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

REVIEW OF CSE'S ACTIVE AND DEFENSIVE CYBER OPERATIONS

NSIRA // Review 2021 - 09

TOP SECRET // SI // CEO // SOLI-CLI

Table of Contents

I. EXECUTIVE SUMMARY

1. (U) The *Communications Security Establishment Act* granted CSE the authority to conduct Active Cyber Operations and Defensive Cyber Operations (ACOs and DCOs). CSE ACOs and DCOs have become a tool of Government of Canada foreign and security policy. In 2021, NSIRA reviewed the governance, as well as the general planning and approval process, of ACO and DCO activities. The Governance Review made several observations about CSE's—and to a lesser extent, GAC's—governance of ACOs and DCOs, and some of these observations identified gaps that resulted in recommendations. Building on the Governance Review, the present report focuses on CSE's ACOs and DCOs themselves; in other words, the review examines the operations, analyzing the implementation of CSE's governance and legal framework in the context of specific ACOs and DCOs.

2. (U) NSIRA incorporated GAC, CSIS, RCMP, and DND/CAF into this review given these organizations' varying degrees of coordination or involvement in CSE's ACOs and DCOs. NSIRA also inspected some technical elements of one case study ACO to verify aspects of the operation independently, as well as to deepen NSIRA's understand of how an ACO works. While NSIRA reviewed all ACOs and DCOs planned or conducted by CSE until mid-2021, this review focused on four such ACOs or DCOs, selected based on having different characteristics from one another.

3. (U) Overall, NSIRA found that ACOs and DCOs that CSE planned or conducted during the period of review were lawful, and noted improvements in GAC's assessments for foreign policy risk and international law. NSIRA further observed that CSE developed and improved its processes for the planning and conduct of ACOs and DCOs in a way that reflected some of NSIRA's observations from the Governance Review.

4. (U) However, NSIRA also made findings pertaining to how CSE could improve aspects of ACO and DCO planning, as well as to communication to the Minister of National Defence and coordination with other Government of Canada entities. More specifically, NSIRA identified areas of potential risk in terms of:

- GAC's capability to independently assess potential risks resulting from CSE ACOs and DCOs;
- The accuracy of information provided, and issues related to delegation, within some of the applications for authorizations for ACOs and DCOs;
- The degree to which CSE engaged with CSIS and RCMP on ACOs and DCOs, and CSE explanations of how it determined whether the objective of an ACO or DCO could not reasonably be achieved by other means;
- The extent to which CSE described the intelligence collection that may occur alongside or as a result of ACOs or DCOs in applications for ACO and DCO authorizations and in operational documentation; and
- Overlap between activities conducted under the ACO and DCO aspects of CSE's mandate, as well as between all four aspects of CSE's mandate.

5. (U) As has been the case in all previous reviews of CSE, NSIRA faced significant challenges in accessing CSE information on this review. These access challenges had a negative impact on the

review. As a result, NSIRA cannot be confident in the completeness of information provided by CSE, and is dissatisfied with CSE's responsiveness.

List of Acronyms

ACO – Active Cyber Operation

CAILS – Constitutional, Administrative and International Law Section (Department of Justice)

[redacted]

CCCS – Canadian Centre for Cyber Security (Cyber Centre), part of CSE

[redacted]

CFIOG – Canadian Forces Information Operations Group (within DND/CAF)

CNE – Computer Network Exploitation, see Glossary of Terms

[redacted]

[redacted]

CSE – Communications Security Establishment

CSE Act – *Communications Security Establishment Act*

CSIS – Canadian Security Intelligence Service

DCO – Defensive Cyber Operation

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

DLS – Directorate of Legal Services (CSE)

FCO – Foreign Cyber Operations

FPCO – Federal Policing Criminal Operations (RCMP)

FPRA – Foreign Policy Risk Assessment (GAC)

GAC – Global Affairs Canada

GC – Government of Canada

[redacted]

GII – Global Information Infrastructure

HRLS – Human Rights Law Section (Department of Justice)

[redacted]

JCAD – Joint Cyber Authorities Document (CSE), see Glossary of Terms

JCOP – Joint Cyber Operations Plan (CSE), see Glossary of Terms

JPAF – Joint Planning and Authorities Framework (CSE), see Glossary of Terms

[redacted]

MFA – Minister of Foreign Affairs

[redacted]

MND – Minister of National Defence

MoU – Memorandum of Understanding

[redacted]

[redacted]

MPS – Mission Policy Suite (CSE)

NSIA – National Security and Intelligence Advisor (to the Prime Minister)

[redacted]

OPP – Ontario Provincial Police

PCO – Privy Council Office

[redacted]

PS – Public Safety Canada

RCMP – Royal Canadian Mounted Police

RFI – Request for Information

SIGINT – Signals Intelligence

SITE TF – Security and Intelligence Threats to Elections Taskforce, consisting of CSE, CSIS, GAC, and RCMP

SME – Subject-Matter Expert

[redacted]

[redacted]

[redacted]

Glossary of Terms

Chief. In this report, 'Chief' refers to the Chief of CSE.

Computer Network Exploitation (CNE). Computer Network Exploitation techniques are undertaken to covertly gain access to computers, computer networks, data networks, personal devices and other computer-controlled equipment.

[redacted]

Five Eyes. This term refers to the intelligence-sharing partnership between Canada, the United States of America, the United Kingdom, Australia, and New Zealand.

Joint Cyber Authorities Document (JCAD). The JCAD is a high-level policy document that organizes cyber operation authorities by theme, [redacted]

Joint Planning and Authorities Framework (JPAF). Referred to throughout this report as CSE's 'cyber operations framework', the JPAF is the governance framework that oversees the development and conduct of CSE's cyber operations. It applies to all ACOs and DCOs.

[redacted]

II. AUTHORITIES

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

III. INTRODUCTION

Review Background

7. (U) The *Communications Security Establishment Act*[2] granted CSE the authority to independently conduct Active Cyber Operations and Defensive Cyber Operations (henceforth: ACOs and DCOs, or 'cyber operations') for the first time.[3] CSE cyber operations have become a tool of Government of Canada foreign and security policy.

8. (U) In 2021, the National Security and Intelligence Review Agency (NSIRA) reviewed the governance, as well as the general planning and approval process, of ACO and DCO activities taking place until the end of August, 2020 (henceforth: Governance Review).[4] The Governance Review made several observations about CSE's—and to a lesser extent, GAC's—governance of ACOs and DCOs, and some of these observations identified gaps that resulted in recommendations. The Governance Review also raised various questions pertaining to how CSE and GAC governance structures are implemented or followed in practice.

9. (U) Building on the Governance Review, this report focuses on CSE's ACOs and DCOs themselves; in other words, the review examines the operations. The report thus examines the operationalization and implementation of CSE's governance and legal framework in the context of specific ACOs and DCOs, building on observations made in the Governance Review. NSIRA requested information pertaining to all ACOs and DCOs that were considered, planned, or conducted prior to July 30, 2021. As such, the findings and recommendations made throughout this report pertain to the facts of cyber operations as they existed in the period of review.[5]

10. (TS//SI) ACOs and DCOs [redacted] which facilitate cyber operations activities. Given this, NSIRA considered or examined elements of [redacted]

[1] *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 2.
[2] *Communications Security Establishment Act*, SC 2019, c 13, s 76 [*CSE Act*].
[3] Throughout this report, the term 'cyber operations' is used interchangeably with the term 'ACOs and DCOs'. While CSE and other GC departments use the term 'foreign cyber operations' (FCO) to describe ACOs and DCOs, NSIRA used language from the *CSE Act* for clarity.
[4] Review of CSE's Governance of Active and Defensive Cyber Operations (NSIRA Review 20-02).
[5] In some cases, NSIRA was able to view or otherwise learn of updates made since July 30, 2021. When these updates are relevant or responsive to analysis in this report, NSIRA has noted accordingly. However, NSIRA was not necessarily informed of all relevant updates after July 30, 2021.

11. (U) This report is structured in the following manner. The report begins with contextual information about ACOs and DCOs. Section IV summarizes four case studies of ACOs and/or DCOs, which serve as the core examples throughout the analysis. Section V details NSIRA's observations, findings, and recommendations pertaining to cyber operations—including but not limited to NSIRA's four case studies—during the period of review. This section is further divided into thematic areas, with the bulk of the analysis focused on:

- Assessments for foreign policy and legal risk;
- The conditions for issuing ACO and DCO authorizations, especially the requirements of subsections 34(1) and 34(4) of the *CSE Act*; and
- Differentiating between ACOs, DCOs, and other CSE activities.

12. (U) The report concludes, in Section VI, with a summary of CSE's overall responsiveness to NSIRA during this review, and supplemental detail or accompanying information is included in annexes.

Methodology

13. (U) NSIRA analyzed a wide range of information in CSE's possession, including extensive documentation related to: process, legal advice, technical detail, consultation with other stakeholders or partners, post-operational assessment, and more. Documents provided to NSIRA included correspondence among CSE personnel and with partners in relation to specific operations and components of operations. NSIRA also received three briefings and two technical demonstrations from CSE subject-matter experts.

14. (U) In addition to information from CSE, NSIRA received information from GAC, CSIS, RCMP, and DND/CAF in the review to fully pursue lines of inquiry. NSIRA analyzed documentation from all four organizations, and received dedicated briefings from GAC, CSIS, and DND/CAF. Across all reviewee departments and agencies, NSIRA made over 30 requests for information (including for briefings) as part of this review.

15. (U) As was described in NSIRA's Terms of Reference (ToR) for this review, this review was intended to test forms of direct access to CSE's information repositories. As is further discussed in Section VI of this report, CSE did not consent to progress on direct access to CSE information holdings, and the review was negatively impacted by challenges in accessing CSE information.

ACO and DCO Background

What are Defensive and Active Cyber Operations?

16. (U) Defensive Cyber Operations (DCOs) are activities on or through the global information infrastructure (GII) to help protect federal institutions' electronic information and information infrastructures and those designated by the Minister of National Defence (MND) as being of importance to Canada.[6] For example, DCOs could be activities that stop or impede foreign cyber threats before they

[6] *CSE Act*, section 18: "The defensive cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to help protect (a) federal institutions' electronic information and information infrastructures; and (b) electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada."

reach Canada's [redacted] Active Cyber Operations (ACOs) are activities on or through the GII 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 internal affairs, defence or security.[7] ACOs allow the Government of Canada (GC) to use CSE's online capabilities to undertake a range of activities in cyberspace that limit an adversary's ability to negatively impact Canada's international relations, defence, or security. The impacts of ACOs and DCOs, as directly experienced by the target, are referred to as the 'effects' of an ACO or DCO.

17. (S) To conduct ACOs and DCOs, CSE relies on its existing access to the GII, foreign intelligence expertise, and domestic and international partnerships to obtain relevant intelligence to support the development of cyber operations.

18. (S) The preliminary gathering of intelligence, [redacted] comprises the majority of the work necessary to conduct an ACO or DCO, whereas the resulting activity in cyberspace [redacted] is only a small component of the overall operation.

Legal foundation for conducting cyber operations

19. (U) The *CSE Act* provides the legal authority for CSE to conduct ACOs and DCOs, and these aspects of the mandate are described in sections 19 and 18 of the Act, respectively. Importantly, the *CSE Act* limits ACOs and DCOs in that they cannot be directed at a Canadian or any person in Canada and cannot infringe on the *Charter of Rights and Freedoms;*[8] nor can they be directed at any portion of the GII within Canada.[9]

20. (U) ACOs and DCOs must be conducted under an authorization issued by the Minister of National Defence (MND) under subsection 29(1) (DCO) or under subsection 30(1) (ACO) of the *CSE Act.*[10] The authorization regime in the *CSE Act* provides CSE with the authority to conduct the activities or classes of activities listed in section 31 of the *CSE Act* in furtherance of the ACO or DCO aspects.[11] ACO and DCO authorizations permit CSE to conduct ACO or DCO activities despite any other Act of Parliament or of any foreign state.[12] In order to issue an authorization, the MND must conclude that there are reasonable grounds to believe that any activity that would be authorized by it is reasonable and proportionate,[13] and must also conclude that the objective of the cyber operation could not reasonably be achieved by other means and that no information will be acquired under the

---

[7] *CSE Act*, section 19: "The active cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to 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."

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

[9] *CSE Act*, paragraph 22(2)(a). *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

[10] *CSE Act,* paragraph 22(2)(b).

[11] The activities authorized by section 31 of the *CSE Act* are: 1) gaining access to a portion of the global information infrastructure, 2) installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting, or intercepting anything on or through the global information infrastructure, 3) doing anything that is reasonably necessary to maintain the covert nature of the activity, and 4) carrying out any other activity that is reasonable in the circumstances and is reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization.

[12] *CSE Act*, subsections 29(1) and 30(1).

[13] *CSE Act,* subsection 34(1): "The Minister may issue an authorization under subsection 26(1), 27(1) or (2), 29(1) or 30(1) only if he or she concludes that there are reasonable grounds to believe that any activity that would be authorized by it is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities."

authorization.[14] In addition, the MND must consult with the Minister of Foreign Affairs (MFA) in order to issue DCO authorizations, and must obtain the MFA's consent in order to issue ACO authorizations.[15] Any authorized ACO or DCO activities cannot cause, intentionally or by criminal negligence, death or bodily harm to an individual; or willfully attempt in any manner to obstruct, pervert, or defeat the course of justice or democracy.[16] Importantly, unlike the authorizations issued under the foreign intelligence, and cybersecurity and information assurance aspects of CSE's mandate, ACO and DCO authorizations are not subject to approval by the Intelligence Commissioner.

IV. CSE ACOs & DCOs: CASE STUDIES

21. (TS//SI) NSIRA received documentation, primarily from CSE, pertaining [redacted] ACOs or DCOs which were either approved, or for which planning was finalized prior to July 30, 2021. All ACOs and DCOs planned, approved, or conducted during the review period were deemed by CSE and GAC, respectively, to be at a risk level [redacted].[17]

22. (S) To more closely review CSE ACOs and DCOs during the review period, NSIRA selected four case studies to focus on in briefings and information requests: [redacted][18] The four were selected on the basis of each operation having different characteristics including, but not limited to: date; techniques used; nature of the target(s); and whether the operation was envisaged together with Five Eyes partners or by CSE alone.[19] Despite the selection of four case studies for this report, NSIRA nevertheless reviewed the materials provided by CSE and others for all ACOs and DCOs for additional context; in some cases, observations about cyber operations that are not among the four case studies are mentioned in this report.

CASE STUDY 1: [redacted]

23. (S) This operation refers to a DCO that was approved but not conducted, to address potential threats during the 2019 Canadian Federal Election by providing an ability to disrupt or interfere with internet infrastructure that might have been used by a foreign entity attacking Elections Canada infrastructure or electronic information. The operation was meant to complement the suite of defensive measures implemented by the Canadian Centre for Cyber Security (CCCS) and the Security and Intelligence Threats to Elections (SITE) taskforce. The DCO was ultimately not required.

24. (S) [redacted] was planned under [redacted] which consolidated CCCS efforts to provide cyber advice, direction, and operational support to the 2019

---

[14] *CSE Act*, subsection 34(4): "The Minister may issue an authorization under subsection 29(1) or 30(1) only if he or she concludes that there are reasonable grounds to believe – in addition to the matters referred to in subsection (1) – that the objective of the cyber operation could not reasonably be achieved by other means and that no information will acquired under the authorization except in accordance with an authorization issued under subsection 26(1) or 27(1) or (2) or 40(1)."

[15] *CSE Act*, subsections 29(2) and 30(2).

[16] *CSE Act*, subsection 32(1).

[17] ACOs and DCOs feature two primary risk assessment processes: the CSE [redacted] process, and the GAC FPRA process. Each process assesses aspects; for example, GAC looks primarily at foreign policy risks, including international law and norms of responsible state behaviour, while CSE's "overall risk" weighs factors such as [redacted]

[18] NSIRA notes that the fact that these ACOs and DCOs were selected does not necessarily mean that they were ultimately conducted by CSE.

[19] In the cyber operations examined during this review, NSIRA observed coordination and collaboration with Five Eyes partners on some CSE ACOs and DCOs. As an example, [redacted]

Federal Election.

25. (TS//SI//CEO) [redacted]

26. (S) A very similar DCO, referred to as [redacted] was planned by CSE for the 2021 Canadian federal elections, but again was not carried out as the required level of threat did not materialize.

CASE STUDY 2: [redacted]

27. (TS) [redacted] The objective of [redacted] was to disrupt the effectiveness of [redacted]

28. (TS//SI//[redacted]) [redacted]

29. (S) [redacted]

CASE STUDY 3: [redacted]

30. (TS//SI//[redacted]) [redacted] to disrupt [redacted]

[20] CSE briefing, RFI-5, February 17, 2022.

31. (TS//SI//[redacted])

32. (TS//SI//[redacted])

33. (TS//SI//[redacted]) was generally considered as a success.

CASE STUDY 4: [redacted]

34. (TS//SI//[redacted])

35. (TS//SI//[redacted]) to disrupt

[redacted]

[redacted][27]

36. (S//SI//[redacted]) A[redacted]

37. (TS//CEO) [redacted] was the first CSE cyber operation [redacted] under an authorization that was [redacted] This [redacted] type of authorization, referred to by CSE as a [redacted] authorization, is discussed later in this report.

38. (C) [redacted] CSE internal compliance was notified by CSE's "Foreign Cyber Operations" (FCO) group of a privacy incident that occurred [redacted] within NSIRA's review period.[28] NSIRA was able to determine that this incident relates to recurring issues related to CSE foreignness assessments. Similar issues have been observed in other reviews—namely, NSIRA's Review of CSE's Self-Identified Privacy Incidents and Procedural Errors (completed in January, 2020) and NSIRA's Review of a Specialized [redacted] Program under the Foreign Intelligence Aspect of CSE's Mandate (completed in August, 2022). NSIRA will conduct a dedicated review on this issue.

V. ANALYSIS

Foreign Policy Risk Assessment and International Law

39. (U) As noted by NSIRA in the Governance Review, CSE cyber operations may carry risks to Canada's foreign policy and international relations.[29] The *CSE Act* requires that the MFA be consulted for DCO authorizations, and the MFA either requests, or consents to, the issuance of an ACO authorization.[30] Although not required by the *CSE Act,* it is a policy decision/agreement between GAC and CSE that GAC plays an active role at the operational level through a Foreign Policy Risk Assessment (FPRA), which "reflects the legislative intention of the *CSE Act*".[31] CSE and GAC follow the CSE-GAC Governance Framework in the course of collaborating on cyber operations.[32] Furthermore, as NSIRA noted in the Governance Review, GAC is involved in the drafting process for ACO and DCO applications.

[redacted]

[28] CSE Document, "Incident Summary Report (Incident [redacted])", GCDocs [redacted], and "Incident_Record_([redacted])", GCDocs [redacted]. CSE discovered the incident in March, 2022, and in June 2022 proactively notified NSIRA of the incident.

[29] Namely, while CSE's foreign intelligence activities seek only to collect information, ACOs and DCOs are designed to deliver effects against various kinds of targets.

[30] *CSE Act*, subsections 29(2) and 30(2).

[31] Written response, GAC RFI-03, Question 1b, February 15, 2022.

[32] For information on the CSE-GAC Governance Framework, see NSIRA review 2020-02, pp23-24.

40. (S//CEO) NSIRA also noted in the Governance Review that GAC FPRAs for CSE cyber operations lacked detail and did not elaborate on certain important factors.[33] During the present review, NSIRA observed that [redacted]

41. (U) In NSIRA's Governance Review, NSIRA found that CSE and GAC had not sufficiently developed a clear and objective framework with which to assess Canada's obligations under international law in relation to cyber operations. NSIRA recommended that CSE should require GAC to conduct and document a thorough legal assessment of each operation's compliance with international law.

42. (TS//SI//SOLICITOR-CLIENT) NSIRA's Governance Review also took notice of the Department of Justice's advice [redacted]. NSIRA notes that the authorizations for this review period required that CSE [redacted][35]

43. (TS//SOLICITOR-CLIENT) For the present review, [redacted] The assessments examined by NSIRA [redacted] In NSIRA's view, the assessments reviewed were sound. This international legal assessment is a positive development in the consideration of international legal obligations and compliance with the authorizations when conducting cyber operations, and provides clarity as to the international legal framework in which CSE's cyber operations are conducted.

44. (TS//SI//SOLICTOR-CLIENT) In NSIRA's Governance Review, NSIRA also recommended that CSE and GAC should provide an assessment of the international legal regime applicable to the conduct of ACOs and DCOs. In April 2022, GAC released a public statement that sets out the Government of Canada's current view on key aspects of international law applicable in cyberspace, and explains how these rules might apply to cyberspace.[36] [redacted][38] Although GAC's public statement was released after CSE began conducting ACOs and DCOs, NSIRA is satisfied that the statement reflects an informed

---

[33] See NSIRA review 20-02, paragraph 78.
[34] See, for example, the GAC FPRAs conducted for [redacted]
[35] 2021-2022 [redacted] MA paragraph 9(e); 2019-2020 and 2020-2021 [redacted] MA paragraphs 11(d).
[36] International Law applicable in cyberspace, Government of Canada, available at https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.
[37] GAC Factual Accuracy comments, September 28, 2022.
[38] [redacted]

consideration of international law in cyberspace, and is a positive development in demonstrating that "Canada is committed to reinforcing the application of international law in cyberspace".[39]

(U) **Finding no. 1: NSIRA finds that the GAC Foreign Policy Risk Assessment process, as well as the related international legal assessment, improved since the Governance Review, for CSE ACOs and DCOs.**

45. (U) In NSIRA's Governance Review, NSIRA recommended that "CSE and GAC should communicate to one another all relevant information and any new developments relevant to assessing risks associated with a cyber operation, both in the planning phases and during its execution."[40] After having reviewed the operations, NSIRA did not observe challenges in communication. On the contrary, documentation from both GAC and CSE, such as meeting records and back-and-forth questions, demonstrated effective and regular communication.

46. (U) GAC told NSIRA that it did not have the expertise to independently assess aspects of CSE's cyber operations, for example the infrastructure and tools used by CSE to conduct such operations. GAC further did not have a role in independently assessing the effectiveness or success of cyber operations. As a result, GAC depended on CSE to provide information and, in some cases, explanations. That said, GAC told NSIRA that CSE had been sharing more information with GAC, and that GAC, for example, had [redacted] access to CSE intelligence reporting that informed cyber operations.[41] NSIRA observed that CSE provided GAC with periodic updates during cyber operations.

(U) **Finding no. 2: NSIRA finds that GAC does not have capability to independently assess potential risks resulting from the techniques used in CSE ACOs and DCOs.**

(U) **Recommendation no. 1: NSIRA recommends that GAC develop or otherwise leverage capability to enable it to independently assess potential risks resulting from the techniques used in CSE ACOs and DCOs.**

Section 32 - Prohibited conduct

47. (U) As per subsection 32(1) of the *CSE Act*, in carrying out any activity under a ACO or DCO authorization, CSE must not cause, intentionally or by criminal negligence, death or bodily harm[42] to an individual; or wilfully attempt in any manner to obstruct, pervert, or defeat the course of justice or democracy.

48. (TS//SI//SOLICITOR-CLIENT) In practice, the prohibited conduct is assessed through CSE's cyber operations framework documents, which include justification of why the activities of the cyber operation will not amount to the prohibited conduct. DLS, an operational stakeholder for cyber operations, provides [redacted] DLS' involvement is [redacted]

[39] International Law applicable in cyberspace, Government of Canada, paragraph no. 2.
[40] NSIRA review 20-02, Recommendation no. 9.
[41] Briefing, GAC RFI-2, November 10, 2021.
[42] In subsection 32(1), bodily harm has the same meaning as section 2 of the *Criminal Code* (subsection 32(2) of the *CSE Act*).

[redacted][43] As indicated in the matrices, the assessment as to whether the cyber operation activity might risk contravening the prohibitions is to be made based on [redacted][44] The prohibition against death or bodily harm by criminal negligence further uses the standard [redacted] NSIRA assesses that the legal opinions and matrices demonstrate a thorough understanding of the prohibitions in section 32 of the *CSE Act*.

49. (TS//SI//SOLICITOR-CLIENT) The conclusions reached [redacted] are re-evaluated [redacted] through use of the matrices, to ensure that the assessment remains reasonable [redacted][45] CSE's Mission Policy Suite on Cyber Operations includes the matrices and provides some guidance on how to interpret the prohibitions and assess for risk, however the obligation to assess is placed [redacted][46] The MPS notes that further guidance may be provided by CSE Mission Policy.

50. (TS//SI//SOLICITOR-CLIENT) However, the assessment of a given operation's activities for legal compliance are not conducted by the Department of Justice, and are not always subject to additional legal consultation when again assessed through CSE's [redacted], as DLS would only [redacted][47] NSIRA does not consider CSE's policy guidance on the prohibitions adequate without further consultation with the Department of Justice, especially given that an operation's compliance with section 32 of the *CSE Act* relies heavily on legal concepts, and such compliance is highly context-specific. NSIRA considers it appropriate for the Department of Justice to be consistently involved in the assessment and validation [redacted], which would minimize any potential legal risk when conducting cyber operations.

(U) **Finding no. 3: NSIRA finds that CSE and the Department of Justice demonstrated a thorough understanding of section 32 of the *CSE Act*. However, CSE does not appropriately consult with the Department of Justice at the [redacted] stage to ensure that the assessment of legal compliance remains valid.**

(U) **Recommendation no. 2: NSIRA recommends that the Department Justice be fully consulted at all stages of an ACO or DCO, particularly prior to operational execution.**

Section 34 of the *CSE Act*

51. (U) This review is the first time that NSIRA was able to assess the requirements in subsections 34(1) and (4) of the *CSE Act* in relation to ACO and DCO authorizations. Importantly, unlike foreign intelligence or cybersecurity authorizations, the Intelligence Commissioner does not review whether the

[43] Written response, CSE RFI-20, Question 3, August 26, 2022. This group is known, in CSE, as the 'FCO' group.
[44] CSE Document, "Bodily Harm Risk Matrix", in MPS Cyber Operations, November 2021 (Annex A, page 11), GCDocs [redacted].
[45] Written response, CSE RFI-20, Question 3. See [redacted]
[46] Section 3.4.2., MPS Cyber Operations, November 2021. CSE factual accuracy comments, September 23, 2022.
[47] See glossary of terms.

conclusions made under subsections 34(1) and (4) and on the basis of which an ACO or DCO authorization was issued by the MND, are reasonable.

Description of legal standards

52. (U) Under subsection 34(1) of the *CSE Act,* the Minister of National Defence may issue an ACO (subsection 30(1)) or DCO (subsection 29(1)) authorization only if he or she concludes that there are reasonable grounds to believe that any activity authorized by it is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities. Additionally, in order to issue ACO or DCO authorizations, subsection 34(4) requires that the MND conclude that there are reasonable grounds to believe that the objective of the cyber operation could not reasonably be achieved by other means and that no information will be acquired under the authorization, except in accordance with an authorization issued under subsection 26(1) (foreign intelligence), or 27(1) or (2) (cybersecurity), or 40(1) (emergency) authorization.

53. (U) Importantly, the written application of the Chief of CSE must set out the facts that would allow the MND to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met.[48]

Application of legal standards

54. (TS//CEO) As part of this review, NSIRA was able to assess CSE's cyber operations against both the governance structure and authorizations. Specifically, operations conducted under the [redacted] authorizations, which [redacted] authorize a [redacted] class of activities. In contrast to [redacted] authorizations for ACOs and DCOs, [redacted] was conducted under [redacted] authorization [redacted] that was specific to the objectives of that operation.

55. (TS//CEO) In NSIRA's Governance Review, NSIRA found that the authorization applications for [redacted] cyber operations did not provide sufficient detail for the Ministers of National Defence and Foreign Affairs to appreciate the scope of activities being requested in the application, but rather, in NSIRA's view, the classes of activities and [redacted] of ACOs and DCOs, as described in both authorizations, [redacted].[49] This may also impact the MND's ability to assess any authorized activities against the requirements of the *CSE Act,* which requires sufficient precision in an application for the MND to satisfy these requirements. While NSIRA acknowledged that authorizations should be reasonably nimble to enable CSE to conduct [redacted] ACOs and DCOs when needed, NSIRA also noted a need for the MND to appreciate, with a certain degree of specificity, the types of activities and objectives that will be carried out under the authorization.

56. (TS//CEO) In addition to providing the facts in the application that would allow the MND to determine the reasonableness and proportionality when issuing an ACO or DCO authorization, CSE assesses and validates the proportionality and reasonableness of any proposed operations through its cyber operations framework. However, unlike the applications to the MND, CSE's internal cyber operations framework documents include: [redacted]

[48] *CSE Act,* subsection 33(2).
[49] See NSIRA review 2020-02, finding no. 1.

[redacted]"[50] CSE policy offers additional guidance on how to assess for proportionality and reasonableness [redacted][51] NSIRA notes that at this more detailed stage of CSE planning the operation, the MND does not again conclude on the reasonableness and proportionality of the objectives to be achieved and the activities authorized in the context of the specific operation.

57. (S) The MND is the Minister responsible for CSE,[52] and section 47 of the *CSE Act* requires the MND to *personally* exercise the powers that are set out in subsections 29(1) and 30(1).[53] In order to issue the authorizations, the conditions in subsections 34(1) and (4) of the Act must be met. Generally, CSE's approach to complying with these requirements is to confirm that the proposed activities "align" with the authorization, and the MND's conclusions are then confirmed internally by CSE throughout [redacted]. Although [redacted] assessment of reasonableness, proportionality, and that the objective of the cyber operation could not be achieved by other reasonable means [redacted] the requirements in section 34 are a pre-condition for the MND to issue an ACO or DCO authorization, and not a pre-condition for CSE [redacted]

58. (TS//CEO) Further, NSIRA observed that in practice, there is a difference between "strategic" and "operational" objectives for cyber operations: [redacted] As mentioned, the *CSE Act* requires that the "nature of the objective to be achieved" and the "objective of the cyber operation" be identified in order to meet the requirements of subsections 34(1) and (4).

59. (TS//SI//CEO) The complete relevant factual context in which the MND must assess cyber authorizations for the requirements of the *CSE Act* is not included in the application, as in practice, [redacted]. Thus, the conclusions on reasonableness and proportionality within the [redacted] authorizations are not necessarily premised on all of the relevant factual information of a cyber operation. In the [redacted] applications for the period of review, the objectives identified in the [redacted] applications and authorizations were thematic, without specificity to an operation. For example, out of the [redacted]

---

[50] Written response, CSE RFI-06, question 4, March 4, 2022.
[51] CSE Document, MPS Cyber Operations 2019, section 3.6.
[52] *CSE Act,* section 6.
[53] The wording of section 47 is clear that the Minister must personally exercise the powers in subsections 29(1) and 30(1): "The Minister must personally exercise the powers that are set out in subsections 26(1), 27(1) and (2), 29(1), 30(1), 36(2), 39(1) and 40(1)." See *The Queen v Harrison,* [1977] 1 SCR 238: "Although there is a general rule of construction in law that a person endowed with a discretionary power should exercise it personally (*delegatus non potest delegare*) that rule can be displaced by the language, scope or object of a particular administrative scheme." See also *Ramawad v Minister of Manpower and Immigration,* [1978] 2 SCR 375.
[54] Written response, CSE RFI-6 question 3: "Through paragraph 2 and 2 and 3 of the [redacted] MAs, and paragraph 2 of the [redacted] MA, the Minister has defined the strategic objectives to be pursued under those Authorizations and provided information substantiating these objectives... When read holistically, each [authorization] provides a thorough definition of the nature of the objectives and activities authorized."
[55] See also CSE written response, RFI-6, questions 3-5: "The development of objectives for operational activities includes consideration of a number of factors, including: [redacted] and considerations put forward by other governmental stakeholders, including GAC. Strategic, operational, and tactical objectives are defined in Joint Planning and Authorities Framework documents..." (RFI-6 Q5).
[56] CSE written response, RFI-6 Q5.

objectives identified in the Chief's application for [redacted].[57] The application elaborates on [redacted].[58] When the objective is defined in such general terms and not grounded in the context of a specific cyber operation, there is no meaningful understanding by the MND of the objectives or the means used to achieve them. As previously mentioned by NSIRA, the [redacted] applications are not sufficiently detailed to permit the Ministers to understand what it is they are authorizing.

60. (TS//SI//CEO) For the [redacted] that was conducted under the authority of the [redacted] authorization, [redacted][59] In these documents, the link between the activities, the objective, the effects and the intended outcome were clear and precisely defined, thereby better demonstrating how the operational activities were reasonable and proportionate. This information was not included in the Chief's application.

61. (TS//SI//CEO) Further, ACOs have the potential to infringe *Charter* rights, given that an objective may be to [redacted] as was the case for [redacted][60] NSIRA notes that the *Charter* may require the MND to take relevant *Charter* values into account when exercising discretion to issue an authorization.[61] Thus, a cyber operation's potential impact on *Charter* rights is possibly relevant to the MND's assessment of reasonableness and proportionality when issuing an authorization.

62. (TS//SI//CEO) The [redacted] applications similarly define the objective to be achieved under the authorization in a manner that identifies the circumstances when there might be a need for enhanced cybersecurity capability, rather than being specific to an operation.[62] Again, the applications defined objectives and activities in [redacted] manner as to make a meaningful determination of the reasonableness and proportionality challenging for the MND. For the [redacted] reviewed, [redacted]

---

[57] 2020-2021 [redacted] Application, paragraph 18(c).
[58] 2020-2021 [redacted] Application, paragraph 54.
[59] See, for example, the [redacted].
[60] For operation [redacted], a CSE subject matter expert confirmed that [redacted] did not give rise to *Charter* protection, [redacted] In the future, NSIRA may review how CSE ensures compliance with the *Charter* when conducting cyber operations.
[61] *Doré v Barreau du Quebec, 2012 SCC 12* at paras 55—58: "How then does an administrative decision-maker apply *Charter* values in the exercise of statutory discretion? He or she balances the *Charter* values with the statutory objectives. In effecting this balancing, the decision-maker should first consider the statutory objectives... Then decision-maker should ask how the *Charter* value at issue will best be protected in view of the statutory objectives. This is at the core of the proportionality exercise, and requires the decision-maker to balance the severity of the interference of the *Charter* protection with the statutory objectives... If in exercising its statutory discretion, the decision-maker has properly balanced the relevant *Charter* value with the statutory objectives, the decision will be found to be reasonable."
[62] See, for example, [redacted] Application 2020-2021, paragraphs 10-11.

[redacted] NSIRA notes that the determination of reasonableness and proportionality in the [redacted] for the [redacted] was particularity unintelligible. This was due to CSE's assessment being [redacted]

63. (TS//SI//CEO) For the requirement in subsection 34(4) that the "objective of the cyber operation could not reasonably be achieved by other means", CSE differentiates between the "considerations underpinning this determination [that] are presented by CSE in the application to the Minister", and [redacted] through CSE's cyber operations framework.[63] It is through the cyber operations framework that CSE [redacted], including through consultation with other GC stakeholders (discussed later).[64] It is also through the cyber operations framework, rather than through the application to the Minister, that [redacted][65]

64. (TS//SI//CEO) Consequently, there is a discrepancy between the information in the application, which is assessed by the MND, and operational documents, which are assessed by CSE, [redacted]. It is possible that an assessment based on strategic objectives and activities is not the same assessment when examining operational and tactical objectives and activities. Further, assessment of whether or not an operation's activities risk amounting to the prohibited conduct in section 32 of the *CSE Act* (as discussed above) is presumably part of the relevant legal and factual context that the MND would need when exercising her or his discretion to issue an authorization. As per subsection 33(2) of the *CSE Act*, CSE is required to set out the facts that would allow the MND to conclude that there are reasonable grounds to believe that the authorization is necessary and the conditions for issuing it are met. For [redacted] applications, it appears that CSE does not include the full factual context that would allow for the MND to meaningfully conclude on whether conditions in subsections 34(1) and (4) required for issuing the authorization have been met.

65. (TS//SI) The Minister of National Defence, as the accountable decision maker authorized by Parliament to issue authorizations when the conditions of the *CSE Act* have been met, must consider all of the circumstances that might be relevant to the exercise of discretion to issue the authorization,[66] and in order to impose any terms, conditions or restrictions that the MND considers advisable, as per subsection 35(d) of the *CSE Act*. All of the relevant information on which the MND needs to meet the conditions in the *CSE Act* for issuing an authorization is not provided to the MND for [redacted] applications. Not providing the full relevant factual context of the operation and activities also impacts the MFA's ability to meaningfully consent to the ACO authorization, or be consulted on the DCO authorization, in accordance with the requirements of subsections 29(2) and 30(2) of the *CSE Act*.

---

[63] Written response, CSE RFI-6, question 5.
[64] Ibid.
[65] Ibid.
[66] *X (Re)*, 2017 FC 1048 at paras 53–54; citing *Baron v Canada*, [1993] 1 SCR 416 at paras 437, 439, 440.

(U) **Finding no. 4: NSIRA finds that CSE's applications for authorizations issued under subsections 29(1) and 30(1) of the *CSE Act* for [redacted] activities did not include all the available information relevant to a meaningful assessment of the requirements in subsections 34(1) and (4) of the *CSE Act*.**

(S) **Recommendation no. 3: NSIRA recommends that CSE abandon the practice of generic ACO and DCO applications (i.e.: [redacted] to the Minister of National Defence, and instead submit individual applications [redacted].**

More recent applications and authorizations

66. (TS//SI//CEO) For the [redacted] authorization was drafted with a specialized, operation-specific approach that included [redacted], rather than being authorized under the [redacted] authorizations. However, this authorization is not defined by a [redacted], and there is no legislative requirement to do so. CSE sought [redacted] authorization for this operation as the activities comprising [redacted], i.e.: [redacted], were not included in the objectives of the [redacted] authorization at the time and thus would not have been authorized. Accordingly, "CSE required authorities to conduct [redacted] activities [redacted]"[67]

67. (TS//SI//CEO) In contrast to the [redacted] authorizations, NSIRA notes [redacted] applications and authorizations, as seen in the [redacted], address some of the concerns identified above for the [redacted] applications given that they included precise justification to the MND as to how the operation met the requirements of the *CSE Act*. The [redacted] applications and authorizations provided significantly more detail as to how the requirements in subsection 34(1) are satisfied, better demonstrating that reasonable grounds to believe that a well-founded and logical connection exists between the nature of the activities and the objectives to be achieved (i.e., the reasonableness and proportionality), and grounded within the relevant context of the operation. Likewise for subsection 34(4), there is more detail as to why the objective of the operation could not reasonably be achieved by other means, including a justification as to why other types of action from the GC, such as non-cyber options, would not reasonably achieve the objectives in the authorization.

Section 34(4) – Stakeholder consultation

68. (S) In NSIRA's Governance Review, NSIRA expressed concerns about CSE consultation with other GC departments and agencies, especially in the context of the alignment of CSE ACOs and DCOs with GC national security and defence policy priorities.[68] Specifically, NSIRA's Governance Review noted the potential value in coordinating with the Privy Council Office (PCO) and Public Safety (PS) in CSE cyber operations, particularly in the context of ensuring cyber operations' alignment with GC national security, foreign policy, and defence priorities. Furthermore, recommendation number three in NSIRA's Governance Review recommended that the National Security and Intelligence Advisor to the Prime Minister (NSIA) be a key stakeholder in consultations about CSE cyber operations.

[67] CSE RFI-06, question 6.
[68] See NSIRA review 2020-02, paragraph 50 and finding 3.

69. (U) To build on the theme of CSE collaboration and engagement with GC stakeholders, NSIRA incorporated CSIS, RCMP, and DND/CAF into this review, in addition to GAC. NSIRA chose these GC entities because they were each implicated in one or more of the ACOs or DCOs examined by NSIRA. NSIRA's focus on incorporating CSIS, RCMP, and DND/CAF into the review was to understand the nature and extent, if any, of these organizations' engagement with CSE—and vice versa—during the planning for or conduct of CSE cyber operations.

70. (TS//SI) As mentioned previously, a precondition to the MND issuing an ACO or DCO authorization is that the MND must conclude that there are reasonable grounds to believe that the objective of the cyber operation could not reasonably be achieved by other means.[69] The Act does not specify how this is to be assessed.

71. (S) According to CSE, "CSE assesses and validates that there are no other means to reasonably achieve an operation's objective through the [cyber operations framework] governance process and through collaboration with internal CSE stakeholders, five eye partners and other GC stakeholders, including GAC, CSIS and RCMP", and that "Operational considerations occur in collaboration with [said stakeholders]."[70] Despite this, documentation examined during this review indicated that CSE assessed, validated, and collaborated with other stakeholders on ACOs and DCOs when, and if, CSE determined this to be necessary—rather than as a consistent rule.

CSIS

72. (TS//SI//CEO) During the review period, CSIS engaged with CSE [redacted], under the authority of CSIS' threat reduction mandate under section 12.1 of the *Canadian Security Intelligence Service Act,*[71] and through CSIS' ability to enter into an arrangement or otherwise cooperate with any department of the Government of Canada, or the government of a foreign state or an institution thereof, provided the respective requirements for Ministerial approval are met. CSIS told NSIRA that it did not conduct any of the activities with CSE under the authority of a warrant issued under section 21.1 of the *CSIS Act*.[72] Other than [redacted], CSIS told NSIRA that it had not received notification from CSE of any other cyber operations.[73] NSIRA did not observe CSE consultation with CSIS [redacted] during the review period, [redacted]

73. (TS//SI) One of the operations on which CSIS worked with CSE was the [redacted]. In

---

[69] *CSE Act*, subsection 34(4). The requirement and wording of "could not reasonably be achieved by other means" is unique to the *CSE Act*.

[70] Written response to CSE RFI-06, Q5.

[71] *Canadian Security Intelligence Service Act,* RSC, 1985, c C-23 [*CSIS Act*].

[72] CSIS briefing, March 22, 2022. CSIS further noted that [redacted].

[73] During the factual accuracy process (September 2022), CSE disputed CSIS' claim, stating that CSE had informed CSIS of [redacted] in an email, and had discussed [redacted] with CSIS in meetings. NSIRA saw emails indicating that CSE provided notification of [redacted] to CSIS. On October 14, 2022, CSE provided NSIRA with an email indicating that [redacted] CSE explained that [redacted].

[74] [redacted] refers to [redacted]

[75] [redacted] refers to [redacted].

the case [redacted], CSIS had a standing Threat Reduction Measure (TRM) in place [redacted] under section 12.1 of the *CSIS Act*. CSIS' role in CSE's [redacted] was the use of [redacted] to support CSE efforts.[76]

74. (TS//SI) On the subject of de-confliction and information sharing, CSIS told NSIRA that it had a bi-weekly subcommittee with CSE wherein the two agencies engage on various kinds of topics. However, CSIS was not informed by CSE of any planned or conducted ACOs or DCOs unless CSE decided that a given ACO or DCO may implicate, overlap with, or affect CSIS equities such as [redacted]. CSIS was also unaware of how many cyber operations CSE had conducted. CSIS told NSIRA that conducting certain elements of CSE cyber operations in tandem generally had resulted in greater effectiveness than if CSIS were to conduct these activities on its own. CSIS used the [redacted] as an example of a case where [redacted].

75. (U) NSIRA notes the differences in the legal authorities and mandates between CSE and CSIS, including the requirements to conduct similar activities in cyberspace. As mentioned, CSIS engages in activities that can be similar to those of CSE, through CSIS' TRM mandate in subsection 12.1(1) of the *CSIS Act,* which is to take measures, within or outside Canada, to reduce a threat to the security of Canada. Before undertaking any TRMs, CSIS is required to consult, as appropriate, with other federal departments and agencies as to whether they are in a position to reduce the threat.[77]

76. (U) In contrast, the *CSE Act* does not have a similar requirement to consult other federal departments or agencies, but rather that there must be reasonable grounds to believe that the objective of the cyber operation could not reasonably be achieved by other means, without specifying how this is to be assessed. The ACO aspect of CSE's mandate is different in purpose than CSIS' TRM mandate,[78] and CSE also has unique technical skills and cyber expertise not available to CSIS.

77. (U) Accordingly, although the mandate and legislative requirements differ for CSIS and CSE, there may be instances where CSIS is better placed to achieve the objective of the cyber operation. However, in cases where CSE would be in a position to reduce the threat, CSE must still ensure that the objective of the cyber operation could not reasonably be achieved by any other means. NSIRA notes the standard is not one of "effectiveness", but rather "could not reasonably be achieved by other means" for CSE, while CSIS must only consult as appropriate. However, these requirements suggest that a comparative exercise must occur.

(U) **Finding no. 5: NSIRA finds that there is potential for overlap between CSE and CSIS activities in the context of capabilities used by CSE to conduct its ACOs and DCOs. However, CSE did not consistently consult with CSIS about CSE's cyber operations.**

RCMP

78. (S) In the context of de-confliction and information sharing on CSE cyber operations, CSE ACO

[76] More specifically, [redacted].

[77] *CSIS Act,* subsection 12.1(3).

[78] As mentioned, the ACO aspect is to carry out activities on or through the GII to 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.

and DCO teams met with the RCMP Federal Policing Criminal Operations (FPCO) Cybercrime Intelligence team on a monthly basis—in addition to ad-hoc meetings—to share information to ensure no conflicts with any ongoing RCMP cybercrime files under investigation.[79] RCMP told NSIRA as an example that, during the monthly CSE-RCMP meetings, [redacted] The information shared may include [redacted][80]

79. (TS//SI//CEO) For the [redacted] applications for the period of review, in relation to the requirement that the objectives in the authorization could not reasonably be achieved by other means, the Chief of CSE wrote that [redacted][81] RCMP confirmed to NSIRA that there had not been any instances of CSE having contacted RCMP to determine whether CSE objectives for a cyber operation could be met by RCMP activities.[82] That said, RCMP considered that "CSE efforts [as of April 13, 2022] to consider whether a cyber operation could [redacted] by law enforcement have been sufficient."[83]

80. (TS) RCMP told NSIRA that in the case of an ACO, the RCMP's collaboration and coordination with CSE would be [redacted][85] However, in addition to these forms of collaboration as described to NSIRA by RCMP NSIRA also observed that [redacted], RCMP considered [redacted] activities under RCMP's own legal authorities, [redacted][87]

81. (TS//SI) The RCMP [redacted] investigation into [redacted]

---

[79] Written response to RCMP RFI-1: Questions for written response, March 7, 2022. Cooperation principles between CSE and RCMP are outlined in a Memorandum of Understanding (MOU) between the two organizations. RCMP told NSIRA that it recognizes that the MOU, dated from 2009, "does not currently reflect CSE's ACOs and DCOs", and noted that the RCMP will be working to ensure that this MOU is updated to reflect the current legal landscape (RCMP response to RFI-2, April 13, 2022).

[80] Written response to RCMP RFI-1: Questions for written response, question 1(a), March 7, 2022.

[81] 2020-2021 [redacted] application paragraph 57; 2020-2021 [redacted] application paragraph 37.

[82] Written response to RCMP RFI-2, question 5(a) (April 13, 2022), and to RCMP RFI-1, question 2 (March 7, 2022).

[83] Written response to RCMP RFI-2, question 4, provided April 13, 2022

[84] Written response to RCMP RFI-2, April 13, 2022. Information sharing between the RCMP and CSE may raise issues related to the intelligence-to-evidence dilemma. The intelligence-to-evidence dilemma arises from the fact that intelligence may contain evidence, but may also contain information that is not evidence. As a result, problems can arise if actionable intelligence is used to inform criminal investigations and prosecutions. NSIRA may examine this issue in the CSE-RCMP context in future reviews.

[85] Written response to RCMP RFI-2, question 3, April 13, 2022.

[86] According to RCMP written response to RFI-2, question 6, April 13, 2022, [redacted] More broadly, 'disruption' can range from [redacted] to any kind of impact caused to a service.

[87] Email: "RE: [redacted] Email: "RE: [redacted]

[88] Email: "SITREP on RCMP/OPP Coordination", [redacted], Email: "FW: [redacted]

RCMP conducting [redacted].[89] [redacted] to be conducted under RCMP [redacted] authorities, but in coordination with CSE's [redacted]. [redacted] it is not clear to NSIRA how CSE assessed that [redacted] could not reasonably be achieved by other means.

82. (S) De-confliction with CSE on [redacted] occurred to ensure that CSE's activities "would not imperil [redacted] criminal law enforcement [redacted]."[90] NSIRA saw [redacted] examples of communication and information-sharing between CSE and RCMP in this context.

DND/CAF

83. (U) Any CSE cyber operation conducted in support of CAF is done under CSE's technical and operational assistance aspect of its mandate, which is beyond the scope of this review. For assistance operations requested by CAF, CAF is responsible to consult with GAC, if necessary, through CAF's own mechanisms (e.g.: DND/CAF's Joint Consultative Mechanism with GAC), which are separate and distinct from CSE's consultative mechanisms with GAC.[91]

84. (S) [redacted]

85. (TS//SI//CEO) In the case of the CSE [redacted], which disrupted and degraded [redacted], formal DND/CAF approval was not required, though DND/CAF was made aware of [redacted] and was given opportunities to raise issues to CSE.[93] DND/CAF told NSIRA that military planners were present within [redacted]. De-confliction during [redacted] focused on equities related to the [redacted]; [redacted]. Thus, according to DND/CAF, de-confliction during [redacted].[94]

86. (U) DND/CAF told NSIRA that the CSE-DND/CAF experience to date on cyber operations has been "excellent", with great communication back-and-forth. While DND/CAF told NSIRA that there remains room to grow, the relationship with CSE on this file was "very good" as of the time of the briefing

[89] During factual accuracy (September 28, 2022), RCMP denied that CSE asked RCMP [redacted], despite email evidence to the contrary. NSIRA notes that, in line with RCMP's legal authority, [redacted].

[90] Written response to RCMP RFI-2, question 7, April 13, 2022

[91] CSE document, "[redacted]", slide 8.

[92] Ibid., slide 7.

[93] DND/CAF RFI-1, Briefing to NSIRA – ACO/DCO Review, slide 9, May 27, 2022.

[94] Ibid.

(May 27, 2022).

Demonstrating a consideration of other means

87. (TS//SI//CEO) Irrespective of instances of consultation or engagement with other GC departments and agencies during the planning and conduct of CSE ACOs and DCOs, NSIRA observed that CSE's cyber operations planning documents focused more on the expediency and ease of accomplishing the cyber operation's objective, and generally did not demonstrate a consideration of the potential for other actors to achieve the same objective with other means.[95]

(U) Finding no. 6: NSIRA finds that despite close collaboration with Global Affairs Canada, and the Department of National Defence and Canadian Armed Forces on ACOs and DCOs, CSE did not demonstrate consistent engagement with CSIS or RCMP to determine whether the objective of an ACO or DCO could not reasonably be achieved by other means.

(U) Recommendation no. 4: NSIRA recommends that CSE always engage with CSIS, RCMP, and any other federal departments or agencies as to whether those departments are in a position to reasonably achieve the objective of a cyber operation.

Acquiring information alongside ACOs and DCOs

Requirements of the CSE Act and the Authorizations

88. (U) As mentioned, under subsection 34(4) of the *CSE Act*, the MND may issue an ACO or DCO authorization only if she or he concludes that there are reasonable grounds to believe that the objective of the cyber operation could not reasonably be achieved by other means and that no information will be acquired under the authorization, except in accordance with an authorization issued under a foreign intelligence, cybersecurity, or emergency authorization. NSIRA interprets this subsection as permitting information collection as part of a cyber operation, so long as there is a valid foreign intelligence, cybersecurity, or emergency authorization that permits collection under the respective aspect. Thus, information collection can occur under a concurrent authorization issued under subsections 26(1), 27(1) or (2), or 40(1).

89. (TS//SI) In NSIRA's Governance Review, NSIRA found that "CSE's internal policies regarding the collection of information in the conduct of cyber operations are not accurately described within the Active and Defensive Cyber Operations Ministerial Authorizations."[96] Given this, NSIRA recommended that in its applications, CSE should "accurately describe the potential for collection activities to occur under separate authorizations while engaging in Active and Defensive Cyber Operations."

[95] For example, paragraphs 56-59 of the 2020-2021 [redacted] application broadly focuses on the need for the ability to [redacted] but otherwise does not provide much justification for why the objectives of the cyber operation could not reasonably be achieved by other means.

[96] NSIRA Review 20-02, finding no. 5.

90. (TS//SI) In the corresponding applications for ACOs and DCOs in the review period, CSE interpreted subsection 34(4) as prohibiting CSE from relying on the authority of the ACO or DCO authorization to acquire information.[97] The ACO and DCO authorizations for the review period stipulate that the classes of activities authorized are subject to the following restriction: "No information will be acquired *as a result of* the activities conducted under this Authorization".[98] CSE's interpretation of the MND's restriction against collecting information "as a result of" the activities authorized is that it "was intended to convey that no information will be acquired "under the authority" of the s. 18 or s. 19 authorization."[99]

91. (TS//SI//CEO) However, NSIRA notes that the corresponding applications do not fully inform the MND that collection activities can occur concurrently, or after the effects of a cyber operation, under a valid foreign intelligence, cybersecurity or emergency authorization. While the applications state that "no information will be acquired through [active or defensive] cyber operations activities",[100] the Chief of CSE only specifies that any information required to *achieve the intended outcome* of ACOs or DCOs would be acquired under the authority of an existing foreign intelligence, cybersecurity, or emergency authorization—and not that information would be collected for foreign intelligence purposes *as a result of* the effects of the ACO or DCO.

Information acquired "as a result" of the cyber operation

92. (U) NSIRA closely examined the details of how, if at all, information was observed and collected concurrent to cyber operations. In addition to considering this issue in the case of several ACOs and DCOs, NSIRA zoomed in on one particular [redacted] to scrutinize logging data and precise operational details including, if applicable, any observations made or information acquired before, during, or after the operation under any concurrent authorities.

93. (U) In examining ACOs and DCOs on this review, NSIRA has concluded that the observation, collection, and analysis of foreign intelligence are vital elements of cyber operations (further described below). Without an ability to acquire information concurrent to cyber operations, CSE would in most cases be significantly hampered in its efforts to plan, execute, and assess cyber operations, in addition to potentially losing out on the ability to collect valuable intelligence.

94. (TS//SI//CEO) As a result, CSE must, and does, rely on its foreign intelligence authorities in order to conduct cyber operations, and this reliance on intelligence collection to enable cyber operations [redacted].[101]

95. (TS//SI//CEO) NSIRA examined if, and how, information was acquired under authorities other

---

[97] See the applications for [redacted] 2021-2022 paragraph 73; [redacted] 2020-2021 paragraph 60; [redacted] paragraph 56; [redacted] 2019 paragraph 40.

[98] See paragraph 11(g) in the ACO and DCO authorizations issued for 2019-2020 and 2020-2021, and paragraph 9(f) in the 2021-2022 [redacted] authorization. As of June 2022, the newest ACO and DCO authorizations contained the same prohibition. See paragraph 12(h) in the ACO and DCO authorizations issued for 2021-2022, paragraph 8(e) in [redacted] authorization issued on March 18, 2022, and paragraph 9(e) in [redacted] authorization re-issued on June 30, 2022.

[99] Written response, CSE RFI-12 question 1.

[100] 2020-2021 [redacted] paragraph 27; 2021-2022 [redacted] paragraph 27; 2021-2022 [redacted] paragraph 28.

[101] See, with regard to following 2021-2022 MAs: [redacted] subsection 2(c) and 5(d); [redacted] subsection 10(c); and [redacted] subsection 6(c). Although CSE could in theory use its cybersecurity and information assurance aspect authorities in conjunction with ACOs or DCOs, NSIRA did not observe any such cases during the review period, [redacted].

than [redacted] alongside [redacted], by examining aspects of foreign intelligence operations and activity that occurred concurrently [redacted].[102] To do so, NSIRA viewed logs [redacted].[103] NSIRA also received two demonstrations from CSE technical operators to better understand how CSE's systems functioned in the context of this type of activity.

96. (TS//SI//CEO) NSIRA was able to verify that information *was* acquired by CSE *as a result of* [redacted] activities [redacted].[104] [redacted].

97. (TS//SI//CEO) It is clear to NSIRA that in practice, information collection must occur "as a result" of the cyber operation in order for CSE to assess the effectiveness of the operation. In the context of [redacted], NSIRA observed that [redacted]

98. (TS//SI) [redacted], NSIRA observed that in practice, information acquired under an authorization permitting collection does occur as a result of a cyber operation, [redacted][108] As a result, any observations or collection alongside, or following, the effect occur as a result of the effect.

99. (TS//SI//CEO) CSE's interpretation of these concurrent collection activities in relation to the restriction in the authorizations is that no information is acquired as a result of ACO or DCO activities, rather "all supporting information collected before, during, or after an operation is collected under separate s.16 [foreign intelligence] or s.17 [cybersecurity and information assurance] authorities, including Ministerial Authorization(s) and activity approvals" and that: "these separate aspects of the

---

[102] CSE told NSIRA that [redacted].
[103] CSE documents: [redacted]. As previously mentioned, the disruption activity in this case is known as [redacted]
[104] For example, NSIRA viewed logs [redacted].
[105] Because an EPR was generated with this information, [redacted]. (Written response to CSE RFI-19, question 3, supported by documentation).
[106] Written response to CSE RFI-9, question 7, April 29, 2022.
[107] Written response to CSE RFI-16 question 1(a), July 25, 2022. According to CSE, an [redacted].
[108] For example, if a CSE [redacted].

mandate do not live in silos, and can take place concurrently."[109]

100. (TS//SI//CEO) Accordingly, NSIRA does not consider the concurrent collection activities, or collection activities that occur as a result of the cyber operation, to be accurately or transparently described within the applications to the MND. Although it may be accurate to describe that any collection activities only occur under the authority of a foreign intelligence or cybersecurity authorization, the potential for collection to occur *as a result of* a cyber operation is not accurately described to the MND in the applications for ACO or DCO authorizations for the period of review. Rather, the applications only describe the reliance on information acquired under a foreign intelligence or cybersecurity authorization to achieve the intended outcome of the cyber operation. The applications state that "no information will be acquired through [active or defensive] cyber operations activities".[110] NSIRA considers it necessary for the Chief's applications to appropriately inform the MND that collection under a valid foreign intelligence, cybersecurity, or emergency authorization, occurs concurrently to, or as a result of, the cyber operations – as such activities occur in practice.[111]

101. (U) The Charter statement on Bill C-59, *An Act respecting national security matters*, made a distinction between CSE's foreign intelligence and cybersecurity and information assurance activities, and ACO and DCO activities.[112] The former were considered to have the potential to interfere with privacy interests, which may engage section 8 of the *Charter*, while ACO and DCO activities were not expected to interfere with privacy interests. For consistency with section 8 of the *Charter*, the independent Intelligence Commissioner, a retired superior court judge, would approve foreign intelligence and cybersecurity and information assurance activities before the activities could interfere with privacy interests, in addition to being authorized by the Minster. In contrast, the prior approval of the Intelligence Commissioner would not be required for ACO and DCO authorizations as those activities would not include the acquisition of private information of a Canadian or a person in Canada, and thus section 8 would not be engaged.

102. (S) Given NSIRA's study of the operations in practice, NSIRA confirmed that a causal relationship exists between the effect of a cyber operation and the collection of information that otherwise would not have been possible to collect without the effect. Thus, given that ACO and DCO activities have a role in enabling other activities that may interfere with privacy interests, the reasoning that informed Bill C-59's limitation of Intelligence Commissioner oversight to foreign intelligence and cybersecurity authorizations, does not align with NSIRA's observations of the causal relationship between cyber operations and intelligence collection.

103. (U) NSIRA's observations of instances wherein intelligence collection depended on the effect of a cyber operation, and the related issues of CSE's transparency towards the Intelligence Commissioner and the MND, could be addressed by expanding the mandate of the Intelligence Commissioner, pursuant to the *Intelligence Commissioner Act*. Specifically, such an expansion could include oversight to determine whether the conclusions made under the *CSE Act,* and on the basis of which ACO and DCO authorizations are issued or amended, are reasonable.

---

[109] Written response, CSE RFI-12, question 1(a), June 16, 2022.

[110] [redacted] application 2021-2022, paragraph 28; [redacted] application paragraphs 73-75.

[111] NSIRA notes that newer applications and authorizations, that did not form part of the period of review, specified that: [redacted] See, for example, paragraph 46 of [redacted] application dated March 18, 2022.

[112] Department of Justice, Charter Statement – Bill C-59: *An Act respecting national security matters*, June 20, 2017, accessible at: www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html

(U) **Finding no. 7: NSIRA finds that the Chief's applications for active and defensive cyber operations activities for the period of review did not accurately describe the causal relationship between a cyber operation, and intelligence collection that can occur as a result of a cyber operation.**

(S) **Recommendation no. 5: NSIRA recommends that the Chief's applications for active and defensive cyber operations inform the Minister of National Defence that acquisition of information under a valid foreign intelligence, cybersecurity, or emergency authorization, occurs as a result of cyber operations.**

104. (U) Of note, and in relation to observations made in NSIRA's Governance Review about information collection during cyber operations, NSIRA observed that governance documents for ACOs generally became clearer in terms of describing the fact that foreign intelligence collection may occur before, during, or after an ACO, and included links to associated foreign intelligence missions. However, these documents did not provide clear information about the details of how such foreign intelligence collection might occur.

105. (TS//SI//CEO) More specifically, key documents such as the JCOP did not always contain links or references to foreign intelligence missions that accompanied cyber operations; when they did, these references were not detailed.[113] For example, in the case of a [redacted] codenamed [redacted],[114] CSE noted in internal after-action evaluation material that the operation suffered from lack of clarity as to concurrent foreign intelligence operations alongside [redacted]

106. (TS) During the review, NSIRA confirmed examples of [redacted]. As such, a clearer link in the ACO or DCO JCOP to foreign intelligence activities and objectives—[redacted]—would both benefit CSE's intelligence requirements, while also providing an operator with greater clarity [redacted] and under what authorities and for what purpose.

107. (TS//SI) In the case of the [redacted].[116] In other words, CSE conducted a risk assessment dedicated to [redacted]

[113] For example, the [redacted] did not reference the accompanying [redacted] in its Annex, and [redacted] says only in a single sentence that foreign intelligence collection [redacted].
[114] [redacted] refers to [redacted].
[115] CSE document, email: [redacted].
[116] CSE document, [redacted].

[redacted]

(U) **Finding no. 8: NSIRA finds that, in its Joint Cyber Operations Plan, CSE did not always provide clarity pertaining to foreign intelligence missions that were, or could have been, conducted alongside ACOs and DCOs.**

(S) **Recommendation no. 6: NSIRA recommends that documentation prepared as part of the CSE's cyber operations framework (the Joint Planning and Authorities Framework) provide clear links to all known applicable foreign intelligence (or cybersecurity) missions—[redacted]—that may accompany the conduct of ACOs and DCOs.**

Differentiating between ACO, DCO, and other mandate aspects

108. (U) During the review, NSIRA considered the inter-relation between activities under the aspects of CSE's mandate for foreign intelligence, cybersecurity and information assurance, DCOs, and ACOs. In closely examining ACOs and DCOs, NSIRA observed that foreign intelligence and cybersecurity activities are similar, in terms of their techniques, to activities taken as part of ACOs and DCOs.

109. (U) Within the *CSE Act*, there is considerable overlap between these aspects of CSE's mandate.[117] The activities and classes of activities that may be authorized under a foreign intelligence authorization in subsection 26(2), and the activities and classes of activities that may be authorized for an ACO or DCO authorization in section 31, are identical. The sole difference is that a foreign intelligence authorization under subsection 26(1) permits acquiring information on or through the global information infrastructure.[118] Likewise, there are similarities between the DCO and cybersecurity aspects of CSE's mandate. Both aspects are for the purpose of helping to protect federal or designated electronic information and information infrastructures. In order to do so, the DCO aspect permits CSE to carry out activities on or through the GII,[119] whereas the cybersecurity aspect is to provide advice, guidance, and services for this purpose, in addition to permitting the acquisition of information to be able to do so.[120]

110. (TS//SI) In order to distinguish between a foreign intelligence activity and an ACO/DCO activity when using similar techniques, CSE focuses on the objective of the activity to distinguish whether it is conducted for foreign intelligence or cyber operations purpose.[121] This is demonstrated, for instance, through CSE's use of [redacted] as both a foreign intelligence and [redacted] technique. In the foreign intelligence applications for [redacted] issued under subsection 26(1) of the *CSE Act*, the Chief of CSE states that CSE [redacted] may engage in activities pursuant to a cyber operations authorization issued under sections 29 and 30 of the *CSE Act*.[122] In the corresponding authorization, as part of the MND's rationale for the reasonableness of the activities authorized, the MND acknowledges that [redacted] can be used to facilitate and enable cyber operations.[123]

---

[117] This does not include activities conducted under the assistance aspect of CSE's mandate, section 20 of the *CSE Act*.
[118] *CSE Act*, paragraph 26(2)(b).
[119] *CSE Act*, section 18.
[120] *CSE Act*, section 17.
[121] Written response to CSE RFI-6, Question 9, March 4, 2022.
[122] [redacted] application paragraph 8.
[123] [redacted] authorization paragraph 10(c).

111. (TS//SI) For example, [redacted] (such as [redacted]) can constitute an effect that degrades, disrupts, influences, responds to or interferes with the capabilities, intentions, and activities of targets. In the case of the [redacted], which relied solely on [redacted], NSIRA observed that this use [redacted] was intended to [redacted]. This kind of [redacted] was tied to the objective of the [redacted]; in contrast, a foreign intelligence operation may use [redacted][124] When distinguishing the purpose of such a technique in this way, NSIRA is able to differentiate foreign intelligence and cybersecurity activities, from ACOs and DCOs.

112. (TS//SI) The interdependency between the aspects of CSE's mandate is further described the 2021-2022 [redacted] applications.[125] In these applications, among other foreign intelligence techniques, CSE added the use of [redacted] as a reasonable activity to enable cyber operations. The corresponding authorizations authorize CSE to conduct any other activity that is reasonable in the circumstances if it is in aid of any activity authorized by the authorization, and any measures reasonably necessary to maintain the covert nature of the activities.[126] This clarifies that [redacted] can deliver [redacted] effects, in addition to their use for foreign intelligence purposes.

ACO or DCO?

113. (TS//SI) While NSIRA is satisfied with how CSE distinguishes otherwise similar techniques used under the foreign intelligence and cybersecurity aspects, from the ACO and DCO aspects, NSIRA continues to question how CSE differentiates between the ACO and DCO aspects.[127]

114. (U) Within the *CSE Act,* there are numerous similarities between ACOs and DCOs. The activities and classes of activities in section 31 that may be authorized under cyber operations authorizations are identical. The prohibited conduct in section 32, and the requirement to not direct any cyber operations activities at a portion of the GII that is in Canada [128] applies to both ACOs and DCOs. Nonetheless, the *CSE Act* clearly distinguishes between the ACO and DCO aspects, as described in sections 18 and 19.[129] Further, the Act distinguishes the purpose for which authorized ACO and DCO

---

[124] For example, as described in paragraph 2(d) of the [redacted] MA, CSE can [redacted].

[125] 2020-2021 [redacted] application, paragraph 28; 2020-2021 [redacted] application, paragraph 18; See also 2021-2022 LFPR ACO application, paragraph 28(d); 2021-2022 [redacted] application, paragraph 16.

[126] 2020-2021 [redacted], paragraphs 7-8; 2020-2021 [redacted] paragraphs 7-8; In the 2021-2022 [redacted] authorizations, the use of [redacted] was specifically authorized. See 2021-2022 [redacted] authorization, paragraphs 7-8; 2021-2022 [redacted] Authorization, paragraphs 8-9.

[127] NSIRA Review 2020-02, finding no. 4. A core element of NSIRA's concern in the Governance Review about this point was the risk that CSE might conduct a DCO that resembles an ACO, but without consultation with the MFA/GAC. However, NSIRA's confirmation that GAC provides an FPRA for ACOs *and* DCOs mitigates some of NSIRA's concern.

[128] *CSE Act*, paragraph 22(2)(a).

[129] Section 18 of the *CSE Act:* "The defensive cyber operations aspects of the Establishment's mandate is to carry out activities on or through the GII to help protect: (a) federal institutions' electronic information infrastructures; and (b) electronic information an information infrastructures designated under subsection 21(1) as being of importance to the Governance of Canada." Section 19 of the *CSE Act*: "The active cyber operations aspect of the Establishment's mandate is to carry out activities on or through the GII to 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."

activities are conducted (i.e., in furtherance of the ACO aspect or DCO aspect of CSE's mandate), and the corresponding authorizations process: for DCO authorizations, the MND must consult with the MFA, whereas for ACOs, the MND may only issue the authorization if the MFA has requested or consented to its issue.[130] Thus, given these distinctions within the *CSE Act,* it is essential for CSE to properly differentiate between ACOs and DCOs.

115. (S) NSIRA notes an apparent difference in nature between DCOs. Some DCOs were designed in anticipation of a potential threat, such as the planned DCO [redacted] focused on elections security. In contrast, other DCOs were designed to better defend against [redacted] threat that caused, and continued to cause, damage to the electronic information and information infrastructure of federal institutions and of designated systems of importance to the GC. An example of the latter is the planned [redacted], which was intended to respond to an ongoing threat from a ransomware actor.

116. (TS//SI) Although it was planned as a DCO, NSIRA observes that CSE could have also planned [redacted] as an ACO, as [redacted] could have fit within the description of the ACO aspect in the *CSE Act*.[131] For example in [redacted]. This activity could be considered as disrupting or interfering with the capabilities of a foreign organization as it relates to defence or security, which could make the operation akin to an ACO.

117. (TS//SI) Although NSIRA observes that the planned DCO [redacted] also had the characteristics of an ACO, NSIRA notes that CSE clearly explained, in its cyber operations framework documentation, why the objectives and nature of [redacted] met the criteria of a DCO as outlined in the *CSE Act* and in the applicable [redacted] DCO authorization. For example, the [redacted] explained the threat posed by the target [redacted] to the electronic information and information infrastructures of Canadian federal institutions and to systems of importance to the GC.[132] To do so, the [redacted]. Given overlap in the *CSE Act* between DCOs and ACOs, NSIRA will continue to assess differences in CSE ACOs and DCOs, and how CSE chooses whether an operation should be conducted as an ACO, or as a DCO.

(U) **Finding no. 9: NSIRA finds that CSE's ACOs and DCOs that were planned or conducted prior to July 30, 2021, including the four case studies analyzed in this report, were lawful.**

(U) **Finding no. 10: NSIRA finds that there is significant overlap between activities conducted under the ACO and DCO aspects of CSE's mandate, as well as between all four aspects of CSE's mandate.**

---

[130] *CSE Act*, subsections 29(2) and 30(2), respectively.

[131] NSIRA notes that CSE's rationale for [redacted] having been planned as a DCO was that [redacted] (CSE, presentation to NSIRA in response to RFI-05, February 17, 2022). NSIRA does not believe that this rationale precludes [redacted] from having been planned as an ACO.

[132] CSE Document, [redacted] GCDocs [redacted].

(U) **Recommendation no. 7: NSIRA recommends that CSE continue to refine, and to define, the distinctions between activities conducted under different aspects of its mandate, particularly between ACO and DCO activities, but also with regard to foreign intelligence and cybersecurity activities.**

VI. CSE's RESPONSIVENESS AND PROVISION OF INFORMATION

Responsiveness and Timeliness

118. (U) Despite improvements in later stages, NSIRA experienced significant and unreasonable delays in the provision of information by CSE on this review, particularly in the case of NSIRA's first RFI, which NSIRA's Chair later raised in a meeting with the Chief of CSE. NSIRA issued two advisory notices to CSE, attached to this report.

119. (U) NSIRA intended this review to test forms of direct access to CSE information repositories as part of NSIRA's broader moves toward information verification.[133] CSE did not consent to progress on access to its information holdings during this review.

120. (U) In response to NSIRA's first RFI, CSE eventually provided approximately 45,000 documents. CSE's search terms, used to provide NSIRA with these documents, contained significant omissions—including omissions of at least [redacted] ACOs, [redacted] which reached substantial planning stages. NSIRA further notes that CSE determined its own methodology for responding to NSIRA's first RFI, which NSIRA considered to be inefficient, burdensome, and flawed. In addition to concerns about the efficiency of CSE's external review processes, NSIRA is concerned about the impact of inaccurate or incomplete narratives being shared with CSE employees on both the review specifically, as well as on trust between CSE employees and NSIRA more broadly.

121. (U) NSIRA also faced challenges with RCMP responsiveness on this review.

122. (U) In contrast, NSIRA was satisfied with the responsiveness of GAC, CSIS, and DND/CAF, who provided responses and information in a manner in line with NSIRA's expectations.

CSE's Problematic Solution for Information Provision

123. (U) In September 2021 CSE unilaterally—and without explanation nor instruction—imposed a new information technology system on NSIRA for the provision of CSE documents, with highly restrictive user settings. NSIRA repeatedly informed CSE that this system was unsatisfactory for NSIRA's review needs and made clear demands for solutions, yet CSE failed to implement any solutions throughout the majority of this review.

[133] For more information on NSIRA's requirements for information verification, consult NSIRA's 2020 and 2021 public Annual Reports, available on NSIRA's public website: https://nsira-ossnr.gc.ca. See also NSIRA's expectations for responsiveness in reviews: https://nsira-ossnr.gc.ca/expectations-for-responsiveness-in-reviews.

VII. CONCLUSION

124. (S) As of July 30, 2021, CSE had approved five ACOs, and approved one DCO since the *CSE Act* came into force on August 1, 2019.[134] Of these, CSE [redacted] did not conduct the DCO. NSIRA is further aware of [redacted] by CSE as of April, 2022. NSIRA notes that the COVID-19 pandemic posed challenges to CSE's work on ACOs and DCOs, primarily in 2020 through mid-2021.

125. (U) During the review period, CSE generally considered that the ACOs it conducted were successful, while planning for DCOs was considered by CSE to have been beneficial despite no DCOs having been executed. NSIRA did not assess for efficacy during this review.

126. (U) NSIRA observed that CSE developed and improved its processes for the planning and conduct of ACOs and DCOs in a way that reflected some of NSIRA's observations from the Governance Review. By closely examining CSE cyber operations and associated activities, NSIRA is able to better understand how CSE cyber operations are conducted, including their relation with other aspects of CSE's mandate. NSIRA's review raised some issues related to how certain aspects of cyber operations are described in authority documents, as well as challenges related to conducting cyber operations in a way that is consistent with the *CSE Act*. NSIRA will continue to review CSE cyber operations, especially as these continue to evolve and feature different characteristics.

127. (U) Given the important changes to CSE's mandate in the *CSE* Act, NSIRA expected a high degree of support and transparency from CSE during the conduct of this review. Despite these expectations, NSIRA was not satisfied with its degree of access to CSE information during this review, and raised concerns about timeliness of information provision, as well as completeness of information. Challenges related to accessing CSE information negatively impacted the quality and depth of this review, as well as NSIRA's confidence in the completeness of information received.

[134] These numbers do not include [redacted] under the technical and operational assistance aspect of CSE's mandate.

ANNEX A: Briefings

128. (U) This annex provides a list of briefings received from stakeholders during this review. The list does not include meetings held with review counterparts, but rather focuses only on substantive briefings with subject-matter experts used to inform the content of this report. The briefings below were held in various formats, including in-person meetings and Secure Video Tele-Conferencing.

(S) Briefings:

- **September 22, 2021**: CSE briefing about the [redacted]
- **November 10, 2021**: GAC briefing about GAC's role in an ACO and a DCO
- **November 25, 2021**: CSE briefing discussing the structure and organization of CSE's Foreign Cyber Operations (FCO) team and how it works with other units within CSE
- **February 17, 2022**: CSE briefing about the operations [redacted]
- **March 22, 2022**: CSIS briefing about the extent of engagement by CSIS in selected CSE ACOs and DCOs
- **May 16, 2022**: CSE technical demonstration about tools, systems, and techniques used in the context of [redacted]
- **May 27, 2022**: DND/CAF briefing about engagement by DND/CAF in CSE's ACOs and DCOs, and about [redacted]
- **August 5, 2022**: CSE technical demonstration related to the acquisition and observation of information [redacted]

ANNEX B: Updates to CSE ACO & DCO Governance

Governance

129. (U) Around April 2021, CSE updated its Joint Planning and Authorities Framework (JPAF) for ACOs and DCOs, which refers to the framework by which CSE plans and conducts its ACOs and DCOs (this report refers to the JPAF as CSE's 'cyber operations framework.' The updated JPAF was intended to provide clarity toward who is consulted and who approves cyber operations, and to separate between resources and planning, risk assessments, and alignment with authorities.[135] The primary change to the JPAF involved the introduction of a new document, the Joint Cyber Authorities Document (JCAD).

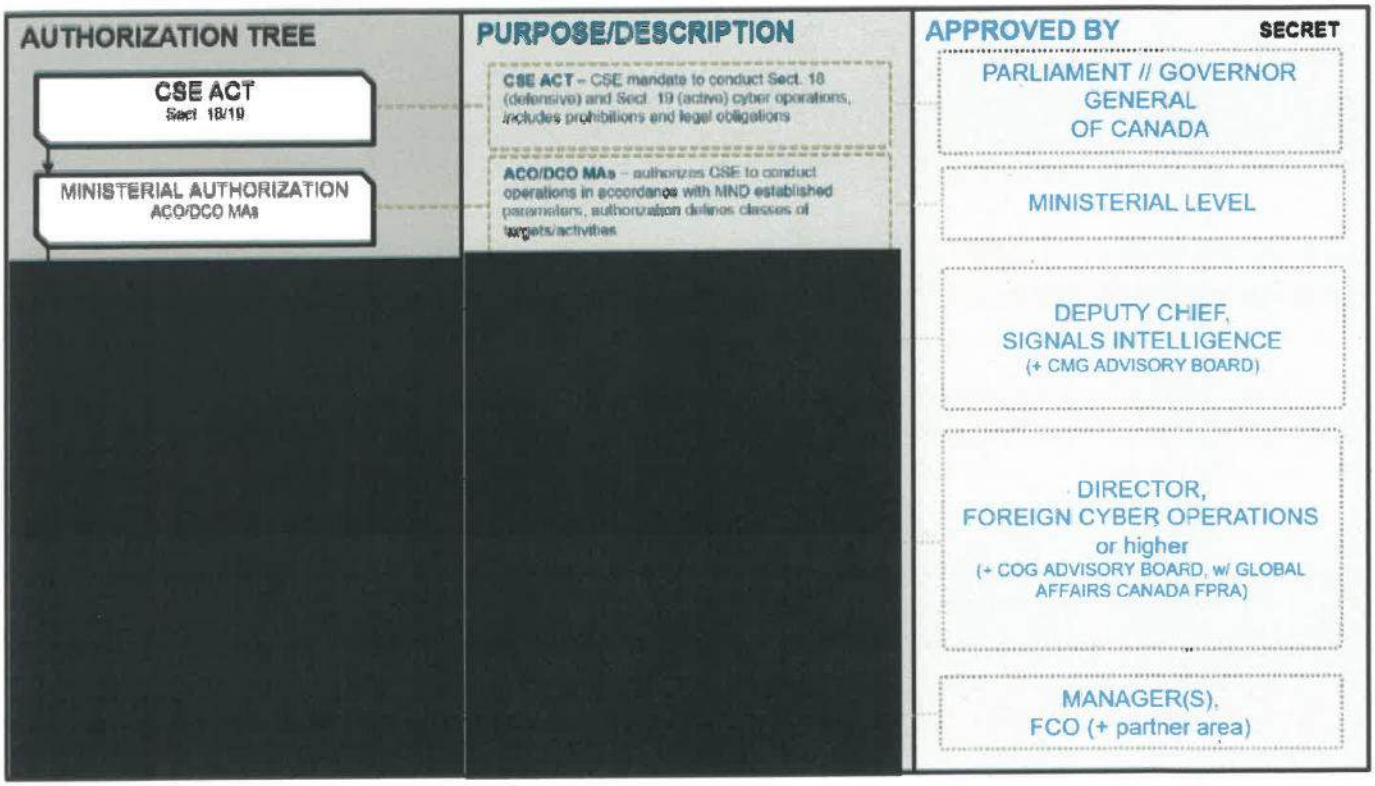
130. (U) The JCAD is a high-level policy document that organizes cyber operation authorities by theme, [redacted] The JCAD is intended to clearly articulate CSE's authorities with its targets and activities, while assessing for risk at the framework level.[137] JCADs, [redacted].

131. (S) Examples of JCAD themes seen by NSIRA included a JCAD [redacted].[138] Other JCADs that were discussed by CSE during the review period included [redacted].

132. (S) As another update since NSIRA's previous review, JCADs were also accompanied by an [redacted], which exists in addition to regular operation-specific [redacted]. The figure below provides an overview of CSE's updated JPAF from April, 2021:

Figure 1: Updated JPAF[139]

[135] CSE document, "JPAF evolution – Overview", slide 3.
[136] The term used internal to CSE to describe the concept of 'theme' is 'line of effort'.
[137] CSE RFI-2, Briefing to NSIRA, September 22, 2021.
[138] CSE document, [redacted]. Operations conducted during the review period under this [redacted].
[139] Created by CSE, for briefing to NSIRA on September 22, 2021.



ANNEX C: Recommendations from NSIRA's Review of CSE's Governance of ACOs and DCOs

Recommendation no. 1: CSE should more precisely define the classes of activities, associated techniques, and intended target sets to be undertaken for Active and Defensive Cyber Operations as well as their underlying rationale and objectives, both in its Applications and associated Ministerial Authorizations for these activities.

Recommendation no. 2: GAC should include a mechanism to assess all relevant foreign policy risk parameters of Active and Defensive Cyber Operations within the associated Ministerial Authorizations.

Recommendation no. 3: CSE and GAC should establish a framework to consult key stakeholders, such as the National Security and Intelligence Advisor to the Prime Minister and other federal departments whose mandates intersect with proposed Active Cyber Operations, to ensure that they align with broader Government of Canada strategic priorities and that the requirements of the CSE Act are satisfied.

Recommendation no. 4: CSE and GAC should develop a threshold that discerns between an Active Cyber Operation and a "pre-emptive" Defensive Cyber Operation, and this threshold should be described to the Minister of National Defence within the applicable Ministerial Authorizations.

Recommendation no. 5: In its applications to the Minister of National Defence, CSE should accurately describe the potential for collection activities to occur under separate authorizations while engaging in Active and Defensive Cyber Operations.

Recommendation no. 6: CSE should include all pertinent information, including targeting and contextual information, within all operational plans in place for a cyber operation, and in materials it presents to GAC.

Recommendation no. 7: CSE should provide a structured training program to its employees involved in the execution of Active and Defensive Cyber Operations (ACO/DCOs), to ensure that they have the requisite knowledge of CSE's legal authorities, requirements, and prohibitions, as required by the associated Ministerial Authorizations.

Recommendation no. 8: CSE and GAC should provide an assessment of the international legal regime applicable to the conduct of Active and Defensive Cyber Operations. Additionally, CSE should require that GAC conduct and document a thorough legal assessment of each operation's compliance with international law.

Recommendation no. 9: CSE and GAC should communicate to one another all relevant information and any new developments relevant to assessing risks associated with a cyber operation, both in the planning phases and during its execution.

ANNEX D: Responses to NSIRA's Requests for Information

Organization	RFI#	Type	Requested	Deadline	Completed	Business Days Late[140]
CSE	1	Documentation[141]	30-Jul-21	20-Aug-21	25-Mar-22	157
CSE	2	Briefing	7-Jun-21	16-Jul-21	22-Sep-21	50
GAC	1	Documentation	24-Sep-21	13-Oct-21	21-Oct-21	6
GAC	2	Briefing	24-Sep-21	10-Nov-21	10-Nov-21	0
CSE	3	Briefing & written	15-Oct-21	5-Nov-21	25-Nov-21	14
CSE	4	Written response	22-Nov-21	10-Dec-21	15-Dec-21	3
CSE	5	Briefing	19-Jan-22	17-Feb-22	17-Feb-22	0
RCMP	1	Written response	20-Jan-22	7-Mar-22	7-Mar-22	0
GAC	3	Written response	23-Jan-22	15-Feb-22	15-Feb-22	0
CSIS	1	Briefing	23-Jan-22	28-Mar-22	22-Mar-22	-4
CSE	6	Written response	24-Jan-22	4-Mar-22	4-Mar-22	0
CSE	7	Written response	4-Mar-22	28-Mar-22	29-Apr-22	26
CSE	8	Written response	4-Mar-22	8-Apr-22	29-Apr-22	17
CSE	9	Written response	4-Mar-22	28-Mar-22	16-May-22	37
CSE	10	Technical demo	4-Mar-22	16-May-22	16-May-22	0
RCMP	2	Written response	17-Mar-22	13-Apr-22	13-Apr-22	0
CSIS	2	Written response	30-Mar-22	25-Apr-22	3-May-22	8
DND/CAF	1	Briefing	8-Apr-22	27-May-22	27-May-22	0
GAC	4	Written response	4-May-22	6-Jun-22	6-Jun-22	0
CSE	11	Written response	5-May-22	19-May-22	16-May-22	-3
CSE	12	Written response	24-May-22	15-Jun-22	15-Jun-22	0
CSE	13	Documentation	26-May-22	22-Jun-22	15-Jun-22	-5
DND/CAF	2	Documentation	27-May-22	13-Jun-22	6-Jun-22	-5
CSE	14	Written response	17-Jun-22	5-Jul-22	5-Jul-22	0
CSE/DOJ	15	Written response	27-Jun-22	6-Jul-22	7-Jul-22	1
CSE	15	Documentation	28-Jun-22	6-Jul-22	6-Jul-22	0
CSE	16	Written response	6-Jul-22	25-Jul-22	25-Jul-22	0
GAC	5	Written response	15-Jul-22	1-Aug-22	29-Jul-22	-1
CSE	17	Documentation	15-Jul-22	28-Jul-22	28-Jul-22	0
CSE	18	Technical demo	21-Jul-22	12-Aug-22	9-Aug-22	-3
CSE	19	Written response	5-Aug-22	26-Aug-22	26-Aug-22	0
CSE	20	Written response	16-Aug-22	30-Aug-22	26-Aug-22	-2
CSE	21	Written response	28-Sep-22	12-Oct-22	12-Oct-22	0

[140] The numbers in this column do not include statutory holidays.
[141] In the case of this RFI, which requested a large volume of documentation, CSE received some documentation as early as September 2021, with a majority of the documentation having been provided by mid-November, 2021.

ANNEX E: Findings & Recommendations

Findings

(U) **Finding no. 1:** NSIRA finds that the GAC Foreign Policy Risk Assessment process, as well as the related international legal assessment, improved since the Governance Review, for CSE ACOs and DCOs.

(U) **Finding no. 2:** NSIRA finds that GAC does not have capability to independently assess potential risks resulting from the techniques used in CSE ACOs and DCOs.

(U) **Finding no. 3:** NSIRA finds that CSE and the Department of Justice demonstrated a thorough understanding of section 32 of the *CSE Act*. However, CSE does not appropriately consult with the Department of Justice at the [redacted] stage to ensure that the assessment of legal compliance remains valid.

(S) **Finding no. 4:** NSIRA finds that CSE's applications for authorizations issued under subsections 29(1) and 30(1) of the *CSE Act* for [redacted] activities did not include all the available information relevant to a meaningful assessment of the requirements in subsections 34(1) and (4) of the *CSE Act*.

(U) **Finding no. 5:** NSIRA finds that there is potential for overlap between CSE and CSIS activities in the context of capabilities used by CSE to conduct its ACOs and DCOs. However, CSE did not consistently consult with CSIS about CSE's cyber operations.

(U) **Finding no. 6:** NSIRA finds that despite close collaboration with Global Affairs Canada, and the Department of National Defence and Canadian Armed Forces on ACOs and DCOs, CSE did not demonstrate consistent engagement with CSIS or RCMP to determine whether the objective of an ACO or DCO could not reasonably be achieved by other means.

(U) **Finding no. 7:** NSIRA finds that the Chief's applications for active and defensive cyber operations activities for the period of review did not accurately describe the causal relationship between a cyber operation, and intelligence collection that can occur as a result of a cyber operation.

(U) **Finding no. 8:** NSIRA finds that, in its Joint Cyber Operations Plan, CSE did not always provide clarity pertaining to foreign intelligence missions that were, or could have been, conducted alongside ACOs and DCOs.

(U) **Finding no. 9:** NSIRA finds that CSE's ACOs and DCOs that were planned or conducted prior to July 30, 2021, including the four case studies analyzed in this report, were lawful.

(U) **Finding no. 10:** NSIRA finds that there is significant overlap between activities conducted under the ACO and DCO aspects of CSE's mandate, as well as between all four aspects of CSE's mandate.

Recommendations

(U) **Recommendation no. 1:** NSIRA recommends that GAC develop or otherwise leverage capability to enable it to independently assess potential risks resulting from the techniques used in CSE ACOs and DCOs.

(U) **Recommendation no. 2:** NSIRA recommends that the Department Justice be fully consulted at all stages of an ACO or DCO, particularly prior to operational execution.

(S) **Recommendation no. 3:** NSIRA recommends that CSE abandon the practice of generic ACO and DCO applications (i.e.: [redacted]) to the Minister of National Defence, and instead submit individual applications [redacted].

(U) **Recommendation no. 4:** NSIRA recommends that CSE always engage with CSIS, RCMP, and any other federal departments or agencies as to whether those departments are in a position to reasonably achieve the objective of a cyber operation.

(S) **Recommendation no. 5:** NSIRA recommends that the Chief's applications for active and defensive cyber operations inform the Minister of National Defence that acquisition of information under a valid foreign intelligence, cybersecurity, or emergency authorization, occurs as a result of cyber operations.

(S) **Recommendation no. 6:** NSIRA recommends that documentation prepared as part of the CSE's cyber operations framework (the Joint Planning and Authorities Framework) provide clear links to all known applicable foreign intelligence (or cybersecurity) missions—[redacted]—that may accompany the conduct of ACOs and DCOs.

(U) **Recommendation no. 7:** NSIRA recommends that CSE continue to refine, and to define, the distinctions between activities conducted under different aspects of its mandate, particularly between ACO and DCO activities, but also with regard to foreign intelligence and cybersecurity activities.