] [redacted]
203 CSE Email, "Validation of [redacted]

[redacted]

100. (TS//SI) While the associated [redacted] did not occur, the issues underpinning it are important from an efficacy perspective. Both CSE [redacted]

101. (TS//SI) In NSIRA's view, developing capabilities separate from specific operations – [redacted] – is a reasonable approach that allows CSE to leverage a tool if the need arises, modifying it as necessary for the specific operational elements. As such, NSIRA encourages CSE to continue to develop tools and capabilities separately from specific operations where possible.

[redacted] *Testing*

102. (TS//SI) During the review period, CSE planned to conduct testing similar to its [redacted] To that end, CSE prepared a risk assessment concerning an operational test of [redacted] [09]

---

[204] CSE Response to RFI-16, Q15, [redacted] Review, February 25, 2022.
[205] CSE Email, [redacted]
[206] CSE Email, "RE: [redacted] See also: CSE Email. [redacted]
[207] [redacted]
[208] Initial discussions indicated that testing could take place [redacted] However, this would have required CSE to [redacted]
[209] CSE Response to RFI-14, Q5, [redacted] Review, January 28, 2022.
CSE Email, [redacted]

VII. CSE'S RESPONSIVENESS AND PROVISION OF INFORMATION

103. (U) This review was undertaken from January 2021 to April 2022. During this time, NSIRA encountered significant delays in the provision of review information by CSE, as well as resistance to the scope of the review as identified in the review's Terms of Reference.[210] CSE's resistance to the scope of this review resulted in the substantially delayed provision of key review materials.[211] CSE's provision of some key review materials four months after the initial request was unacceptable, and caused undue delays and difficulties for NSIRA personnel during the course of this review, ultimately contributing to a delay in its completion.[212]

104. (U) In addition, midway through the review, CSE imposed highly restrictive settings on a new information technology system, which was then used to provide review materials to reviewers. These restrictive settings posed a significant impediment to NSIRA's review activities, preventing reviewers from performing basic information management and analytical tasks.

105. (U) Together, these challenges contributed to delays on this review, and prevented NSIRA from performing a thorough verification of the information provided by CSE upon the conclusion of the review. In relation to its search methodology, CSE explained that it relied on the identification of the correct stakeholders within CSE with access to the information. The identified stakeholders then retrieved the information and provided it to the CSE review liaison team or would direct the liaison team to locate the required information. CSE explained the various repositories used to locate specific documentation over the course of the review period as well as its methodology for Outlook searches.

106. (U) Nonetheless, during the course of this review, NSIRA reviewers identified the existence of certain responsive materials that had not been provided by CSE. While CSE explained that it tends to "err on the side of inclusion when providing relevant documents," its justifications for not providing the identified information tended to be that the stakeholders searched information holdings to provide NSIRA with information deemed to be the "most recent, relevant, and highest value to NSIRA."[213]

---

[210] Meeting with CSE liaison unit to clarify review process and scope, August 10, 2021.
CSE Email to NSIRA, "FW: [redacted] Review: RFI-05," July 6, 2021.
[211] NSIRA requested documentation associated with all operational activities performed in support of the [redacted] program as part of RFI-05 on June 29, 2021. Materials specific to each operation began to be provided on September 9, 2021, with substantive document provision ongoing until December 2021. Annex D summarizes the timelines associated with the provision of materials by CSE in support of this review.
[212] CSE also later expressed resistance to the scope of another NSIRA review presently undertaken, which manifested in similar delays in CSE's provision of information required a part of that review.
[213] CSE Response. RFI-23 Q1.

107. (U) Additionally, in responding to NSIRA's request regarding its search methodology, CSE identified over one hundred emails that were responsive to previous RFIs and were only provided to NSIRA during the factual accuracy stage (after the report had been drafted).[214] CSE stated that this information was inadvertently omitted when all other review materials were transferred to reviewers. This event is in line with previous reviews where CSE identified information relevant to the review at very late stages of the review process.

108. (U) Upon request, CSE also provided to NSIRA a list of documents, identified but not provided to NSIRA alongside a rationale. CSE claimed that certain documents contained Exceptionally Compartmented Information (ECI) information owned by [redacted] and therefore were out of CSE's control to disseminate further. NSIRA finds this rationale wholly unsupported. Should documents contain ECI information, NSIRA would expect to receive the appropriate indoctrination in order to access the materials. Furthermore, NSIRA should be made aware of the existence of this information during the research and analysis stages of the review in order to resolve the issue prior to the report's completion.

109. (U) Altogether, these issues have resulted in NSIRA's limited confidence in the completeness of information provided throughout this review and high dissatisfaction with the responsiveness of CSE.

VIII. CONCLUSION

110. (TS) The goals and objectives of the [redacted] program are those that can effectively enable CSE to fill important gaps relating to Canada's key intelligence requirements. The program has extensive and varied technical expertise that can enable CSE [redacted] to collect information that would address these gaps.

111. (TS//SI) At the same time, the novel nature of certain [redacted] activities, such as [redacted] warrants a close examination of the operational activities and their associated risks in order to lead the governance model for these activities toward greater maturity. Careful management of [redacted] operations and all of the program's associated activities is particularly important given the nature of the program's [redacted] targets – [redacted] Inadequate management of risks and associated equities in this context could lead to increased vulnerabilities, challenges to Canada's international relations, and reputational harm.

---

[214] The emails were pertaining to [redacted] an operation that served as the basis for several case studies throughout the report.

112. (TS) NSIRA recognizes that while changes in CSE's corporate governance processes may have contributed to this lack of consistency, with the recent adoption of a uniform risk assessment mechanism, it would be prudent for CSE to ensure all operations within the purview of the [redacted] program are subject to a thorough governance regime. Given the present absence of such a regime, and given the early stages of [redacted] NSIRA believes that the development of clear policies and procedures for [redacted] activities is an appropriate next step – especially if CSE is to undertake more complex and sensitive [redacted] operations as the function matures.

ANNEX A: CSE Briefings

113. (TS//SI) Meetings with CSE Stakeholders

- February 19, 2021: Preliminary briefing introducing the program
- June 22, 2021: Discussion on [redacted]
- July 19, 2021: Briefing on operational activities
- July 27, 2021: Technical briefing on [redacted] activities
- August 10, 2021: Meeting with liaison unit to clarify review process and scope
- September 28, 2021: Discussion about [redacted] program
- March 4, 2022: Meeting with [redacted] stakeholders and CSE's targeting unit to review targeting justifications for [redacted] targets

ANNEX B: List of Operations

Operation	Type	Status	Notes
[redacted]			

[215] Given that this operation falls within the scope [redacted]

[216] Given that this operation falls within the scope [redacted]

[217] During the factual accuracy stage, CSE stated that it does not, in fact, have an ongoing operation by this name, while the operation [redacted] This contradicts a previous CSE response to an NSIRA request for information, in which CSE states that the operation is ongoing.

ANNEX C: [redacted]

[redacted]

(TS//SI) [redacted]

[redacted]

[redacted]

(TS//SI) [redacted]

[redacted]

ANNEX D: CSE's Responses to NSIRA's Requests for Information

RFI # Response Part	Type	Requested	Deadline	Received	Business Days Early/Late
RFI-1 part 1	Documents	26-Jan-21	12-Feb-21	12-Feb-21	0
RFI-1 part 2	Briefing	26-Jan-21	19-Feb-21	19-Feb-21	0
RFI-1 part 3	Questions	3-Mar-21	19-Mar-21	19-Mar-21	0
RFI-2 part 1	Documents	19-Mar-21	6-Apr-21	6-Apr-21	0
RFI-2 part 2	Questions	19-Mar-21	6-Apr-21	8-Apr-21	2
RFI-2 part 3	Questions	19-Mar-21	6-Apr-21	13-Apr-21	5
RFI-2 part 4	Documents	19-Mar-21	6-Apr-21	23-Apr-21	13
RFI-2 part 5	Documents	19-Mar-21	6-Apr-21	30-Apr-21	18
RFI-2 part 6	Documents	19-Mar-21	6-Apr-21	18-Jun-21	53
RFI-2 part 7	Documents	19-Mar-21	6-Apr-21	30-Jun-21	61
RFI-2 part 8	Documents	19-Mar-21	6-Apr-21	23-Jul-21	78
RFI-3 part 1	Documents	3-Jun-21	17-Jun-21	17-Jun-21	0
RFI-4 part 1	Briefing	17-Jun-21	2-Jul-21	19-Jul-21	11[218]
RFI-5 part 20	Documents	29-Jun-21	16-Jul-21	29-Nov-21	96
RFI-5 part 1	Documents	29-Jun-21	16-Jul-21	16-Jul-21	0
RFI-5 part 10	Documents	29-Jun-21	16-Jul-21	25-Aug-21	28
RFI-5 parts 11 and 12	Documents	29-Jun-21	16-Jul-21	17-Sep-21	45
RFI-5 part 13	Documents	29-Jun-21	16-Jul-21	24-Sep-21	50
RFI-5 part 14	Documents	29-Jun-21	16-Jul-21	18-Oct-21	66
RFI-5 part 15	Documents	29-Jun-21	16-Jul-21	12-Oct-21	62
RFI-5 part 16	Documents	29-Jun-21	16-Jul-21	4-Oct-21	56
RFI-5 parts 17 and 18	Documents	29-Jun-21	16-Jul-21	12-Oct-21	62
RFI-5 part 19	Documents	29-Jun-21	16-Jul-21	8-Oct-21	60
RFI-5 part 2	Documents	29-Jun-21	16-Jul-21	21-Jul-21	3
RFI-5 part 3	Documents	29-Jun-21	16-Jul-21	22-Jul-21	4
RFI-5 part 4	Documents	29-Jun-21	16-Jul-21	23-Jul-21	5
RFI-5 part 5	Documents	29-Jun-21	16-Jul-21	4-Aug-21	13
RFI-5 parts 7 and 8	Documents	29-Jun-21	16-Jul-21	9-Sep-21	39
RFI-5 part 9	Questions	29-Jun-21	16-Jul-21	25-Aug-21	28

[218] In this circumstance, NSIRA accepted that the delay was both a result of NSIRA's availability and CSE's internal pressures. This delay is therefore not at issue.

RFI # Response Part	Type	Requested	Deadline	Received	Business Days Early/Late
RFI-6 parts 1 and 2	Questions	26-Jul-21	6-Aug-21	9-Sep-21	24
RFI-7 part 1	Questions	30-Jul-21	13-Aug-21	13-Aug-21	0
RFI-7 parts 2 and 3	Documents	30-Jul-21	13-Aug-21	9-Sep-21	19
RFI-7 part 4	Questions	30-Jul-21	13-Aug-21	16-Sep-21	24
RFI-7 part 5	Questions	30-Jul-21	13-Aug-21	24-Sep-21	30
RFI-7 part 6	Documents	30-Jul-21	13-Aug-21	27-Sep-21	31
RFI-8 part 1	Questions	12-Aug-21	27-Aug-21	23-Aug-21	-6
RFI-10 part 1	Questions	6-Oct-21	20-Oct-21	27-Oct-21	5
RFI-9 part 1	Documents	6-Oct-21	20-Oct-21	15-Oct-21	-5
RFI-9 part 2	Documents	6-Oct-21	20-Oct-21	27-Oct-21	5
RFI-11 part 1	Documents	13-Oct-21	27-Oct-21	27-Oct-21	0
RFI-11 part 2	Documents	13-Oct-21	27-Oct-21	28-Oct-21	1
RFI-12 part 1	Questions	3-Nov-21	17-Nov-21	24-Nov-21	5
RFI-13 part 1	Documents	3-Nov-21	17-Nov-21	17-Nov-21	0
RFI-13 part 2	Documents	3-Nov-21	17-Nov-21	17-Nov-21	0
RFI-14 part 1	Documents	17-Nov-21	8-Dec-21	23-Dec-21	11
RFI-14 part 2	Documents	17-Nov-21	8-Dec-21	5-Jan-22	20
RFI-14 parts 3 and 4	Questions	17-Nov-21	8-Dec-21	28-Jan-22	37
RFI-14 part 5	Questions	17-Nov-21	8-Dec-21	14-Feb-22	48
RFI-15 part 1	Questions	18-Nov-21	9-Dec-21	28-Jan-22	36
RFI-15 part 2	Questions	18-Nov-21	9-Dec-21	4-Feb-22	41
RFI-15 part 3	Documents and Questions	18-Nov-21	9-Dec-21	14-Feb-22	47
RFI-17 part 1	Questions	18-Nov-21	9-Dec-21	28-Jan-22	36
RFI-17 part 2	Questions	18-Nov-21	9-Dec-21	11-Feb-22	46
RFI-18 part 1	Questions	18-Nov-21	9-Dec-21	30-Nov-21	-9
RFI-18 part 2	Request	18-Nov-21	9-Dec-21	19-Nov-21	-16
RFI-16 part 1	Documents	22-Nov-21	13-Dec-21	29-Nov-21	-12
RFI-16 parts 2 and 3	Documents	22-Nov-21	13-Dec-21	17-Dec-21	4
RFI-16 part 4	Documents	22-Nov-21	13-Dec-21	20-Dec-21	5
RFI-16 part 5	Questions	22-Nov-21	13-Dec-21	4-Feb-22	39
RFI-16 part 6	Questions	22-Nov-21	13-Dec-21	9-Feb-22	42
RFI-19 part 1	Documents and Questions	18-Jan-22	8-Feb-22	11-Feb-22	3
RFI-20 part 1	Questions	11-Feb-22	4-Mar-22	4-Mar-22	0
RFI-21 part 1	Questions	4-Mar-22	25-Mar-22	25-Mar-22	0
RFI-22 part 1	Questions	18-Mar-22	4-Apr-22	4-Apr-22	0

ANNEX E: Findings and Recommendations

Findings

(U) Finding no. 1: NSIRA finds that CSE has not updated the Minister of National Defence since [redacted] on [redacted] its relationship with a foreign partner ((S) [redacted].

(U) Finding no. 2: NSIRA finds that in the context of a joint operation, CSE's analytic exchanges with a partner ((S) [redacted] did not comply with all of CSE's internal policy requirements relating to such exchanges with [redacted] partners.

(TS) Finding no. 3: NSIRA finds that CSE's applications to the Minister of National Defence for Foreign Intelligence Authorizations for [redacted] Activities did not describe the full extent of CSE's involvement in activities [redacted]

(U) Finding no. 4: NSIRA finds that CSE did not appropriately apply its Mistreatment Risk Assessment process to information shared with a foreign partner, ((S) [redacted]). CSE conducted a mistreatment risk assessment only after having already shared substantial information with the partner.

(U) Finding no. 5: NSIRA finds that CSE did not appropriately justify [redacted] mistreatment risk for [redacted] targets of an operation.

(U) Finding no. 6: NSIRA finds that CSE [redacted] collection and reporting activities on an individual, [redacted] before receiving confirmation from Immigration, Refugees, and Citizenship Canada [redacted]

(U) Finding no. 7: NSIRA finds that CSE does not have a mechanism to obtain timely and concrete verification of a person's Canadian status in order to verify that it is not directing its activities at Canadians.

(TS) Finding no. 8: NSIRA finds that CSE has not developed policies and procedures to govern its participation in [redacted] within the [redacted] program.

(TS) Finding no. 9: NSIRA finds that CSE's contributions to [redacted] operations with its [redacted] partners are not governed by any written arrangements with operational activities [redacted]

(TS) Finding no. 10: NSIRA finds that CSE's contributions to [redacted] operations led by a [redacted] partner have not been accompanied with the operational planning and risk assessment as described by CSE to the Minister of National Defence.

(TS) Finding no. 11: NSIRA finds that CSE does not obtain operational plans or risk assessments developed by its [redacted] partners leading the [redacted] operations, nor contributes to the development of these plans or their associated parameters.

(U) Finding no. 12: NSIRA finds that CSE's application for the [redacted] Authorization did not inform the Minister of National Defence that it intends to conduct testing and evaluation activities under the authority of the Authorization.

Recommendations

(U) Recommendation no. 1: CSE should update the Minister of National Defence on [redacted] its relationship with a foreign partner ((S) [redacted]).

(U) Recommendation no. 2: CSE should comply with the Releasable SIGINT Products requirements pursuant to the Foreign Intelligence Mission Policy Suite when conducting analytic exchanges with [redacted] partners in the performance of all operational activities.

(TS) Recommendation no. 3: CSE should describe to the Minister of National Defence the full extent of its participation in [redacted] activities when applying for Foreign Intelligence Authorizations.

(S) Recommendation no. 4: CSE must perform a Mistreatment Risk Assessment prior to every instance of sharing information [redacted] in accordance with parameters established with the Minister of National Defence, Minister of Foreign Affairs, and the Privy Council Office in the development of CSE's working arrangement with this partner.

(U) Recommendation no. 5: When performing a Mistreatment Risk Assessment, CSE should specify why and how its risk rating applies to each individual implicated in the sharing of information with a foreign partner.

(U) Recommendation no. 6: CSE should ensure that a foreignness assessment is completed prior to commencing collection and reporting on individuals. CSE should also develop policy requirements for the documentation, tracking, and management review of foreignness assessments.

(U) Recommendation no. 7: CSE should develop a mechanism with Immigration, Refugees, and Citizenship Canada, or other federal institutions as appropriate, to facilitate timely and concrete confirmation of the Canadian status of individuals implicated in CSE's operational activities.

(TS) Recommendation no. 8: CSE should develop policies and procedures to govern its participation in [redacted] within the [redacted] program.

(TS) Recommendation no. 9: CSE should develop written arrangements with its [redacted] partners implicated in [redacted] activities, to set the parameters for collaborating on these activities.

(TS) Recommendation no. 10: When collaborating on a [redacted] operation with a [redacted] partner, CSE should prepare an operational plan and conduct a risk assessment associated with the activity with a view to ensuring an operation's alignment with CSE's priorities and risk tolerance levels. CSE should also ensure that parameters and any caveats for the partner's [redacted] be outlined and acknowledged.

(U) Recommendation no. 11: When applying for a Ministerial Authorization, CSE should disclose to the Minister any related testing or evaluation activities that it intends to undertake pursuant to paragraph 23(1)(c) of the CSE Act.