National Security and Intelligence Review Agency

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

~~TOP SECRET // SI //CEO // SOLICITOR-CLIENT PRIVILEGE~~

REVIEW OF INFORMATION SHARING ACROSS ASPECTS OF CSE'S MANDATE

(NSIRA REVIEW 2020-07)

This report has been modified slightly from the final version which was provided to the Minister. An error in the language of Finding 4, wherein two different versions were presented within the report and the summary, has been corrected for publication. The correct language was always represented in the body of the final report. The incorrect language has been replaced with the correct language for publication.

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: 1-833-890-0293 Fax: 613-907-4445

I EXECUTIVE SUMMARY

1. (U) This review examined the Communications Security Establishment's (CSE) legal authority for sharing information obtained in the course of one aspect of its mandate ("aspect") for the purposes of fulfilling another aspect of its mandate. Specifically, the review focused on internal information sharing within CSE between the foreign intelligence (FI), and the cybersecurity and information assurance (cybersecurity) aspects of its mandate.

2. (U) NSIRA examined whether CSE's internal sharing of information relating to a Canadian or a person in Canada (IRTC) is consistent with the *Privacy Act,* which limits how collected personal information can be used by a federal institution, and the *CSE Act,* which applies to CSE's incidental collection and use of IRTC. NSIRA concluded that from the descriptions of the aspects in sections 16 and 17 of the *CSE Act,* there may be instances where information acquired under one aspect can be used for the same, or a consistent purpose, as another. This would satisfy *Privacy Act* requirements for sharing information internally. However, this cannot simply be assumed as the purposes of the aspects differ within the *CSE Act*. CSE must conduct case-by-case compliance analysis that considers the purpose of the collection and sharing.

3. (U) NSIRA considers it necessary for the Chief of CSE's application for a Ministerial Authorization to fully inform the Minister of how IRTC might be used and analysed by CSE, including the sharing of IRTC to another aspect, and for what purpose. With one exception, the Chief's applications for the period of review appropriately informed the Minister of National Defence that retained IRTC might be used to support a different aspect. Moreover, the foreign intelligence applications appropriately informed the Minister how CSE assessed "essentiality" for IRTC collected under the FI aspect.

4. (U) Under CSE policy, an assessment of IRTC's relevance, essentiality, or necessity to each aspect is required for sharing information across the aspects. CSE policy offers definitions and criteria for assessing and applying these thresholds to the information. NSIRA found that CSE's policy framework with regards to the internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate is compliant with the *CSE Act.*

5. (U) The information provided by CSE has not been independently verified by NSIRA. Work is underway to establish effective policies and best practices for the independent verification of various kinds of information, in keeping with NSIRA's commitment to a 'trust but verify' approach.

II AUTHORITIES

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

III INTRODUCTION

2. (U) This review examined the Communications Security Establishment's (CSE) legal authority for sharing information obtained in the course of one aspect of its mandate ("aspect") for the purposes of fulfilling another aspect of its mandate. Specifically, the review focused on internal information sharing[1] within CSE between the foreign intelligence (FI), and the cybersecurity and information assurance (cybersecurity) aspects of its mandate. Broadly, this review also documented activities pertaining to the internal sharing of information relating to a Canadian or a person in Canada between the foreign intelligence and cybersecurity aspects, in order to inform future reviews by NSIRA.

3. (~~TS~~) The Office of the Communications Security Establishment Commissioner (OCSEC) previously studied the sharing of, and access to, cyber threat information between CSE's SIGINT and IT Security Branches.[2] OCSEC's review found that CSE's cyber threat information sharing and accessing activities between CSE's SIGINT and IT Security were consistent with *National Defence Act* and *Privacy Act* authorities, and that information shared between the branches posed a minimal risk to the privacy of Canadians.[3]

4. (U) With the coming into force of the *CSE Act,* on August 1, 2019, CSE's legal authorities for conducting its activities have changed since OCSEC's review. In light of this change of legal authority for CSE, NSIRA decided to re-assess and evaluate whether CSE's internal information sharing activities between the FI and cybersecurity aspects are consistent with the *CSE Act* and the *Privacy Act.*

5. (U) NSIRA expects that CSE's internal sharing of IRTC complies with the *CSE Act* and the *Privacy Act*. As such, the focus of this review was to examine the legal authority that allows for CSE to share IRTC between the FI and cybersecurity aspects.

6. (U) The *Communications Security Establishment Act* (*CSE Act*), creates five distinct aspects to CSE's mandate.[4] The *CSE Act* distinguishes between each aspect and its associated activities, as listed below:

- Foreign intelligence (FI) (section 16): to acquire information from the global information infrastructure (GII),[5] and to use, analyse and disseminate the information for the purpose of providing foreign intelligence;

[1] CSE considers information collected under one aspect and then used for the purposes of another as an internal "use" of that information (further discussed in the *Compliance with the CSE Act and the Privacy Act* section of this review). However, for clarity, this review will refer to the internal use or disclosure of information between the FI and cybersecurity aspects as "internal sharing".
[2] OCSEC's *Study of Sharing and Accessing of Cyber Threat Information between CSE's SIGINT and IT Security Branches, 2016-2017.*
[3] OCSEC letter the Minister of National Defence, February 24, 2017.
[4] Subsection 15(2) of the *CSE Act.*
[5] As per section 2 of the *CSE Act*, the global information infrastructure includes electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks.

- Cybersecurity and information assurance (cybersecurity) (section 17): to provide advice, guidance and services to help protect electronic information and information infrastructures of federal institutions or those designated under subsection 21(1) of the *CSE Act*, and to acquire, use and analyse information to do so;

- Defensive cyber operations (section 18): to carry out activities on the GII to help protect electronic information and information infrastructures of federal institutions or those designated under subsection 21(1) of the *CSE Act*;

- Active cyber operations (section 19): to carry out activities on the GII to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of foreign entities; and

- Technical and operational assistance (section 20): to provide technical and operational assistance to federal law enforcement, security agencies, the Canadian Armed Forces and the Department of National Defence.

7. (U) The *CSE Act* also distinguishes between the aspects by requiring different Ministerial Authorizations (MAs) for CSE's activities, except for assistance activities (s. 20).[6] Under the *CSE Act,* and with the exception of assistance activities, CSE's activities must not be directed at a Canadian or any person in Canada, and must not infringe the *Canadian Charter of Rights and Freedoms.*[7] Under the FI and cybersecurity aspects, CSE's activities must not contravene any other Act of Parliament or involve the acquisition of information on or through the GII that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada, unless carried out under a MA.[8]

8. (U) The Minister of National Defence may issue a MA that permits CSE to conduct activities or classes of activities that may contravene any other Acts of Parliament, and, in the case of FI and cybersecurity, would involve the acquisition of information that would interfere with the reasonable expectation of privacy of a Canadian or a person in Canada.[9] FI and cybersecurity MAs must be approved by the Intelligence Commissioner (IC), who must review whether the conclusions made by the Minister in issuing the authorization are reasonable.[10]

9. (U) Thus, CSE is permitted to incidentally[11] acquire information relating to a Canadian or a person in Canada in the course of carrying out activities that are authorized by an FI (s. 26(1)), cybersecurity (s. 27(1) or 27(2)), or emergency (s. 40) MA.[12] CSE refers to this information as

[5] Subsections 22(3) & (4) of the *CSE Act.*
[6] Under the technical and operational assistance aspect, CSE, in the course of providing assistance, has the same authority to carry out any activity as would the respective federal law enforcement or security agency, the Canadian Armed Forces or the Department of National Defence (section 25 of the *CSE Act*).
[7] Subsection 22(1) of the *CSE Act.*
[8] Subsections 22(3) & (4) of the *CSE Act.*
[9] Subsections 22(3) & (4) of the *CSE Act.*
[10] Section 12–14 of the *Intelligence Commissioner Act.*
[11] Subsection 23(5) of the CSE Act defines *incidentally*: "with respect to the acquisition of information, means that the information acquired was not itself deliberately sought and that the information-acquisition activity was not directed at the Canadian or person in Canada."
[12] Subsection 23(4) of the *CSE Act.* Under section 40 of the *CSE Act*, the Minister may issue an emergency authorization for FI or cybersecurity activities if the conditions in section 34 required for issuing a FI or cybersecurity authorization are met, but the time required to obtain the Intelligence Commissioner's approval would defeat the purpose of issuing the authorization.

information relating to a Canadian or a person in Canada (IRTC).[13] In order to issue an authorization, the Minister must be satisfied that CSE will only use, analyse or retain IRTC when it meets the "essentiality" conditions in section 34 of the *CSE Act*, which are different for the FI and cybersecurity aspects. For FI, "essentiality" means an assessment of whether the information is essential to international affairs, defence or security.[14] For cybersecurity, "essentiality" means an assessment of whether the information is essential to identify, isolate, prevent or mitigate harm to (i) federal institutions' electronic information or information infrastructures, or (ii) electronic information or information infrastructures designated under subsection 21(1) of the *CSE Act.*[15]

10. (U) As the *CSE Act* distinguishes between the aspects and the corresponding MAs, NSIRA examined CSE's legal authority for sharing IRTC between the FI and cybersecurity aspects.

11. (U) Due to operational and access-related challenges, including due to the COVID-19 pandemic, this review was not able to independently assess and verify CSE's compliance with the law or compliance with the restrictions and authorities in place when internally sharing and using information between aspects. Additionally, NSIRA was not able to independently observe, investigate or validate the systems used when sharing data between aspects (consult Annex F for a description of processes and methods used by CSE to share information between the two aspects). These data sharing systems may be examined in future NSIRA reviews.

12. (U) NSIRA also intended to review the internal sharing of information with the active (ACO) and defensive (DCO) cyber operations aspects of CSE's mandate, including compliance with the requirements in subsection 34(4) of the *CSE Act* on acquiring information while conducting ACO and DCO cyber operations. Among other things, this subsection stipulates that no information may be acquired pursuant to ACO and DCO authorizations unless done in accordance with an FI (*CSE Act,* s. 26(1*)*), cybersecurity (*CSE Act,* ss. 27(1) & 27(2)), or emergency (*CSE Act,* s. 40(1)) authorization. This facet of the review was instead covered in NSIRA's review of *CSE's Active Cyber Operations and Defensive Cyber Operations - Governance,* and will be further examined in NSIRA's second review of ACO and DCO activities later in 2021.

13. (U) Importantly, this review did not examine the disclosure of Canadian identifying information (CII) outside of CSE.[16]

[13] For example, see Mission Policy Suite, Cybersecurity, page 1 (November 2020) [MPS, Cybersecurity].

[14] For FI, the essentiality requirement comes from paragraph 34(2)(c) of the *CSE Act*: "the measures referred to in section 24 will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security."

[15] For cybersecurity, the essentiality requirement comes from paragraph 34(3)(d) of the *CSE Act: "*the measures referred to in section 24 will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential identify, isolate, prevent or mitigate harm to (i) federal institutions' electronic information or information infrastructures, in the case of an authorization to be issued under subsection 27(1), or (ii) electronic information or information infrastructures designated under subsection 21(1) as being of important to the Government of Canada, in the case of an authorization to be issued under subsection 27(2)."

[16] NSIRA previously examined a selected sample of CSE's disclosures of CII under the authority of the *National Defence Act*. See NSIRA review 08-501-3: *CSE's Disclosures of Canadian Identifying Information*. Under the authority of section 31 of the *NSIRA Act,* NSIRA is currently directing CSE to conduct a study under section 31 of the *NSIRA Act* to demonstrate that their disclosures of CII are done in a manner that is compliant with the *CSE Act.*

III BACKGROUND

What is IRTC?

14. (U) While the *CSE Act* mentions IRTC several times,[17] it is not clearly defined. In practice, IRTC is the information about Canadians or persons in Canada that may be incidentally collected by CSE while conducting FI or cybersecurity activities under the authority of an MA. According to CSE policy, IRTC is any information recognized as having reference to a Canadian or person in Canada, regardless of whether that information could be used to identify that Canadian or person in Canada.[18]

15. (U) There is a distinction to be made between IRTC and Canadian identifying information (CII). For example, the *CSE Act* uses both IRTC and CII throughout the Act to describe types of information. Where IRTC is any information recognized as *having reference* to a Canadian or a person in Canada, CII is information that could be used to *identify* a Canadian or a person in Canada and that has been used, analyzed or retained under a FI or emergency authorization. CSE describes CII as a subset of IRTC.[19] CII may be disclosed by CSE to designated persons under section 43 of the *CSE Act.*

Internal Sharing of IRTC at CSE

16. (~~TS~~) In some circumstances, CSE policy allows for IRTC collected under the authority of one aspect to be shared for use under another aspect (see Annex D for a description of the other types of information that is shared between the FI and cybersecurity aspects). CSE policy permits FI to be used internally to fulfill cybersecurity requirements.[20] Information retained under the cybersecurity aspect may be used by CSE personnel operating under the FI aspect, unless the information is subject to any conditions imposed on it by external clients or disclosing entities.[21] According to CSE, sharing information across aspects of the mandate enables CSE to carry out its activities in support of Government of Canada priorities.[22]

17. (~~TS~~) In the cybersecurity context, CSE explained that any IRTC shared internally in support of the FI aspect [description of CSE operations]

[17] See sections 24, 23(4), 34(2)(c), 34(3)(d), & 44(1) of the *CSE Act.* For example, it is described in section 34 as "information acquired under [an] authorization that is identified as relating to a Canadian or a person in Canada".
[18] Although not in force during the period of review, MPS Foreign Intelligence, v.5.0, approved on February 18, 2021, CSE's definition of IRTC in policy is as follows: "IRtC is any information recognized as having reference to a Canadian or person in Canada, regardless of whether that information could be used to identify that Canadian or person in Canada. It can include Canadian identifying information (CII), which is any information that identifies, or could be used to identify, a Canadian or person in Canada, including entities such as corporations and other organizations (e.g. phone numbers, email addresses, etc.). IRtC can also include information that will not necessarily lead to the identification of a Canadian or person in Canada (such as a Canadian postal code or other information about a non-identifiable Canadian or person in Canada)."
[19] CSE factual accuracy comments, August 19, 2021.
[20] [description of CSE operations]
[21] MPS, Cybersecurity, section 26.2. These are entities that request Cyber Centre services through an established client arrangement, such as federal institutions and SOIs. It also refers to consumers, subscribers, and those who access Cyber Centre services, such as Cyber Alerts.
[22] *Sharing information for use across aspects of the CSE Mandate*, CSE Briefing for NSIRA February 7, 2020, page 6.

[description of CSE operations] [3] [24]

18. (~~TS//SI~~) An example that CSE provided [example of CSE operations] [6] [7] Sharing this information across the aspects of the mandate enabled CSE to help protect GC information and information infrastructures as well as those of Systems of Importance (SOI), by identifying, isolating and mitigating the threat, and provided GC decision-makers with a comprehensive view of the foreign threats targeting Canada.

19. (~~TS~~) After reviewing a random selection of reports,[28] in addition to receiving information by CSE and interviewing analysts familiar with working on both FI and cybersecurity,[29] NSIRA learned that the IRTC shared[30] between the FI and cybersecurity aspects generally included: [list of operational data utilized in the system] CSE policy permits [1]

20. (U) CSE asserts that although IRTC is shared across the aspects, activities will not be directed at Canadians or persons in Canada.[32] As previously mentioned, CSE must not direct its activities at a Canadian or any person in Canada.

IV FINDINGS AND RECOMMENDATIONS

Compliance with the *CSE Act* and the *Privacy Act*

What Acts Apply to the Internal Sharing of Information?

21. (~~S~~) The relevant statutes that apply to CSE's internal information sharing are CSE's enabling statute, the *CSE Act*, and the *Privacy Act.* The *CSE Act* does not provide a clear authority to share IRTC between the aspects. Likewise, the *CSE Act* disclosure provisions for CII in sections 43–45 do not *prima facie* contemplate internal sharing of IRTC, as to disclose information under these provisions, the Minister would need to authorize CSE to collect and

[23] CSE response to RFI-08, October 8, 2020, Q5.
[24] CSE response to RFI-14, March 19, 2021, Q5.
[25] *Sharing information for use across aspects of the CSE Mandate*, CSE Briefing for NSIRA February 7, 2020, pages 4-5.
[26] For example, [example of CSE operations]
[27] [example of CSE operations]
[28] NSIRA reviewers selected at random [number] that were accessible to both FI and cybersecurity personnel between the FI and cybersecurity aspects of the mandate, for the period of review.
[29] CSE response to RFI-11, November 12, 2020, Q4.
[30] Technically, these reports are accessible to personnel working on both aspects rather than being directly 'shared' between specific analysts.
[31] MPS, FI, annex D, (D.xv).
[32] CSE response to RFI-06, September 17, 2020, Q7. NSIRA was not able to independently verify the accuracy of this statement.

disclose CII to itself. Additionally, CSE is not a designated entity under section 45 of the *CSE Act* for the purposes of receiving disclosed information under sections 43 and 44.[33]

22. (U) IRTC could constitute personal information as defined in section 3 of the *Privacy Act*, which is information about an identifiable individual that is recorded in any form. For example, Canadian IP addresses, may constitute both IRTC for the purposes of the *CSE Act* and personal information under the *Privacy Act*.[34] Pursuant to section 4 of the *Privacy Act,* the collection of personal information must relate directly to an operating program or activity of the institution, which includes CSE's mandated activities in the *CSE Act.*

23. (U) The *Privacy Act* also requires that personal information be used and disclosed in manner consistent with sections 7 and 8 of the *Privacy Act.* For reference, Section 7 of the *Privacy Act* states:

> Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except
>
> (a) For the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
>
> (b) For a purpose for which the information may be disclosed[35] to the institution under subsection 8(2).

24. (U) NSIRA examined whether CSE's internal sharing of IRTC is consistent with the *Privacy Act,* which limits how collected personal information can be used by a federal institution. NSIRA concluded that in some circumstances, as described later in the report, internal sharing of IRTC that constitutes personal information between the FI and cybersecurity aspects might satisfy *Privacy Act* requirements. This compliance assessment requires a case-by-case analysis.

CSE Directorate of Legal Services' (DLS) Legal Analysis

25. (~~Protected B//Solicitor-Client Privilege~~) NSIRA examined CSE DLS's[36] legal analysis, provided by Department of Justice (DOJ) lawyers, [legal opinion or advice] [redacted][7] [redacted]

[33] *Ministerial Order Communications Security Establishment, Disclosure of Canadian Identifying Information (Foreign Intelligence)*, signed July 23, 2019; and *Ministerial Order Communications Security Establishment, Disclosure of Information related to Canadians or Persons in Canada (Cybersecurity and Information Assurance),* signed July 22, 2019.

[34] The Supreme Court of Canada stated that in some circumstances the use of an IP address may give rise to a reasonable expectation of privacy. "In my view, the identity of a person linked to their use of the internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address, and telephone number." R. v. Spencer, 2014 SCC 43, at para. 47. Likewise, IP addresses can be considered personal information if it can be associated with an identifiable individual. See *What an IP Address Can Reveal About You,* A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada, May 2013.

[35] Note that the French translation of the *Privacy Act* uses *communiquer* as the equivalent of the English "disclosure" in sections 7 and 8. Both language versions of a bilingual statute are official and authoritative expressions of the law. *See Reference Re: Manitoba Language Rights* [1985] S.C.J. No. 36.

[36] Note that that the legal advice CSE receives from DLS is from the Department of Justice.

[37] [document name] [redacted] from CSE Legal Services to Director General, Policy, Disclosure and Review, dated 17 December 2019, page 2 [document name] [redacted]

[redacted][8] [redacted][9]

26. (~~Protected B//Solicitor-Client Privilege~~) In DOJ's opinion, [legal opinion or advice] [redacted][0] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

38 [related to legal opinion or advice] [redacted]

39 [related to legal opinion or advice] [redacted]

40 [related to legal opinion or advice] [redacted]

[redacted]

27. (~~Protected B//Solicitor-Client Privilege~~) According to DOJ, [redacted] [legal opinion or advice] [redacted][1]

[redacted][2]

Compliance with the Privacy Act

28. (U) NSIRA observes that, in assessing compliance with section 7 of the *Privacy Act*, CSE emphasizes compliance with paragraphs 34(2)(c) and 34(3)(d) of the *CSE Act* to support the internal sharing of personal information across the various aspects of the mandate.

29. (U) As noted, section 7 of the *Privacy Act* requires that personal information under the control of a government institution shall not be used without the consent of an individual, except for two purposes: (1) the purpose for which it was obtained, or for a use consistent with that purpose; or (2) for a purpose for which the information may be disclosed to the institution under subsection 8(2) of the Act. Importantly, a use of information need not be identical to the purpose for which information was obtained; it must only be *consistent* with that purpose.[43]

30. (U) CSE's reliance on section 34 of the *CSE Act* poses a challenge for compliance with the *Privacy Act* because section 34 does not identify the actual purpose of the incidental collection of the IRTC, or provide an authority for internal sharing. Rather, section 34 conditions the Minister's authority to issue an MA on prerequisites. Paragraphs 34(2)(c) and 34(3)(d) of the *CSE Act* specify that the Minister must be satisfied that the privacy protection measures in section 24 of the

[41] CSE DLS response to RFI-6, September 16, 2020, [related to legal opinion or advice] [redacted]

[42] CSE DLS follow up email from meeting with NSIRA, October 20, 2020.

[43] *R. v. Bernard*, 2014 SCC 13, at para 31. In other words, there need only be a sufficiently direct connection between the purpose and the proposed use, such that an individual would reasonably expect that the information could be used in the manner proposed.

Act will ensure that IRTC will be used, analysed, and retained only if it complies with the respective essentiality requirements for FI and cybersecurity, as the case may be. These conditions establish a required threshold for the use, analysis and retention of IRTC collected under a MA, and not an authority for internal sharing of IRTC.

31. (U) Depending on the factual circumstances in which the IRTC is shared, CSE's sharing of IRTC that constitutes personal information between the FI and cybersecurity aspects could be supported by the *CSE Act* and the *Privacy Act* when the information is shared for the purpose for which it was obtained, or for a use consistent with that purpose. This would require a case-by-case assessment to ensure that the purpose for which the IRTC is shared internally is for the same purpose for which it was collected, a purpose consistent with that original purpose for collection, or as permitted by section 7(b), that the sharing is permitted for one of the reasons identified by Parliament in subsection 8(2) of the *Privacy Act*. As mentioned, CSE does not consider internal sharing a disclosure of information. NSIRA notes that the issue of whether internal sharing in this way constitutes a "use" or a "disclosure", under the *Privacy Act* is unclear.[44] Regardless, NSIRA observes that in relying solely on the "essentiality" criteria in section 34, CSE is not assuring itself that it has lawful authority for internal sharing.

32. (U) A justification under section 7(a) or paragraph 8(2)(a) of the *Privacy Act* requires CSE to identify the purpose of the incidental collection and internal sharing, which is found in the corresponding aspect of CSE's mandate. CSE's purpose for collecting, and authority to collect, personal information comes from the *CSE Act.* Sections 16 and 17 of the *Act* identify FI and cybersecurity as operating programs and activities of the institution, and provide the authority to collect information for those purposes. As noted, MAs must authorize collection when activities might contravene any other Act of Parliament, or involve the acquisition of information from or through the GII that interferes with a reasonable expectation of privacy of a Canadian or a person in Canada. From the descriptions of the aspects in sections 16 and 17 of the *CSE Act,* there may be instances where information acquired under one aspect can be used for the same, or a consistent purpose, as exists for another, thus satisfying *Privacy Act* requirements for sharing information internally. However, this cannot simply be assumed as the purposes of the aspects are described differently within the Act.

33. (U) Section 16 of the *CSE Act* authorizes CSE to acquire information from or through the GII, and to use, analyse and disseminate the information for the purpose of providing foreign intelligence in accordance with Government of Canada (GC) priorities.[45] Section 17 of the *CSE Act*, in turn, authorizes CSE to provide advice, guidance and services to help protect the electronic

---

[44] *Gauthier v. Canada (Minister of Consumer & Corporate Affairs)* [1992] F.C.J. No. 1040, suggests that use of personal information by another section of a department is a disclosure, and that information sharing between sections of a department is a consistent use of that information. In *Gauthier,* the Court found that the disclosure of personal information to another section of a department in order to respond to a person's correspondence was consistent with section 8(2) of the *Privacy Act*: "Sections 7 and 8 of the Privacy Act provide that information about an individual cannot be use or disclosed without the individual's consent. There are certain exceptions to this general rule, however Section 8(2) provides that information about an individual can be disclosed without consent if the information is used for a purpose consistent with the purpose for which the information was obtained." Accordingly, internal sharing of IRTC between the aspects could be considered as a disclosure under sections 7(b) and 8(2) of the *Privacy Act*. If internal use is considered a disclosure, the requirements in sections 43-45 of the *CSE Act* for CSE to disclose information would apply to internal sharing. The Minister would be required to designate persons or classes of persons within CSE for the purposes of section 43 and subsection 44(1).

[45] Section 16 of the *CSE Act* states: "'The foreign intelligence aspect of the Establishment's mandate is to acquire, covertly or otherwise, information from or through the global information infrastructure, including be engaging or interacting with foreign entities located outside Canada or by using any other method of acquiring information, and to use, analyse and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities."

information or information infrastructures of federal institutions and designated systems of importance, and to acquire, use and analyse information, from the GII or from other sources, in order to provide such advice, guidance and services.[46]

34. (~~TS//SI~~) When sharing FI-acquired IRTC to support CSE's cybersecurity aspect, there is arguably no shift in purpose if cybersecurity is among the purposes for which the FI is obtained, used, analysed and disseminated. For the period of this review, [related to GC priorities] [redacted] [7] Sharing FI information to fulfill CSE's section 17 cybersecurity objectives of providing advice, guidance and services to help protect federal and designated electronic information and infrastructures could be considered as the same purpose, or consistent with the purpose, for which the IRTC was originally obtained. Where the FI is used in the section 17 aspect to protect federal and designated electronic information and infrastructures, the purpose of collection and the subsequent use of that information could remain the same.

35. (U) For cybersecurity-acquired IRTC, sharing information to the FI aspect could be permissible if the FI purpose is the same as, or consistent with, the purpose for which the information was initially acquired, i.e., for the purpose of providing advice, guidance and services to help protect federal and designated information infrastructures or electronic information. Thus, sharing cybersecurity IRTC to the FI aspect would be permissible under the *Privacy Act* if the internal sharing ultimately serves the purpose of helping to protect federal and designated information infrastructures or electronic information.

36. (U) In sum, if the purpose of CSE's acquisition of personal information is for the purpose of, or consistent with, delivering on the foreign intelligence and/or cybersecurity aspects, CSE's internal sharing of IRTC can be consistent with section 7(a) or paragraph 8(2)(a) of the *Privacy Act,* provided that purpose of the information collection and sharing is identified and justified. CSE must also always satisfy any conditions from the *CSE Act* and relevant MAs on the collection and use of IRTC. To support internal sharing of personal information between the aspects, further analysis is required based on the factual circumstances of each case.

(U) Finding no. 1: CSE's internal sharing of information between the FI and cybersecurity aspects of the mandate has not been sufficiently examined for compliance with the *Privacy Act.*

[46] The cybersecurity and information assurance aspect is described in section 17: "The cybersecurity and information assurance aspect of the Establishment's mandate is to (a) provide advice, guidance and services to help protect (i) federal institutions' electronic information and information infrastructures, and (ii) electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada; and (b) acquire, use and analyse information from the global information infrastructure or from other sources in order to provide such advice, guidance and services."
[47] *National SIGINT Priorities List, version # 2020.02.01.*

(U) Recommendation no. 1: CSE should obtain additional legal advice on its internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate, explicitly in relation to compliance with the *Privacy Act*, which thoroughly addresses the following two issues:

1) Whether the internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate is a use or a disclosure of information for the purposes of the *Privacy Act*; and

2) Whether uses and disclosures are done in accordance with sections 7 and 8 of the *Privacy Act.*

The Ministerial Authorizations

37. (U) The *CSE Act* does not allow the Minister to authorize internal sharing of IRTC, as MAs may only authorize, in the case of FI, the activities or classes of activities listed in subsection 26(2), or for cybersecurity, access and acquisition of the information referred to in subsections 27(1) and 27(2). Any internal sharing of IRTC that constitutes personal information must be done in accordance with the *Privacy Act.*

38. (U) As mentioned, section 24 of the *CSE Act* requires CSE to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of IRTC. When issuing a MA, the Minister must conclude that these measures will ensure that any acquired IRTC will only be used, analysed or retained if it meets the essentiality thresholds in paragraphs 34(2)(c) or 34(3)(d). The Minister may issue these authorizations if they are of the view that such activities would be "reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities."[48] As the Minister considers the reasonableness of the activities proposed against either an FI or cybersecurity purpose, it is conceivable that some activities might be reasonable and proportionate in one context, but not in the other. As activities authorized under subsection 26(2) might acquire a broader range of information than what is contemplated in subsections 27(1) and 27(2), the sharing of FI to cybersecurity might allow for CSE to use more information for a cybersecurity purpose than what is permitted under cybersecurity authorizations alone, and may require different privacy protection measures when using such information.

39. (U) To issue an MA, the Chief of CSE must set out the facts in an application that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary, and that the conditions for issuing it are met.[49] NSIRA considers it necessary for the Chief's application to fully inform the Minister of how IRTC might be used and analysed by CSE, including the sharing of IRTC to another aspect, and for what purpose. This information would also allow for the Minister to make a determination under section 35 whether any other terms,

[48] Subsection 34(1) of the *CSE Act.*
[49] Subsection 33(2) of the *CSE Act.*

conditions, or restrictions are advisable to protect the privacy of Canadians when issuing a FI or cybersecurity authorization.

40. (~~TS//SI~~) For the authorizations issued during 2020, most of the Chief of CSE's applications indicated that collected and retained information might be used under a different aspect, while the text of most of the corresponding MAs did not mention use under a different aspect.[50] This situation was reversed in one instance: [example of CSE operations] [redacted] [1]

41. (~~TS//SI~~) Moreover, the 2020 FI applications and authorizations indicate that in order to meet the essentiality condition for retention of IRTC under subsection 34(2)(c) of the *CSE Act,* IRTC will be retained if it is assessed as essential to cybersecurity.[52] In these instances, cybersecurity is included under the concept of "essential to security", thus providing the Minister with additional context as to how the essentiality conditions are assessed and met by CSE.[53] NSIRA considers this information necessary for the Minister to assess whether the conditions listed in section 34 of the *CSE Act* for issuing the authorization are met.

(U) Finding no. 2: With one exception, the Chief of CSE's applications for Ministerial Authorizations issued in 2020 informed the Minister of National Defence that retained information might be used to support a different aspect.

(U) Finding no. 3: The applications for foreign intelligence authorizations by the Chief of CSE for the period of review appropriately informed the Minister of National Defence how the essentiality condition in paragraph 34(2)(c) is met for IRTC collected under the FI aspect.

(U) Recommendation no. 2: All foreign intelligence and cybersecurity applications from the Chief of CSE should appropriately inform the Minister of National Defence that retained information might be used to support a different aspect.

Assessment of Essentiality, Necessity, and Relevancy

42. (U) Under CSE policy, an assessment of IRTC's relevance, essentiality, or necessity to each aspect is required for sharing information across the aspects (see Annex G for CSE's policy thresholds and definitions used to assess IRTC when shared between the aspects). These terms

[50] The following applications mention that IRTC will be used to support a different aspect, but do not mention it in the corresponding MA: Application for Cybersecurity Activities – Federal (June 26, 2020), para 58; [document name] (August 25, 2020), para 96; [document name] (August 25, 2020), para 68.
[51] At para 19.
[52] The following FI MAs indicate that IRTC will be retained if it is assessed as essential to international affairs, defence, security or cybersecurity: [document name] at paras 77, 137; [document name] at paras 6(d), 94, 103, 165, 166, 168; [document name] at paras 41—44, 54(d) & (g); [document name] at paras 65, 144; and [document name] at paras 40 –41, 57(d).
[53] CSE response to RFI-09, October 27, Q5.

come from the *CSE Act*, but are not defined in the Act. CSE policy offers definitions and criteria for assessing and applying these thresholds to the information. NSIRA did not assess these policy thresholds or definitions for lawfulness, or how these requirements are satisfied by CSE when internally sharing IRTC. This may be examined in future reviews.

43. (~~TS~~) CSE policy also sets forth the criteria by which to authorize the sharing of IRTC across aspects (see Annex E for the approval processes at CSE for sharing information). Before any IRTC may be shared across aspects of the mandate, the information must be assessed for essentiality to the aspect for which it was acquired. If it does not pass this initial essentiality threshold, the information must be deleted.[54]

44. (~~Protected B//Solicitor-Client Privilege~~) According to CSE, [redacted] [legal opinion or advice] [redacted]

45. (U) NSIRA agrees that the *CSE Act* does not require that internally shared IRTC between the FI and cybersecurity aspects meet both of the essentiality conditions of paragraphs 34(2)(c) and 34(3)(d) of the *CSE Act*. Subsections 22(3) and 22(4) of the *CSE Act* require an FI or cybersecurity MA when the activities carried out in furtherance of either aspect involve acquiring information from the GII that may interfere with a reasonable expectation of privacy, or for activities that might contravene an Act of Parliament. MAs may only authorize the activities or classes of activities listed in subsection 26(2) for FI, or to access information infrastructures and acquire the information referred to in subsections 27(1) and 27(2). As mentioned, the "essentiality" thresholds in section 34 condition the Minister's authority to issue an MA on the prerequisite of the privacy protection measures in section 24. Such a requirement can be understood as applying to use, analysis and retention of IRTC collected by CSE under the authority of a MA and within the confines of a single aspect. Therefore, there is no legal requirement within the *CSE Act* that CSE observe the essentiality threshold of the aspect of which the IRTC is internally shared. IRTC must only meet the original essentiality condition of either paragraph 34(2)(c) or 34(3)(d) when IRTC is acquired, as required by the MA authorizing its actual incidental collection.

(U) Finding no. 4: CSE's position that they do not need to assess "essentiality" twice when sharing information between the foreign intelligence and cybersecurity aspects of the mandate is compliant with paragraphs 34(2)(c) and 34(3)(d) of the *CSE Act*.

V CONCLUSION

46. (U) As the *CSE Act* distinguishes between the aspects and the corresponding MAs, NSIRA examined CSE's legal authority for sharing IRTC between the FI and cybersecurity aspects of its mandate. NSIRA concludes that internal sharing may be consistent with the *Privacy Act* in some

[54] CSE response to RFI-06, September 16, 2020, Q6.
[55] CSE DLS response to RFI-06, September 17, 2020, Q2. [legal opinion or advice] see CSE response to RFI-11, March 19, 2021, Q14.

circumstances. However, CSE must give further consideration to the purpose of the collection of the IRTC to justify any internal sharing of IRTC.

47. (U) This review also established a foundational understanding of some of the processes, systems, and compliance measures applied by CSE when sharing IRTC across aspects. Although NSIRA was not able to independently verify this information, NSIRA intends to build upon this information in future reviews.

ANNEX A: OBJECTIVES, SCOPE, AND METHODOLOGY

1. (U) Initially, NSIRA intended to examine the internal sharing of IRTC between aspects of CSE's mandate in a thematic manner that covered several operational areas and several aspects. The review intended to examine the sharing of information between aspects of CSE's mandate for the period of August 1, 2019 to August 1, 2020, with the objective to independently assess and evaluate:

- Compliance with legal, ministerial, and policy requirements, including adequate management of compliance risks when conducting information sharing activities between aspects of CSE's mandate; and,

- CSE's policies, procedures and practices on the internal sharing of information between aspects of the mandate.

2. (U) Due to operational realities, including COVID-19 related disruptions and access challenges, the objectives, scope, and methodology of this review were significantly reduced from the original Terms of Reference (sent to CSE on August 28, 2020), to focus mainly on the legal authority for sharing of information between the FI and cybersecurity aspects.

3. (U) For this review, NSIRA examined documents and records relevant to the sharing of information between aspects of CSE's mandate, from the coming into force of the *CSE Act* on August 1, 2019, until August 1, 2020.

4. (U) Two interviews were conducted with CSE employees involved with information sharing across CSE's aspects, and an interview was conducted with a Department of Justice lawyer in CSE's Directorate of Legal Services familiar with the legal framework of such activities.

5. (U) NSIRA also completed a foundational description of some of the processes, systems, and compliance measures in place when sharing such information, in order to establish a baseline of knowledge to inform future reviews.

ANNEX B: MEETINGS AND BRIEFINGS

Briefing. “Information Sharing: Sharing information for use across aspects of the CSE Mandate”, NSIRA Briefing, February 7, 2020.

NSIRA meeting with counsel from the Department of Justice at CSE DLS, October 13, 2020.

NSIRA meeting with CSE analysts, October 20, 2020.

ANNEX C: FINDINGS AND RECOMMENDATIONS

(U) Finding no. 1: CSE's internal sharing of information between the FI and cybersecurity aspects of the mandate has not been sufficiently examined for compliance with the *Privacy Act.*

(U) Recommendation no. 1: CSE should obtain additional legal advice on its internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate, explicitly in relation to compliance with the *Privacy Act*, which thoroughly addresses the following two issues:

> 1) Whether the internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate is a use or a disclosure of information for the purposes of the *Privacy Act*; and
>
> 2) Whether uses and disclosures are done in accordance with sections 7 and 8 of the *Privacy Act.*

(U) Finding no. 2: With one exception, the Chief of CSE's applications for Ministerial Authorizations issued in 2020 appropriately informed the Minister of National Defence that retained information might be used to support a different aspect.

(U) Finding no. 3: The applications for foreign intelligence authorizations by the Chief of CSE for the period of review appropriately informed the Minister of National Defence how the essentiality condition in paragraph 34(2)(c) is met for IRTC collected under the FI aspect.

(U) Recommendation no. 2: All foreign intelligence and cybersecurity applications from the Chief of CSE should appropriately inform the Minister of National Defence that retained information might be used to support a different aspect.

(U) Finding no. 4: CSE's position that they do not need to assess "essentiality" twice when sharing information between the foreign intelligence and cybersecurity aspects of the mandate is compliant with paragraphs 3*4(2)(*c*)* and 3*4(*3*)(*d*)* of the CSE Act.

ANNEX D: PARTNER AND CLIENT INFORMATION AND PUBLICLY AVAILABLE INFORMATION SHARED BETWEEN THE FI AND CYBERSECURITY ASPECTS

1. (~~Protected B~~) Under the cybersecurity aspect, federal and non-federal clients may disclose cyber threat information to CSE as Canada's lead agency for cybersecurity, or when seeking CSE services to analyse and mitigate known or suspected cyber incidents. Disclosed information may be used for FI purposes provided that it is done so for the purposes of identifying, isolating, preventing or mitigating harm to federal systems or systems of importance to the GC.

2. (~~Protected B~~) The documentation that governs CSE's arrangements with GC and non-federal clients specifies that information obtained by CSE from a given client's network or system that is relevant to the cybersecurity aspect may be shared with partners [CSE operational information] or internal partners for GC clients) involved in cybersecurity for the purposes of identifying, isolating, preventing or mitigating harm to federal systems or systems of importance to the GC.[56] However, this type of documentation does not explicitly mention that clients' information might be used for FI purposes. For the purposes of obtaining the informed consent of disclosing entities, NSIRA considers it appropriate for CSE to be fully transparent with how clients' information might be used by CSE.

3. (~~Protected B~~) When client information is shared with [CSE operational information] partners, the information is anonymized and identifiable information is omitted. Any releasable cybersecurity products created from client information must only contain information necessary to mitigate a cyber compromise.[57] Additionally, disclosing entities may also impose specific restrictions on the use and sharing of their data at the time of disclosure.[58]

4. (~~TS~~) As per subsection 21(1) of the *CSE Act*, CSE is permitted to acquire and use publicly available information without seeking a MA. Currently, [related to legal opinion or advice] [redacted] [9]

[56] CSE response to RFI-09, October 20, 2020, Q4; *Template_CONOP_Digital Signatures; LoR Cybersecurity Authorization Non-Federal Infrastructures; Template – LoR (Letter of Request) Digital Signatures,* rreceived as part of RFI-15, March 24, 2021, Q4.
[57] MPS, Cybersecurity, section 22.2.
[58] MPS, Cybersecurity, section 20.7. Note that NSIRA did not independently verify any collection, use or sharing of client information by CSE.
[59] CSE response to RFI-11, November 17, 2020, Q7. NSIRA did not receive [related to legal opinion or advice]

ANNEX E: APPROVAL PROCESS AND SHARING RELEASE APPROVALS

Approval Processes for Sharing IRTC

1. (~~TS//SI~~) The appropriate approval authority for sharing information is outlined in CSE internal policy, where the nature of the information dictates the release authority. CSE policy requires management approval (known as the release authorities) before sharing unsuppressed IRTC between aspects. However, policy does not stipulate the actual process for approval; this is determined by the relevant operational areas in accordance with their business practices.[60] The Mission Policy Suite (MPS) requires all management decisions to be documented and retained in a central repository for transparency and accountability purposes. Those records must be accessible for review purposes.[61] However, for this review, NSIRA was unable to independently verify and assess the approval process for internally shared IRTC.

2. (~~TS~~) Generally, CSE requires management approval for sharing information contained within a report for use across aspects of the mandate, and will elevate the appropriate release authority when the information contains IRTC.[62] The appropriate release authority and conditions for release are outlined in policy (discussed below). The release authority is responsible for the information exchange, and must be informed if any changes are made to the data that result in a change in the type of privacy-related information to be shared.[63]

3. (~~TS~~) Automated sharing techniques [related to GC priorities] [redacted][4]

Cybersecurity IRTC to Foreign Intelligence

4. (U) Retained IRTC under the cybersecurity aspect can be shared to FI as a Releasable Cybersecurity Product (RCP), which must meet the requirements listed below. The release authority is determined by the privacy impact that the release of information may have on an individual or entity, which is in turn determined by the level of sensitivity and privacy impact of the IRTC.[65] Depending on the level of sensitivity of the IRTC, operational managers or supervisors from the Canadian Centre for Cyber Security (CCCS, or Cyber Centre)[66] must approve RCPs containing IRTC.[67]

5. (U) The requirements for a RCP as per CSE policy include the following:[68]

[60] CSE response to RFI-06, September 17, 2020, Q8; CSE response to RFI-08, October 8, 2020, Q4.
[61] CSE response to RFI-06, September 17, 2020, Q8.
[62] CSE response to RFI-08, October 8, 2020, Q4.
[63] CSE response to RFI-08, October 8, 2020, Q4.
[64] MPS, Cybersecurity, section 25.6; MPS, FI, section 29.2.
[65] See MPS, Cybersecurity, section 7.1.
[66] The CCCS is part of CSE. The CCCS leads the government's response to cyber security events, and it functions under the cybersecurity aspect of CSE's mandate.
[67] MPS, Cybersecurity, section 25.2.
[68] CSE response to RFI-14, March 19, 2021, Q5.

Requirement	When and How the Requirement is Applied
Purpose is to provide advice, guidance, and services	At the time of sharing – why am I sharing this information?
Product only contains retained information	The decision to use and retain information is made at the time the raw data is assessed for relevance and necessity (and in the case of IRTC, essentiality) to the cybersecurity aspect of the mandate.
Privacy Protection	At the time of sharing, as appropriate (e.g., being shared back with the system owner/administrator who already has access to the information on their own systems; or to a broader audience with strict limits on the use of the information). No suppression is required if the IRTC is shared for use under the FI aspect of the mandate when the sharing is for the purposes of supporting activities to help protect the electronic information and information infrastructures of the GC or SOI to the GC
Classification and limitations on use and handling	Either at the time of sharing, or applied at a later stage to the onward use and dissemination of the information by FI. Can include pre-approved uses and conditions, as well as limitations placed by the data/system owner if applicable. Can be applied by report-authoring platforms to End Product Reports (EPRs), restrict the use and dissemination of CSE information.
Auditable	At the time of acquisition, applied automatically by CSE systems. All data entering CSE is automatically tagged with a unique identifier, as well as information regarding origin (e.g., MA vs non-MA, disclosing client if applicable etc.), access restrictions if applicable, aspect of the mandate under which the data was acquired, date and time of acquisition, use and handling requirements.
Approved for release	At the time of sharing. The approval authority depends on the nature of the information. See table in s. 25.2 in the MPS cybersecurity chapter.

Foreign Intelligence IRTC to Cybersecurity

6. (~~TS~~) IRTC under the FI aspect can be released to CCCS as a Releasable SIGINT Product (RSP). RSPs that contain information with a recognized Canadian privacy interest, or based on material with a Canadian privacy interest, require DC SIGINT approval for release, which can be delegated.[69]

7. (~~TS~~) In order to create a RSP to share information for use under the cybersecurity aspect, the following table summarizes how the criteria required in policy must be met:

Requirement	When and How the Requirement is Applied

[69] MPS, FI, section 27.8.

Information is relevant to FI	At the time of assessment. Must be met prior to use.
Privacy protection e.g., suppression of IRTC	At the time of sharing, if necessary. Suppression is mandatory for IRTC included in an EPR shared outside CSE. CCCS clients that receive these EPRs may request this CII through the regular Action-On process. Otherwise, no suppression required if IRTC is necessary for cybersecurity purposes, but other measures to protect privacy are used, for example, restricting the audience for the information.
Sanitization	Either at the time of sharing, or to be applied if/when cybersecurity use requires the information be sanitized to protect CSE equities.
Serialization	At the time of acquisition, applied automatically by CSE systems. All data entering CSE is automatically tagged with a unique identifier, as well as information regarding origin [example of CSE operations] access restrictions if applicable, aspect of the mandate under which the data was acquired, date and time of acquisition, use and handling requirements.
Caveats	Either at the time of sharing, or applied at a later stage to the onward use and dissemination of the information by cybersecurity. Can include pre-approved actions-on. Automatically applied by report-authoring platforms to EPRs, limit the use and dissemination of CSE information.
Approved for release	At the time of sharing. The approval authority depends on the nature of the information. See table in s. 27.8 of MPS FI chapter.

Internal Reviews of Information Sharing

8. (~~TS~~) Internal sharing of information between the aspects is subject to CSE internal review, for both automated sharing and data-based queries. SIGINT Compliance, the group responsible for internal compliance activities under the FI aspect, reviewed CSE-originated queries for 2019 and 2020, and found that query activity was complaint.[70] The CCCS' Internal Program for Operational Compliance (IPOC) did not prioritize compliance monitoring reviews for the past two fiscal years in order to monitor other activities that posed a higher-risk to compliance.[71]

9. (~~TS~~) Automated sharing techniques are also subject to review. SIGINT Compliance is required to revalidate all instances of automated sharing between the FI and cybersecurity aspects every 12 months.[72] The most recent review for the period of July 2019 to September 2020

[70] CSE response to RFI-11, March 19, 2021, Q5.
[71] CSE response to RFI-11, March 19, 2021, Q5. However, during the period under review, CSE noted that IPOC's Compliance Monitoring and Incident Management team (IPOC[redacted] has not yet drafted the Internal Compliance Monitoring Plan for FY 2021-22 and will consider a review of queries for inclusion in that plan.
[72] MPS, FI, section 29.2. The first such review was conducted from June 2018 to June 2019, see *Automated Sharing Between Part (a) and Part (b), Review Conducted by SIGINT Compliance,* CSE response to RFI-04, February 20, 2020, Q1.

found that the [number] of automated sharing were compliant with policy requirements, except for [number] that CSE was unable to assess.[73]

[73] *Annual Validation of Automated Sharing (2020) Review conducted by SIGINT Compliance*, CSE response to RFI-13, January 21, 2021, Q2. Note that due to CSE's pandemic-related critical staffing operational posture, SIGINT Compliance conducted a streamlined review to validate all instances of automated sharing. For instances of automated sharing that were previously reviewed and determined to be compliant in 2019, SIGINT Compliance only sought an attestation from the operational director that no material changes have occurred since the last review. If the operational director provides an attestation, the instance is assessed as compliant.

ANNEX F: METHODS AND PROCESSES OF SHARING

1. (~~TS~~) This section describes the methods and processes used by CSE to share information between the FI and cybersecurity aspects. There is a multitude of systems, methods, and processes that enable information sharing between these aspects, both suppressed and unsuppressed. Note that the processes described below are not static, and that CSE's systems, methods, and processes can change anytime.[74]

2. (~~TS~~) Generally, access to information for each aspect is restricted by [redacted] [related to legal opinion or advice] [redacted]

3. (~~TS//SI~~) For example, [description of CSE operations] [redacted] [6]

4. (U) As required by section 24 of the *CSE Act*, CSE must have measures in place to protect the privacy of Canadians and persons in Canada in the use of information related to them acquired in furtherance of the FI or cybersecurity aspects.

5. (~~TS~~) Suppression and minimization of IRTC is not required by CSE policy when sharing information internally; it is a default practice to share IRTC unsuppressed across the FI and cybersecurity aspects.[77] According to CSE, although not mandated by policy, analysts are encouraged to anonymize or remove privacy-related information where it is not essential for the person using the information to understand the context and value.[78] CSE recognizes that suppression and minimization are a best effort practice, and is of the opinion that CSE is not in contravention of the law should suppression, minimization, anonymization not occur when sharing information between the aspects.[79]

Cross-Aspect Access to both SIGINT and Cyber Centre Raw Data

6. (~~TS~~) When accessing data from another aspect that is not within a reporting product (i.e., RSPs or RCPs), analysts are subject to the policy requirements of the data they are accessing.

---

[74] For example, see CSE response to RFI-11, February 2, 2021.
[75] CSE response to RFI-11, February 2, 2021, Q11.
[76] CSE response to RFI-06, September 17, 2020, Q4. [description of CSE operations] [redacted]
[77] CSE response to RFI-09, October 19, 2020, Q6.
[78] [description of CSE operations] [redacted]
[79] CSE response to RFI-08, October 8, 2020, Q4.

7. (~~TS//SI~~) Under the FI aspect, [description of CSE operations]

8. (~~TS//SI~~) For example, [description of CSE operations]

[80]

9. (~~TS//SI~~) While analysing raw FI data, Cyber Centre personnel must follow all applicable foreign intelligence authorities and policy requirements. The use, handling, and retention of this information is further subject to any restrictions applied to the foreign intelligence data.[81]

10. (~~TS//SI~~) SIGINT personnel may access and use Cyber Centre systems if they meet the requirements in section 26.1 of the MPS Cybersecurity.[82] Access to Cyber Centre systems and raw cybersecurity data is similarly restricted to individuals with an operational need-to-know and mandatory annual policy and compliance training and knowledge testing. [description of CSE operations]

[3]

Reporting – RCPs and RSPs

11. (U) Retained information is internally shared through formal reporting processes in the form of either RSPs, which includes EPRs, or RCPs.

12. (~~TS//SI~~) Cyber Centre personnel operating under cybersecurity requirements may also be internal clients without access to raw FI data.[84] Foreign intelligence information is shared to some cybersecurity personnel as an RSP, meaning that the information has met the requirements for release in CSE policy, including suppression and approval, and is subject to any restrictions on the intelligence data. For the period of review, there [number] RSPs approved for release from the FI aspect that were made available to personnel operating under the cybersecurity aspect.[85]

13. (~~TS//SI~~) Cybersecurity information can be reported and released to SIGINT personnel for subsequent use under the FI aspect via RCPs. Information released through RCPs must meet the requirements for release within CSE policy, and the use must be consistent with the cybersecurity

[80] CSE response to RFI-11, February 2, 2021, Q11. See also MPS, FI, section 3.3.
[81] MPS, FI, sections 20 and 26.5.2.
[82] MPS Cybersecurity, sections 26.1 and 26.2.
[83] CSE response to RFI-11, February 2, 2021, Q11.
[84] Note that the categories of internal partners (part of the SPC) and internal clients who receive FI reporting, are not mutually exclusive.
[85] Note that this does not mean that CCCS personnel accessed any or all of these reports, but based on CCCS personnel's SLINGSHOT login permissions, they have access to these reports to potentially use under the cybersecurity aspect. NSIRA was not able to verify the further use or access of these reports.

aspect of CSE's mandate and used for a subsequent use related to relevant GC priorities.[86] For the period of review, [number] RCPs were disseminated to authorized recipients in SIGINT.[87]

Receiving Suppressed Identifiers from Reporting

14. (~~TS~~) Suppressed IRTC in EPRs disseminated through SLINGSHOT[88] can be requested by internal CSE clients through the existing CII external disclosures process. This is the only mechanism by which suppressed identities can be accessed and released. Supressed IRTC can be requested by submitting a request to the Action-On team (D2A). The requestor must provide the legal authority and operational justification to receive the unsuppressed information.[89] Between August 1, 2019 and August 1, 2020, [description of CSE operations] [redacted] 0

15. (~~TS~~) Although the mechanism for releasing this information is the same as the external disclosures process, it is not considered a "disclosure" of information but an internal "use" of information. As such, the disclosure regime requirements of sections 43 to 46 of the *CSE Act* do not need to be met in order for supressed information to be released to internal CSE clients.[91]

Joint-Reporting

16. (~~TS//SI~~) Information may also be shared between the foreign intelligence and cybersecurity aspects for the purposes of disseminating foreign intelligence under cybersecurity authorities. This foreign intelligence information must first be used for foreign intelligence purposes, and then may be shared to CCCS personnel use under the cybersecurity aspect and only then released under their authorities.[92]

17. (~~TS//SI~~) Approval for sharing of foreign intelligence information under the cybersecurity aspect of the mandate must abide by the appropriate release approval authorities for both aspects.[93] [description of CSE operations] [redacted] 4

Automated Sharing (forms of RSP or RCP)

18. (~~TS~~) Automated sharing is defined in CSE policy as "the use of automated techniques or processes to expedite the dissemination of [releasable reporting products]".[95]

19. (~~TS//SI~~) There are various automated feeds used at CSE to exchange information between the aspects. [description of CSE operations] [redacted]

---

[86] MPS, Cybersecurity, section 26.2.

[87] While these reporting products were shared with authorized recipients in SIGINT, this does not mean that all items were accessed or used by SIGINT for foreign intelligence purposes. [description of CSE operations] [redacted] NSIRA was not able to verify the further use or access of these reports.

[88] [description of CSE operations] [redacted]

[89] MPS FI, section 28.7; MPS, Cybersecurity, section 25.4.6; CSE response to RFI-11, November 17, 2020, Q9.

[90] CSE response to RFI-08, March 10, 2021, Q1.

[91] CSE DLS response to RFI-6, September 16, 2020, Q3; CSE response to RFI-8, March 10, 2021, Q2.

[92] MPS, FI, section 27.9.

[93] MPS, FI, section 27.8.1.

[94] CSE response to RFI-11, November 17, 2020, Q8.

[95] MPS, FI, section 29.2.

[redacted]

20. (~~TS//SI~~) [description of CSE operations and systems] [redacted][6]

[redacted]

21. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

22. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

[redacted]

23. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

24. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

[redacted]

25. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

26. (~~TS//SI~~) [description of CSE operations and systems] [redacted][7]

[redacted]

[96] This information was collated from the following responses: CSE response to RFI-7, March 19, 2020, Q.4-5; CSE response to RFI-11, September 17, 2020.

[97] [description of CSE operations] [redacted]

27. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

28. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

29. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

30. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

31. (~~TS//SI~~) From CSE's assessment, [description of CSE operations and systems] [redacted]

32. (~~TS//SI~~) [description of CSE operations and systems] [redacted]

Other Methods of Sharing

33. (~~TS~~) More informal methods of information exchange may occur between the two aspects. As CSE teams work closely together, analysts might gain knowledge of information that can be useful for either aspect of the mandate. Analysts may exchange general knowledge without any formal reporting.[98] CSE policy provides for analytic exchanges whereby analysts may engage with partners working under a different aspect to work on common objectives by exchanging

[98] CSE response to RFI-11, November 17, 2020, Q2.

information.[99] However, any data exchange must meet the requirements of issuing a RCP or RSP, although the data need not be released through the formal product dissemination systems.[100]

[99] MPS, FI, section 27.14.1; CSE response to RFI-7, March 19, 2021, Q4-5.
[100] CSE noted the language in CSE policy is unclear and will be clarified in future iterations (MPS, Cybersecurity, section 26.2: "while this information does not need to be formally shared"). CSE response to RFI-14, March 19, 2021, Q4.

ANNEX G: POLICY THRESHOLDS FOR INTERNAL SHARING

1. (U) Generally, CSE policy provides that IRTC may be shared internally according to the thresholds outlined below. As mentioned, NSIRA did not assess these thresholds or definitions for lawfulness, but may do so in future reviews. Additionally, NSIRA did not assess how these policy requirements are satisfied in practice.

Foreign Intelligence Aspect to Cybersecurity Aspect

2. (~~TS~~) Under the FI aspect, IRTC must be essential and relevant to the FI aspect prior to sharing, as per the essentiality condition in 34(2)(c) of the *CSE Act*. According to CSE policy, the information must be considered essential to international affairs, defence or security, including cybersecurity.[101] Essential is not defined in CSE policy, though policy provides criteria by which to assess the IRTC as it relates to protecting the lives or safety of individuals, or to serious criminal activity relating to the security of Canada.[102]

3. (~~TS~~) To share FI IRTC information for use under the cybersecurity aspect of the mandate, the IRTC information must be relevant to the cybersecurity aspect. IRTC must further be assessed for necessity to the cybersecurity aspect, meaning whether the information is necessary to help protect GC systems and designated systems of importance. It is a policy decision to apply the threshold of necessity from subsection 44(1) of the *CSE Act*.[103]

4. (~~TS~~) CSE policy requires the standard of necessity, [description of CSE operations] This information is necessary to fulfill the cybersecurity mandate as it enables activities that protect GC systems and designated SOIs (such as by blocking traffic). However, the identifiable individual or entity is not the focus of the activity.[104] Therefore, CSE is of the opinion that since there is a lower risk to the reasonable expectation of privacy of the individual in the cybersecurity context, the threshold of necessity is sufficient for sharing FI-acquired IRTC to the cybersecurity aspect.[105]

Cybersecurity Aspect to Foreign Intelligence aspect

5. (~~TS//SI~~) Under the cybersecurity aspect, IRTC acquired under a MA must be both relevant and essential prior to sharing,[106] as per the essentiality condition under paragraph 34(3)(d) of the *CSE Act*. In CSE policy, IRTC is considered essential when without the information, CSE would be unable to protect federal systems or SOIs and the electronic information on those systems.[107] However, non-MA acquired IRTC, such as client information,[108] must only be necessary.[109]

---

[101] See MPS, FI, section 18.7. However, CSE policy specifically refers to private communications only, and not necessarily IRTC.
[102] MPS, FI, section 18.7.
[103] CSE response to RFI-04, September 17, 2020, Q6-7.
[104] CSE response to RFI-14, March 19, 2021, Q5.
[105] CSE response to RFI-11, March 19, 2021, Q14.
[106] CSE response to RFI-09, October 19, 2020, Q3.
[107] "Essential", within CSE policy, is information that is deemed essential when, without it, CSE would be unable to help protect federal systems or SOIs and the electronic information on those systems. MPS, Cybersecurity, section 9.2.2
[108] A client is an entity that requests Cyber Centre services through an established client arrangement, such as federal institutions and SOIs. It also refers to consumers, subscribers, and those who access Cyber Centre services, such as Cyber Alerts.
[109] CSE response to RFI-7, March 19, 2021, Q4. "Necessary", within CSE policy, is defined as information that is required for the understanding of malicious cyber activities, including behavioural patterns, capabilities, intentions or vulnerabilities patterns, for the purpose of helping to protect federal institutions and designated systems of importance. MPS, Cybersecurity, section 10.3.1.

6. (~~TS~~) The shared IRTC is also assessed for essentiality to the FI aspect (that is, essential to international affairs, defence or security), for both MA and non-MA cybersecurity information. It is a policy decision to further assess cybersecurity-acquired IRTC for essentiality under the FI criteria, [description of CSE operations] [redacted][10]

7. (~~TS//SI~~) As explained by CSE, the cybersecurity-acquired IRTC shared internally in support of the FI aspect is for the purposes of protecting federal institutions or SOIs and the electronic information they contain. This IRTC is used to identify foreign threats to Canadian systems,[111] which aligns with the [related to GC priorities] [redacted]

[110]CSE response to RFI-14, March 19, 2021, Q5; CSE response to RFI-11, March 19, 2021, Q.14.
[111] CSE response to RFI-14, February 11, 2021, Q3.

ANNEX H: INTERNAL SHARING OF IRTC AT CSE