National Security and Intelligence Review Agency

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

~~TOP SECRET // [redacted] // CEO~~

REVIEW OF THE COMMUNICATIONS SECURITY ESTABLISHMENT'S (CSE) MINISTERIAL AUTHORIZATIONS AND MINISTERIAL ORDERS UNDER THE *CSE ACT*

(NSIRA REVIEW 08-501-5)

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5

I EXECUTIVE SUMMARY

1. (U) Following the coming into force of *the Communications Security Establishment Act* (*CSE Act*), CSE received a new set of Ministerial Authorizations (MA) – written documents by which the Minister of National Defence authorizes CSE to engage in activity that risks contravening an "Act of Parliament or interfering with a reasonable expectation of privacy of a Canadian or person in Canada." The *CSE Act* also created a legislative authority for the Minister of National Defence to "designate electronic information or information infrastructures or classes of electronic information or information infrastructures as being of importance to the Government of Canada" through a Ministerial Order (MO).

2. (U) NSIRA's Foundational Review[1] of CSE's Ministerial Authorizations (MAs) and Ministerial Orders (MOs) represents a different approach to reviewing MAs than that of the Office of the Communications Security Establishment Commissioner (OCSEC), CSE's former independent external review body. While OCSEC previously reported on the number of private communications, we leave this matter to CSE's classified annual report to the Minister. Further, it is not necessary to review whether Ministerial Authorizations are based on reasonable conclusions, which is now the responsibility of the Intelligence Commissioner. NSIRA chose to approach the Ministerial Authorizations as an opportunity to learn about CSE's operational activities, and the Ministerial Orders were reviewed as supplementary to the Ministerial Authorizations.

3. (U) The Minister authorized seven MAs and three MOs in 2019 under the *CSE Act*.[2] NSIRA received comprehensive briefings on activities authorized by each MA and was able to use this material to inform NSIRA's three-year CSE review plan.

4. (U) Based on the records provided by CSE, NSIRA believes that CSE employed considerable rigour in the MA application process. However, NSIRA has made the following five findings and corresponding recommendations to improve CSE's transparency and accountability:

- (U) Finding no. 1: The application requests from the Chief of CSE, presented the Minister of National Defence with sufficient information to meet the conditions of subsection 33(2) of the *CSE Act*. The new applications provide more information than previous applications under the *National Defence Act*, and allow for better transparency of CSE's activities.

- (S) Finding no. 2: Although these activities have not yet occurred, there is no indication that CSE has fully assessed the ramifications – legal or otherwise – of

1. A foundational review is intended to provide a broad overview of a subject to establish a baseline knowledge and/or to inform future reviews.
2 See Annex C for a list of Ministerial Authorizations and Ministerial Orders.

the activities authorized in the [redacted] Authorization.[3] [redacted]

- (S) Recommendation no. 1: CSE should seek a fulsome legal assessment on activities authorized by [redacted] prior to undertaking any collection activities under the [redacted] MA. The legal advice should address whether there is an implicit justification regime created in the [redacted] MA.

- (U) Finding no. 3: The [redacted] letters in relation to the Minister of National Defence's consultation with the Minister of Foreign Affairs for Active and Defensive Cyber Operations were not dated. That specific consultation event with Global Affairs Canada was not sufficiently documented.

- (U) Recommendation no. 2: CSE should ensure that the ACO/DCO consultation process with Global Affairs Canada is documented as precisely as possible to allow for an easy verification of its compliance with the sequencing required in the Act.

- (C) Finding no. 4: CSE was unable to provide an assessment of its obligations under international law relevant to the conduct of Active Cyber Operations.

- (U) Recommendation no. 3: CSE should seek a formal legal assessment of the international legal regime applicable to the conduct of active cyber operations prior to undertaking any such operations.

- (U) Finding no. 5: The *Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under a Foreign Intelligence Ministerial Authorization* only included [redacted]

- (U) Recommendation no. 4: An order issued under section 45 of the *CSE Act* should be as precise as possible in clearly detailing the list of persons or classes of persons designated to receive Canadian identifying information disclosed by CSE.

4. (U) This foundational review highlighted the need to focus on Active and Defensive Cyber Operations immediately following the completion of this review, given that the Intelligence Commissioner does not approve these activities and that they represent a new aspect of CSE's mandate.

[3] This Authorization has since been renamed to [redacted]

II AUTHORITIES

5. (U) This review was conducted under the authority of paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency Act*.

III INTRODUCTION

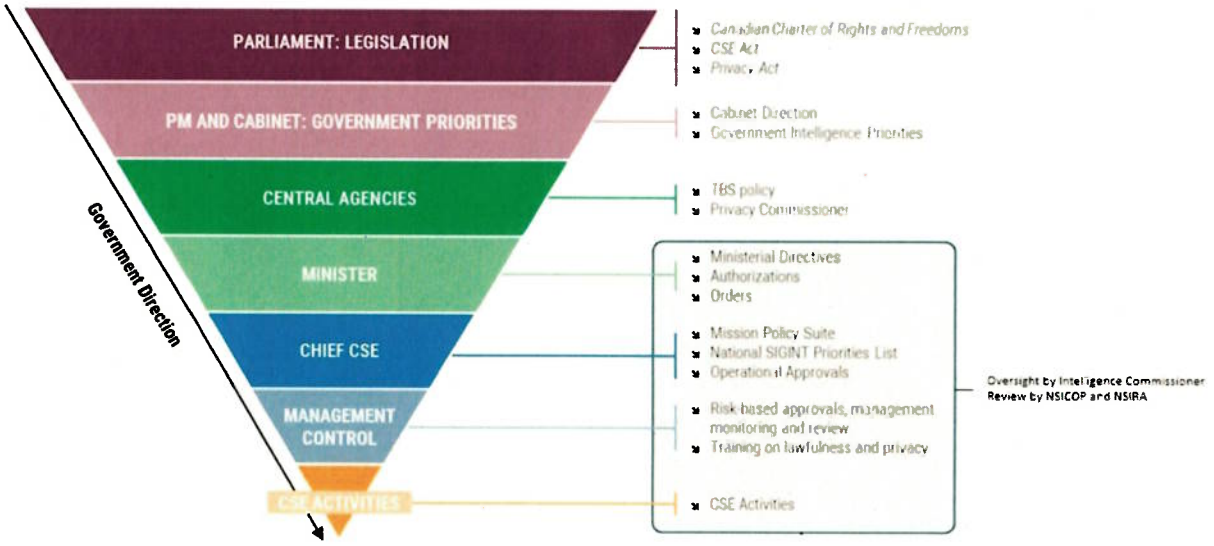
6. (U) *The Communications Security Establishment Act* (*CSE Act*) came into force on August 1, 2019 replacing part V.I of the *National Defence Act* (NDA) as the main legislation for CSE. Following the coming into force, CSE received new Ministerial Authorizations (MA). In addition, the *CSE Act* also created a legislative authority for the Minister of National Defence to "designate electronic information or information infrastructures or classes of electronic information or information infrastructures as being of importance to the Government of Canada" through a Ministerial Order (MO).

- **Ministerial Authorization (MA):** is a written document by which the Minister authorizes the department to engage in activity that risks contravening an "Act of Parliament or interfering with a reasonable expectation of privacy of a Canadian or person in Canada."
- **Ministerial Order (MO):** is the instrument by which a Minister makes its orders and do not require the approval of the Cabinet. It is created under the authority granted to a Minister under a statute or regulation.

These documents are authored by CSE, and issued by the Minister of National Defence.

UNCLASSIFIED//OUO

CSE Authorities and Direction



7. (U) This report provides an overview of CSE's MAs and MOs with a focus on specific activities that are either newly authorized by the CSE Act or have not been the subject of previous reviews by OCSEC.

IV BACKGROUND

8. (U) The Minister of National Defence issues MAs, which permit CSE to engage in activities that would otherwise be unlawful.[4] The *CSE Act* authorizes five types of MAs: Foreign Intelligence, Cybersecurity - federal infrastructures, Cybersecurity - non-federal infrastructures, Active Cyber Operations, and Defensive Cyber Operations. Each MA contains a range of activities that can be authorized.[5]

9. (U) To issue an MA under the *CSE Act* the Minister must conclude, on a written application from the Chief of CSE, that there are reasonable grounds to believe that the authorization is necessary, and that the conditions for issuing it are met.[6] Akin to the NDA, the *CSE Act* lists conditions that must be satisfied for each authorization, including a general condition that authorized activities must be reasonable and proportionate, having regard to the nature of the objective and the nature of the activities.[7] The Minister may also amend an authorization if there has been a significant change in the application.[8]

10. (U) The Intelligence Commissioner (IC), under the *Intelligence Commissioner Act* section 12, reviews and approves Foreign Intelligence and Cybersecurity MAs issued by the Minister of National Defence. Active Cyber and Defensive Cyber Operations Authorizations issued by the Minister of National Defence do not require IC approval.[9] MAs for activities other than ACO and DCO do not come into force until the IC has approved them.

11. (U) Subsection 21(1) of the *CSE Act* also provides the legislative authority to the Minister to designate "any electronic information, any information infrastructures or any class of electronic information or information infrastructures as electronic information or information infrastructures..." as of importance to the Government of Canada. Related to disclosure of information, for the purposes of both Cybersecurity and Foreign Intelligence, section 45 provides the legislative authority to the Minister to designate persons and classes of persons who may receive information relating to a Canadian or

---

[4] Subsections 22 (3) and (4) of the *CSE Act* prohibit CSE from carrying out activities in furtherance of its foreign intelligence and cybersecurity aspects of its mandates that contravene any other Act of Parliament or involve the acquisition of information that interferes with a reasonable expectation of privacy unless they are carried out under an authorization.

[5] Sections 27 and 28 of the *CSE Act* permit the Minister of National Defence to issue foreign intelligence and cybersecurity authorizations to CSE authorizing any activity specified in the MA in furtherance of its mandate.

[6] *CSE Act*, s. 33(2).

[7] *CSE Act*, s. 34

[8] *CSE Act*, s. 39.

[9] The Active Cyber and Defensive Cyber Operations Authorizations require engagement with the Minister of Foreign Affairs.

a person in Canada.

V FINDINGS AND RECOMMENDATIONS

12. (U) The Minister may issue a Foreign Intelligence Authorization as per subsection 26(1) of the *CSE Act*. Three Ministerial Authorizations were issued under 26(1) of the *CSE Act* in 2019:

a. (S) [redacted]
b. (S)
c. (S)

13. (U) Only one authorization was issued under each of the following subsections of the *CSE Act*:

a. Cybersecurity Authorization – federal infrastructures (27(1));
b. Cybersecurity Authorization – non-federal infrastructures (27(2));
c. Defensive Cyber Operations Authorization (29(1)); and
d. Active Cyber Operations Authorization (30(1)).

14. (S) In contrast to the MAs issued under the NDA, Ministerial Authorizations under the *CSE Act* provide more in-depth information about CSE's activities. The *CSE Act* MAs include a detailed explanation of the classes of activities with examples to illustrate the full scope of the activities being authorized.

15. **(U) Finding no. 1: The application requests from the Chief of CSE presented the Minister with sufficient information to meet the conditions of subsection 33(2). The new applications provide more information than previous applications under the *NDA*, and allow for better transparency of CSE's activities.**

Ministerial Authorization (MA) – Foreign Intelligence – [redacted]

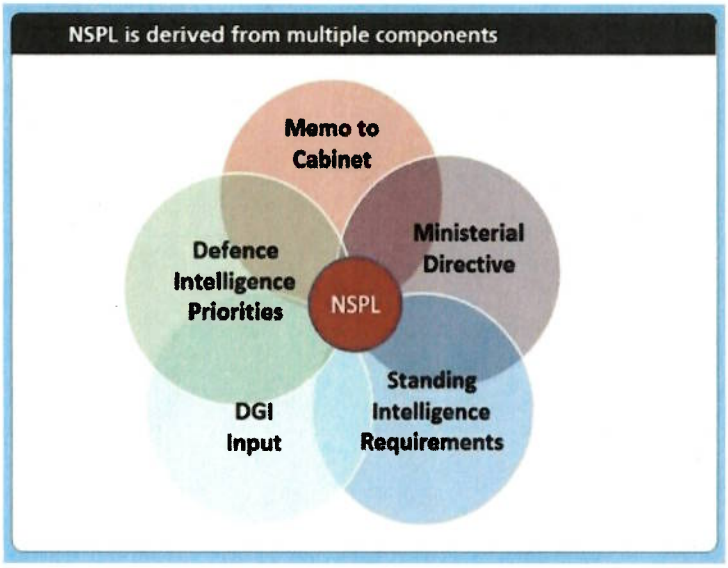
16. (TS/[redacted]) [redacted]

[10] [redacted]

[11] Application to the Minister of National Defence for Foreign Intelligence Authorization [redacted] p. 1.

17. (TS// [redacted] Activities section of the MA application contained information regarding the necessity of this activity. The application states that from July 1, 2018 to December 31, 2018, CSE issued no reports from [redacted][12] However, it later states, "the value derived from this program is significant and without it, CSE's capacity to produce foreign intelligence would be greatly diminished."[13] The value of the activity is unclear from the content of the MA application. CSE's Evaluation Team is currently conducting an evaluation [redacted][14] and as a result, NSIRA will not be reviewing this activity until 2022.

18. (TS) As part of the review of the [redacted] MA, NSIRA staff examined the National SIGINT Priorities List (NSPL). The NSPL is derived from the Standing Intelligence Requirements (SIRs) and the Ministerial Directive to CSE, along with additional components as represented below. The NSPL is a clear representation, organized by tiers, of the government's intelligence priorities as they relate to signals intelligence and it serves to focus CSE's capabilities on the highest foreign intelligence priorities.[15] CSE, in response to a request for information, explained [redacted] to manage its resources in relation to the NSPL. CSE also stated [redacted] on the NSPL.[16]



[12] Ibid., p. 21.
[13] Ibid., p. 26.
[14] CSE response to NSIRA request for certain audit and evaluation reports, received January 3, 2020.
[15] Application to the Minister of National Defence for Foreign Intelligence Authorization [redacted], p. 3.
[16] CSE response to RFI #6, received January 23, 2020.

19. (S) On June 21, 2019, the Minister of National Defence issued a Directive to CSE on the Government of Canada's Intelligence Priorities for 2019-2021. Four priorities were listed:

[redacted]

Ministerial Authorization (MA) – Foreign Intelligence – [redacted]

20. (TS/[redacted] This MA explains that CSE conducts [redacted]

[redacted]

21. (TS) Included in the [redacted] MA is an exceptionally controlled information (ECI) [redacted][18] [redacted] NSIRA staff received a special indoctrination into the [redacted] program to examine [redacted]

22. (TS) [redacted] activities will be examined by NSIRA in further detail in 2021-2022.

Ministerial Authorizations (MA) – Foreign Intelligence – [redacted]

23. (S) Another [redacted] MA issued under the *CSE Act* is [redacted] These are activities [redacted] The CSE area that conducts these activities is [redacted]. There are [redacted] levels of

[17] Application to the Minister of National Defence for Foreign Intelligence Authorization [redacted] p. 1.

[18] [redacted] for an exceptionally controlled information (ECI) program. Individuals must be read-in to this specific program in order to access the information. Due to the sensitive nature of [redacted] further information is not included in this report.

operations:

[redacted]

24. (S// [redacted] could fall under other Foreign Intelligence Authorizations. CSE stated [redacted]

25. (S) The table below depicts the number of [redacted] as of February 18, 2020.[21]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]			

26. (TS) NSIRA asked for legal assessments of areas of high concern for activities under [redacted] MA. CSE provided a legal opinion [redacted]. In that [redacted] opinion, CSE Legal Services advised that [redacted]

[19] [redacted]

[20] CSE response to question 1 of RFI #10, received February 12, 2020.
[21] CSE response to question 2 and 3 of RFI #10, received February 18, 2020.

[redacted]. According to this legal opinion, [redacted]

27. (S) There are no restrictions surrounding [redacted] NSIRA will be examining this in detail in a future review of [redacted] activities.

28. (U) The MA reflects activities that are being contemplated by CSE for the duration of that MA period. At the same time, CSE does not perceive MAs as an exhaustive list of every action that CSE will or will not take.[23] Additionally, CSE self-imposed [redacted] in this MA.

29. (TS) Another area of concern for NSIRA is the reference in the MA application for [redacted]. Similar activities conducted by other security and intelligence departments have been found to require an explicit statutory justification regime. [redacted]. The *CSE Act* contains no such justification regime. NSIRA will be examining this in detail in a future review of [redacted] activities.

30. (TS) CSE further explains in the MA Application that it will conduct a situational risk assessment to ensure that [redacted][25] The situational risk assessment process will be examined by NSIRA in a review of [redacted] in order to understand [redacted]

---

[22] CSE Legal Services, "[redacted]

[23] CSE report comments, received September 22, 2020.

[24] CSE Foreign Intelligence Application for [redacted] p. 5.

[25] Ibid., p. 23.

31. (TS) [redacted] Authorization [redacted] In addition to the expected [redacted] in the course of CSE's [redacted], such as:

[redacted]

32. **(S) Finding no. 2: Although these activities have not yet occurred, there is no indication that CSE has fully assessed the ramifications – legal or otherwise – of the activities authorized in the [redacted] Authorization.** [redacted]

(S) Recommendation no. 1: CSE should seek a fulsome legal assessment on activities authorized by the [redacted] prior to undertaking any collection activities under the [redacted] The legal advice should address whether there is an implicit justification regime created in the [redacted] MA.

Ministerial Authorizations (MA) – Cybersecurity – Federal Institutions

33. (S) The Cybersecurity MA for Federal Institutions most resembles its NDA predecessor in scope and activities. The authorization allows CSE to defend government systems and networks and to provide advice and guidance for strengthening their cybersecurity posture. CSE conducts the following activities under this MA:[27]

- **Network-Based Sensors (NBS)** involve providing network defence services, primarily by deploying sensors on computer networks thereby giving CSE access to all network traffic flowing through federal institutions;
- **Host-Based Sensors (HBS)** are software modules installed on devices and network equipment that automatically acquire information residing on or passing through the devices and then securely transmits the acquired information to CSE; and

---

[26] [redacted] MA Application, pp. 20-1.

[27] Application to the Minister of National Defence For Cybersecurity Authorization Activities on Federal Infrastructures, pp. 4, 9.

- **Cloud-Based Sensors (CBS)** involve the application of defensive solutions for federal infrastructures that use a third party cloud service provider.

34. (S) The above sensors collect data that is automatically used by CSE's Dynamic Defence to stop or mitigate malicious cyber activity. Dynamic Defence allows CSE to act immediately on the information that has been acquired, thereby protecting electronic information and information infrastructures of federal institutions. [redacted]

35. (U) NSIRA plans to review one of the three Cybersecurity Activities listed under the MA for Federal Institutions in each year of NSIRA's CSE three year review plan.

Ministerial Authorizations – Cybersecurity – Non-Federal Institutions

36. (S) A non-federal MA is a new instrument for CSE, as in the past CSE would assist system owners under their own authority, and would not be able to use their whole suite of tools. CSE requires a MA for non-federal institutions when any tool or service deployment risks contravening an Act of Parliament or when there is a reasonable expectation of privacy.

37. (S) NSIRA also examined the first cybersecurity MA allowing CSE to acquire information on a non-federal institution's infrastructure. This MA did not follow the same process and timeline as the other MAs signed by the Minister in summer 2019. On [redacted] 2019, CSE observed strong evidence that a foreign state-sponsored actor had significantly compromised a Canadian company.[29] This company [redacted] infrastructure that is considered a system of importance to the Government of Canada as defined in the *Ministerial Order Designating Electronic Information and Information Infrastructure of Importance to the Government of Canada*.

38. (S) The [redacted] formally requested CSE's assistance in [redacted] and the Minister approved the MA shortly thereafter. The Intelligence Commissioner later approved the authorization. The ability to create and approve cybersecurity MAs in an expeditious manner demonstrates that CSE can react to, and assist with, mitigating harm to systems of importance to the government.

39. (U) The only potential question identified [redacted] NSIRA will be focusing on CSE's private sector relationships in 2022.

[28] CSE response to RFI #5, received January 13, 2020.
[29] Application to the Minister of National Defence for Cybersecurity Activities on Non-Federal Infrastructure, p. 2.

Ministerial Authorizations – Active and Defensive Cyber Operations

40. (U) The Active and Defensive Cyber Operations aspects of CSE's mandates and MAs provide new powers for CSE to take action against targets or cyber threats. The IC does not approve the ACO/DCO MAs. In response to NSIRA's questions on the matter, CSE explained that ACO and DCO are tools leveraged to facilitate authorized activities, and do not acquire private communications. As they do not require any additional authorities not already included in other MAs, IC approval would be redundant.

41. (U) In accordance with subsections 29(2) and 30(2) of the *CSE Act*, CSE requires consultation and consent from the Minister of Foreign Affairs in order to conduct these activities.

- For ACO operations, the Minister of Foreign Affairs must have requested the authorization or has consented to its issue.
- For DCO operations, the Minister of Foreign Affairs must have been consulted.

42. (TS) In the period of review, CSE provided letters of consent from the Minister of Foreign Affairs, but they were not dated. CSE could not provide a date, as they were received electronically. NSIRA requested the dates of the letters from Global Affairs Canada, who responded that [redacted]

43. **(U) Finding no. 3: The [redacted] letters in relation to the Minister of National Defence's consultation with the Minister of Foreign Affairs for Active and Defensive Cyber Operations were not dated. That specific consultation event with Global Affairs Canada was not sufficiently documented.**

(U) Recommendation no. 2: CSE should ensure that the ACO/DCO consultation process with Global Affairs Canada is documented as precisely as possible to allow for an easy verification of its compliance with the sequencing required in the Act.

44. [redacted] The application for ACO authorization states that the activities "will conform to Canada's obligations under international law"[31] and a condition of the MA states,

[30] Email response from GAC dated February 3, 2020.
[31] Application to the Minister of National Defence for Active Cyber Operations Activities, p. 1.

"activities will not contravene Canada's obligations under international law."[32] However, when prompted for an assessment of their obligations, CSE responded they [redacted] "[33] Additionally, CSE responded that [redacted] "[34] In NSIRA's view, CSE has not sufficiently examined its obligations under international law.

45. **(U) Finding no. 4: CSE was unable to provide an assessment of its obligations under international law relevant to the conduct of Active Cyber Operations.**

(U) Recommendation no. 3: CSE should seek a formal legal assessment of the international legal regime applicable to the conduct of active cyber operations prior to undertaking any such operations.

46. (S) On November 29, 2019, NSIRA received a briefing on ACO/DCO activities. NSIRA understood from the briefing that [redacted] However, in response to a request for information to provide the first three-month update to the Minister on ACO, CSE [redacted] [35] This response differed from information provided to NSIRA at the briefing.

47. (S) Upon discussion with CSE, it was explained that [redacted] NSIRA sent a clarification request for all operations in any stage of planning on January 30, 2020, and whether any reports had been written based on ACO activities. CSE [redacted] [6] On the final day of the examination stage of this review, CSE notified NSIRA [redacted] [7] Due to the information received from CSE, NSIRA will immediately conduct a review dedicated to ACO/DCO where the governance and policy framework for these operations can be examined in-depth.

---

[32] Subsection 11(d) of the Communications Security Establishment Active Cyber Operations Authorization [redacted]
[33] RFI #7 response, received February 21, 2020.
[34] CSE comments on draft report, received September 22, 2020.
[35] RFI #3 response, received January 10, 2020.
[36] RFI #3 Clarification Response from CSE, received February 14, 2020.
[37] CSE email sent on February 21, 2020.

Ministerial Orders

48. (U) As stated in section 45 of the *CSE Act*, the "Minister may, by order, designate persons and classes of persons for the purposes of section 43 and subsection 44(1)" for disclosure of Canadian identifying information (CII) if the information has been used, analysed or retained under the following authorizations or activities:

- Cybersecurity and information assurance;
- Foreign Intelligence Authorization; and
- Emergency Authorizations.

49. (U) The Minister may also designate "any electronic information, any information infrastructures or any class of electronic information or information infrastructures as electronic information or information infrastructures..." as of importance to the Government of Canada under subsection 21(1). This designation is relevant to the following aspects of CSE's mandate:

- Defensive Cyber Operations (subsection 18(b)); and
- Cybersecurity and information assurance (subparagraph 17(a)(ii)).

50. (U) NSIRA concluded that the Ministerial Orders related to Cybersecurity and information assurance (subsections 21(1) and 44(1)) were clear and increased transparency.

51. (U) The *Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under a Foreign Intelligence Ministerial Authorization*, on the other hand, raised concerns.

52. (TS) An eight-page briefing package was prepared for the Minister of National Defence seeking his approval of the MO. The first seven pages of the briefing package consisted of an Overview Note, which included the [redacted]

53. (S) The Ministerial Order was found at page 8, the last page of the Overview Note. The MO listed the designed persons or classes of persons as follows: [redacted]

54. (U) NSIRA understood that the Ministerial Order related to Foreign Intelligence Authorizations should be interpreted in consideration of the seven-page Overview Note attached and transmitted as one package.

55. (U) To determine whether CII was only being disclosed to persons and classes of persons listed in the Ministerial Order Overview Note, NSIRA examined all approved requests for Canadian Identifying Information from foreign requesters ("Requests Outside of Canada") since the Ministerial Order was signed on [redacted]

56. (S//CEO) [redacted] requests provided by CSE's [redacted] are as follows:

[redacted]

57. (S) Requests for the disclosure of CII [redacted]

58. (S) When questioned regarding the inconsistencies between the Overview Note language and the application by CSE, CSE ultimately stated that [redacted]

59. (U) Although CSE complied with the language contained in the Ministerial Order, it took a series of meetings and written exchanges to distinguish between the content of the Overview Note (which clearly listed designated persons and classes of persons), and the MO itself [redacted]

60. **(U) Finding no. 5: The *Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under a Foreign Intelligence Ministerial Authorization* only included** [redacted]

[redacted]

(U) Recommendation no. 4: An order issued under section 45 of the *CSE Act* should be as precise as possible in clearly detailing the list of persons or classes of persons designated to receive Canadian identifying information disclosed by CSE.

61. (U) As a result of discussions between CSE and NSIRA, the MND issued a new Ministerial Order on August 25, 2020. It will be part of a designated review of s. 43 of the *CSE Act* and the essential threshold.

VI CONCLUSION

62. (U) The foundational review of the Ministerial Authorizations and Ministerial Orders issued under the *CSE Act* provided NSIRA with an overview of CSE's operational activities. The review was used to inform NSIRA's three-year CSE review plan, and to identify issues requiring deeper examination as part of those reviews.

63. (U) Overall, NSIRA commends CSE's informative briefings on topics covering all aspects of the foreign intelligence and cybersecurity mandates. NSIRA also appreciates the collaborative efforts of CSE's External Review staff in the course of this review.

64. (U) Building on the foundation of this review, NSIRA looks forward to working with CSE to expand our knowledge and understanding of CSE's mission and challenges.

ANNEX A: Objective

(U) The objective of this review was to examine all Ministerial Authorizations and Ministerial Orders granted under the *CSE Act* in 2019 in order for NSIRA to establish a baseline knowledge for which to conduct future reviews. This review was fundamental in informing NSIRA's CSE three-year review plan.

ANNEX B: Scope and Methodology

(U) All Ministerial Authorizations and Ministerial Orders issued by the Minister of National Defence under the *CSE Act* in 2019, accompanying material provided by CSE to the Minister of National Defence or the Minister of Foreign Affairs, and the decisions of the IC were examined as part of this foundational review.

(U) In addition, the *NDA* MAs issued in [redacted] were examined in order to compare the contents with the MAs issued under the *CSE Act*.

(U) NSIRA researchers submitted eleven requests for information to CSE from December 2, 2019 to January 30, 2020. Responses were received by NSIRA from December 18, 2019 to February 21, 2020. Nine briefings were organized by CSE for NSIRA. Dates and topics are listed in Annex D. Additionally, informal meetings were held with NSIRA researchers' counterparts at CSE to discuss the status of the review and to clarify information and document requests.

(U) Researchers also examined relevant CSE policies, procedures, and practices relating to the operational activities authorized by MAs. Additionally, researchers examined all approved requests for the disclosure of Canadian Identifying Information to recipients outside of Canada since the Ministerial Orders were signed on [redacted]

ANNEX C: List of Ministerial Authorizations and Ministerial Orders

(U) There were seven ministerial authorizations issued under the *CSE Act* in 2019:

- **(S) Cybersecurity (Federal Institutions)** authorizes activities on federal infrastructures "that involve accessing a federal institution's electronic information and information infrastructure and acquiring any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it."[39] The activities authorized include Host Based, Network Based, and Cloud Based Sensors. The application was signed [redacted] by Chief, CSE, and approved by the Minister on [redacted] Of note, a change in requirements from the *NDA* MA to the *CSE Act* MA is that instead of reporting to the Minister on the number of private communications, CSE now reports the number of private communications *disclosed*.

- **(S) Cybersecurity (Non-Federal Institutions)** authorizes cybersecurity activities on [redacted] and acquiring any information originating from, directed to, stored on or being transmitted on or through that infrastructure for helping to protect it.[40] The IC was informed verbally of the non-Fed MA on [redacted] followed by transmittal of the signed MA from the Minister's office to the IC on [redacted].

- **(TS//[redacted]) Active Cyber Operations** authorizes CSE to "conduct online activities that degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign target that adversely affect Canada's international affairs, defence or security interests"[41]. The application was signed [redacted] by Chief, CSE, and approved by the Minister on [redacted]

- **(TS//[redacted]) Defensive Cyber Operations** authorizes CSE to "respond directly to cyber threats in order to better protect the electronic information and information infrastructures of both federal institutions and those designated as important to the Government of Canada." The application was signed [redacted] by Chief, CSE, and approved by the Minister on [redacted]

- **(TS//[redacted])** [redacted] authorizes CSE to undertake [redacted]

[39] Application to the Minister of National Defence for Cybersecurity Authorization Activities on Federal Infrastructures, p. 1.
[40] Application to the Minister of National Defence for Cybersecurity Authorization Activities on Non-Federal Infrastructures, p. 1.
[41] Application Made By The Chief, Communications Security Establishment (CSE) To The Minister Of National Defence (MND) For An Authorization Under Subsection 30(1) Of The Communications Security Establishment Act (*CSE Act*), p. 4.

[redacted]"[42] The application was signed [redacted] by Chief, CSE, and approved by the Minister on [redacted]

- **(TS/[redacted])** [redacted] authorizes activities that involve [redacted]"[43] The application was signed [redacted] by Chief, CSE, and approved by the Minister on [redacted]

- **(TS//[redacted])** [redacted] authorizes activities that involve [redacted] The application was signed [redacted] by Chief, CSE, and approved by the Minister on [redacted]

(U) There were three ministerial orders issued under the *CSE Act* on July 22, 2019:

- **(S) Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under a Foreign Intelligence Ministerial Authorization**: This MO identifies the persons or classes of persons that may receive CII collected under a foreign intelligence MA.

- **(S) Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under the Cybersecurity and Information Assurance Aspect of the Mandate**: This MO identifies the persons or classes of persons that may receive CII collected under a cybersecurity MA.

- **(S) Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada**: This MO identifies critical infrastructure, information, entities, and organizations as "of importance". This designation allows CSE to provide cybersecurity assistance under a non-federal institution or defensive cyber operations MA.

---

[42] Application to the Minister of National Defence for [redacted] p. 1.
[43] Application to the Minister of National Defence for Foreign Intelligence Authorization [redacted] p. 1.
[44] Application to the Minister of National Defence for Foreign Intelligence [redacted] p.1.

ANNEX D: Briefings

- (U) November 29, 2019: ACO/DCO
- (U) December 20, 2019: Ministerial Orders
- (TS//[redacted] January 29, 2020: [redacted]
- (TS) January 29, 2020: [redacted]
- (U) January 29, 2020: [redacted]
- (U) February 6, 2020: [redacted]
- (S) February 7, 2020: Cybersecurity briefing (focusing on HBS, CBS, and NBS)
- (U) February 7, 2020: Legislative and Policy Overview
- (U) August 5, 2020: Legal meeting on MO designating recipients of CII from FI

ANNEX E: Findings and Recommendations

- (U) **Finding no. 1**: The application requests from the Chief of CSE, presented the Minister of National Defence with sufficient information to meet the conditions of subsection 33(2) of the *CSE Act*. The new applications provide more information than previous applications under the *National Defence Act*, and allow for better transparency of CSE's activities.

- (S) **Finding no. 2**: Although these activities have not yet occurred, there is no indication that CSE has fully assessed the ramifications – legal or otherwise – of the activities authorized in [redacted] Authorization.[45] [redacted]

- (S) **Recommendation no. 1**: CSE should seek a fulsome legal assessment on activities authorized by [redacted] MA prior to undertaking any collection activities under [redacted] MA. The legal advice should address whether there is an implicit justification regime created in [redacted] MA.

- (U) **Finding no. 3**: The [redacted] letters in relation to the Minister of National Defence's consultation with the Minister of Foreign Affairs for Active and Defensive Cyber Operations were not dated. That specific consultation event with Global Affairs Canada was not sufficiently documented.

- (U) **Recommendation no. 2**: CSE should ensure that the ACO/DCO consultation process with Global Affairs Canada is documented as precisely as possible to allow for an easy verification of its compliance with the sequencing required in the Act.

- [redacted] **Finding no. 4**: CSE was unable to provide an assessment of its obligations under international law relevant to the conduct of Active Cyber Operations.

- (U) **Recommendation no. 3**: CSE should seek a formal legal assessment of the international legal regime applicable to the conduct of active cyber operations prior to undertaking any such operations.

- (U) **Finding no. 5**: The *Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under a Foreign Intelligence Ministerial Authorization* only included [redacted]

[45] This Authorization has since been renamed to [redacted]

- (U) **Recommendation no. 4**: An order issued under section 45 of the *CSE Act* should be as precise as possible in clearly detailing the list of persons or classes of persons designated to receive Canadian identifying information disclosed by CSE.

ANNEX F: THE *CSE ACT*: CHEAT SHEET

UNCLASSIFIED

THE CSE ACT: CHEAT SHEET

	FOREIGN INTELLIGENCE 16	CYBER SECURITY AND INFORMATION ASSURANCE 17	DEFENSIVE CYBER OPERATIONS (DCO) 18	ACTIVE CYBER OPERATIONS (ACO) 20	TECHNICAL AND OPERATIONAL ASSISTANCE 21
MANDATE	**NOT DIRECTED AT CANADIANS**				**SUBJECT TO REQUESTS FROM:** • federal law enforcement and security agencies • the Canadian Armed Forces (CAF) • the Department of National Defence (DND)
MANDATE	**ACTIVITIES REQUIRING MINISTERIAL AUTHORIZATION** MAs protect CSE where our activities would contravene any other act of Parliament *(*or any foreign state for DCO + ACO only)*: would interfere with a reasonable expectation of privacy in relation to a Canadian or person in Canada				
CONDITIONS	• Be reasonable and proportionate • The information acquired could not be reasonably obtained by any other means • Unselected information could not be reasonably acquired by other means • Measures are in place to protect the privacy of Canadians		• Respond to GC intelligence priority objective • Be reasonable, necessary and proportionate • Activities or classes of activities are specified • Start and expiration dates are specified		• CSE would have the same authority to carry out an activity as the agency requesting the assistance • CSE would also be subject to any restrictions or conditions placed on the agency requesting that assistance,such as a warrant or applicable law In addition, for assistance to DND and the CAF, CSE would: • receive a written request from DND or CAF authorized by an appropriate representative • comply with all instructions, parameters, and limits of the authorized CAF activity • comply with all relevant Ministerial Directives issued to CSE by the MND • adhere to agreements or arrangements with DND and CAF • comply with all CSE policies and procedures related to the provision of assistance
CONDITIONS	Information identified as relating to a Canadian or a person in Canada will be used, analyzed or retained only if the information is essential… … to international affairs, defence or security | … to identify, isolate, prevent or mitigate harm		CSE IS STRICTLY PROHIBITED FROM: • Acquiring information *(meaning that all information used to plan/conduct an ADO/DCO operation must be acquired under an FI or cybersecurity MA)* • Intentionally, or by criminal negligence, causing death or bodily harm; • Interfering with the pursuit of justice or democracy		
CONDITIONS		**Designation:** MND may designate any electronic information, any information infrastructures or any class of either as being of importance to the GC			
CONDITIONS	**MEASURES TO PROTECT PRIVACY** • Policies, training, retention, suppression, management approvals, ACL, audit, review, DLS, D2 • Canadian Identifying Information (CII) is only disclosed to designated people/classes of people if the disclosure is essential to international affairs, defence, security, or cyber security				
EXCEPTIONS	• **Using publicly available information** that has been published or broadcast for public consumption, is accessible to the public on the GII or otherwise or is available to the public on request, by subscription or by purchase *(does not include information where a Canadian or person in Canada has a reasonable expectation of privacy.)* • Carrying out activities on information infrastructures to **identify**, **isolate**, **prevent** and/or **mitigate** the **activity** and/or **impact** of **malicious software** on the infrastructure • **Testing or evaluating** products, software, and systems for **vulnerabilities** • Analysing information in order to provide advice and guidance on the **integrity of supply chains** and on the **trustworthiness of e-communications, equipment and services** • Acting as an **investigatory body** under the Investment Canada Act, **reviewing foreign investment** in Canada by analysing and assessing information relating to both the foreign and the Canadian side of the transaction to provide advice to the Ministers of PS / ISED				
APPROVALS	**APPROVED BY MINISTER OF NATIONAL DEFENCE** MND must be satisfied that the conditions set out in law are met, including that the activities are reasonable, necessary and proportionate, and that appropriate privacy protections are in place		DCO — approved if Minister of Foreign Affairs is consulted	ACO — approved if requested, or consented to, by Minister of Foreign Affairs	
APPROVALS	**APPROVED BY INTELLIGENCE COMMISSIONER** • The IC must be satisfied that the ministerial conclusions are reasonable • The IC reviews CSE's MAs before CSE can conduct any operations • The approval of the IC would be binding, meaning that CSE must have the IC's approval to proceed with those activities				
OVERSIGHT	**NSIRA: NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY** • Responsible for reviewing all national security activities across the GC • Reviews CSE's activities for **lawfulness**; Ensures that CSE's activities are **reasonable**, **necessary** and **compliant** with ministerial direction • Is the new review body for any complaints against CSE				
OVERSIGHT	**INTELLIGENCE COMMISSIONER** • Mandated to approve foreign intelligence and cyber security authorization issued by the Minister of National Defence				
OVERSIGHT	**NSICOP: NATIONAL SECURITY AND INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS** • Reviews CSE activities, including the measures it has in place to protect the privacy of Canadians				

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada